Coates-Wiles theorem

08 September 2023 15:58

§0. Overview

K – im. quadratic field, $\mathcal{O} = \mathcal{O}_K$ – ring of integers

E – ell. curve over $\mathbb{Q}$ with CM by $\mathcal{O}$

Thm. (Coates-Wiles '77) $L(E/\mathbb{Q}, 1) \neq 0 \Rightarrow E(\mathbb{Q})$ is finite.

$E \rightsquigarrow$ Hecke character $\psi = \psi_{E/K}$ s.t. $L(E/\mathbb{Q}, s) = L(\psi, s)$

Thm 1. If $L(\psi, 1) \neq 0$ then for a suitable prime π in $\mathcal{O}$, $S_\pi(E/K) = 0$.

Thm 1 $\Rightarrow$ CW thm: $\exists$ injective map $E(K)/\pi E(K) \hookrightarrow S_\pi(E/K)$

if $S_\pi = 0 \Rightarrow E(K)/\pi = 0 \overset{\text{(Mordell-Weil)}}{\Longrightarrow} \mathrm{rk}\, E(K) = 0 \Rightarrow E(K)$ finite $\square$

We fix a prime $p > 7$ split in K, $\mathfrak{p} \mid p$ in $\mathcal{O}$, so $p = \mathfrak{p}\bar{\mathfrak{p}}$

$F = K(E[\mathfrak{p}])$ – totally ramified at $\mathfrak{p}$, $\underline{\mathfrak{P}} \mid \mathfrak{p}$ in $\mathcal{O}_F$

$\Delta = \mathrm{Gal}(F/K)$, $A = \mathrm{Cl}(F)$, χ_E = character by which Δ acts on $E[\mathfrak{p}]$

$\chi_E : \Delta \to \mathbb{F}_p^\times$

To prove $S_\pi(E/K) = 0$ we need to establish:

$$A^{\chi_E} = 0 \qquad \text{and} \qquad \delta_1(\varepsilon) \neq 0 \text{ for some } \varepsilon \in \mathcal{O}_F^\times$$

Both of these come down to studying the ell. unit $\eta(1, \mathcal{O})$, specifically when it's a p-th power.

§1. When is $\eta(1, \mathcal{O})$ a p-th power?

$\eta(1,\theta) \in \mathcal{O}_F^\times$ is defined as a value $\Lambda_{E,\mathfrak{q}}(P)$ where $\mathfrak{q}$ is some auxiliary ideal

and $P \in E[\mathfrak{p}]$, $P = \xi(\psi(\mathfrak{p})^{-1}\Omega)$, where Ω is a period of E

$\xi : E(\mathbb{C}) \to \mathbb{C}/\mathcal{O}\cdot\Omega$

We'll work in the formal group of E: we parametrize points $(x,y) \in E(F_\mathfrak{p})$ by $z = -x/y$

- this is a bijection between nbhd of $0 \in E(F_\mathfrak{p})$ and nbhd of 0 in $F_\mathfrak{p}$

We have $\Lambda_{E,\mathfrak{q}}(P) = \Lambda_{\mathfrak{p},\mathfrak{q}}(z)$ for $P = (x,y)$, $z = -x/y$

where $\Lambda_{\mathfrak{p},\mathfrak{q}} \in \mathcal{O}_\mathfrak{p}[[T]]^\times$

Lemma: For $Q \in E[\mathfrak{p}]$, we have $Q \in E_1(F_\mathfrak{p})$, and if $Q = (x,y) \neq 0$ then $v_\mathfrak{p}(-x/y) = 1$

We get a map $E[\mathfrak{p}] \xrightarrow{(x,y) \mapsto -x/y} \hat{E}[\mathfrak{p}] \xrightarrow{z \mapsto 1+z} (1+\mathfrak{p}\mathcal{O}_{F,\mathfrak{p}})/(1+\mathfrak{p}^2\mathcal{O}_{F,\mathfrak{p}})$

- Δ-equivariant isomorphism.

Define $\delta : \mathcal{O}_{F,\mathfrak{p}}^\times \to (1+\mathfrak{p})/(1+\mathfrak{p}^2) \xrightarrow{\sim} E[\mathfrak{p}]$ - Δ equivariant hom.

Note: if $u \in \mathcal{O}_{F,\mathfrak{p}}^\times$ is a p-th power, then $\delta(u) = 0$

Prop: For suitable $\mathfrak{q}$ ($N\mathfrak{q} \not\equiv \psi(\mathfrak{q}) \pmod{\mathfrak{p}}$), $L(\psi,1)/\Omega$ is integral at $\mathfrak{p}$,

and $L(\psi,1)/\Omega \equiv 0 \pmod{\mathfrak{p}}$ iff $\delta(\eta(1,\theta)) = 0$

Proof: Let $z = -x/y$ for $P = (x,y) \in E[\mathfrak{p}]$ from before, so $\eta(1,\theta) = \Lambda_{\mathfrak{p},\mathfrak{q}}(z)$. Here

$$\Lambda_{\mathfrak{p},\mathfrak{q}}(T) = \Lambda_{\mathfrak{p},\mathfrak{q}}(0) + \underbrace{\Lambda_{\mathfrak{p},\mathfrak{q}}(0)\,12f\,(N\mathfrak{q} - \psi(\mathfrak{q}))\cdot\frac{L(\psi,1)}{\Omega}}_{\in \mathcal{O}_\mathfrak{p}}\,T + O(T^2) \in \mathcal{O}_\mathfrak{p}[[T]]^\times$$

$\Rightarrow \Lambda_{\mathfrak{p},\mathfrak{q}}(0) \in \mathcal{O}_\mathfrak{p}^\times$ and $\in \mathcal{O}_\mathfrak{p}$. $\rightsquigarrow$ by our choices, $\frac{L(\psi,1)}{\Omega} \in \mathcal{O}_\mathfrak{p}$.

Why does such $\mathfrak{q}$ exist?

$p > 7$ implies that $F = K(E[\mathfrak{p}])/K$ is a proper extension. By CFT $\exists$ prime $\mathfrak{q}$ st

Why does such $\mathfrak q$ exist?

$p>7$ implies that $F=K(E[\bar{\mathfrak p}])/K$ is a proper extension. By CFT, $\exists$ prime $\mathfrak q$ s.t.
for $x=(1,\dots,1,\underset{\substack{\uparrow\\ \text{uniformizer in } \mathcal{O}_{\mathfrak q}}}{\pi'},1,\dots)\in\mathbb{A}_K^\times$, $[x,K]$ acts nontrivially on $K(E[\bar{\mathfrak p}])$.

By CM, this action on $E[\bar{\mathfrak p}]$ by $\psi(x)\cdot x^{-1}$. $\rightsquigarrow \psi(\mathfrak q)\not\equiv 1 \pmod{\bar{\mathfrak p}}$

$\Rightarrow \bar\psi(\mathfrak q)\not\equiv 1 \pmod{\mathfrak p} \underset{\mathfrak p\nmid\psi(\mathfrak q)}{\Longrightarrow} N\mathfrak q\not\equiv\psi(\mathfrak q) \pmod{\mathfrak p}$ — take $\mathfrak a=\mathfrak q$.

We look at image of $\eta(1,0)=\Lambda_{\mathfrak p,\mathfrak a}(z)$ in $1+\underline{\mathfrak p}^2$, which is

$$\Lambda_{\mathfrak p,\mathfrak a}(0)\left(1+124(N\mathfrak a-\psi(\mathfrak a))\frac{L(\bar\psi,1)}{\Omega}\right) \qquad (\mathrm{mod}\ 1+\underline{\mathfrak p}^2)$$

$\Lambda_{\mathfrak p,\mathfrak a}(0)\in\mathcal{O}_{\mathfrak p}^\times$, we can write it as $a_0+a_1\pi+a_2\pi^2+\dots$. But

$v_{\underline{\mathfrak p}}(\pi)=$ ram. index of $F/K=p-1>2$

$$\delta(\Lambda_{\mathfrak p,\mathfrak a}(0))=0 \Rightarrow \delta(\eta(1,0))=\delta\left(1+124(\ )\frac{L(\bar\psi,1)}{\Omega}\right)$$

$$=0 \text{ iff } \frac{L(\bar\psi,1)}{\Omega}\equiv 0\ (\mathfrak p)$$ $\square$

Cor. If $L(\bar\psi,1)/\Omega\not\equiv 0 \pmod{\mathfrak p}$ then $\eta(1,0)^{\chi_E}\in\left((\mathcal{O}_{F,\underline{\mathfrak p}}^\times)^{\chi_E}\right)^p$

Proof: $\delta(\eta(1,0)^{\chi_E})=\underbrace{\delta(\eta(1,0))}_{\in E[p]=E[p]^{\chi_E}}{}^{\chi_E}=\delta(\eta(1,0))\overset{\text{Prop}}{\neq}0 \Rightarrow \eta^{\chi_E}$ not a p-th power. $\square$

§2. Conclusion of the proof.

We need: $A^{\chi_E}=0$ and $\delta_1(\mathcal{O}_F^\times)\neq 0$

We know that $A^{\chi_E}=0 \Leftarrow \eta(1,0)^{\chi_E}\notin\mu_F^{\chi_E}\cdot\left((\mathcal{O}_{F,\underline{\mathfrak p}})^{\chi_E}\right)^p$

Prop: If $L(\bar\psi,1)/\Omega\not\equiv 0 \pmod{\mathfrak p}$ then $A^{\chi_E}=0$

Proof: It is enough to check $\mu_F^{\chi_E}=0$. If not, then $\mu_p\subseteq\mu_F^{\chi_E}$. Therefore

Proof: It is enough to check $\mu_F^{\chi_E} = 0$. If not, then $\mu_p \subseteq \mu_F^{\chi_E}$. Therefore

$\exists$ Δ-equivariant map $E[p] \twoheadrightarrow E[\mathfrak{p}] \xrightarrow{\sim} \mu_p$, so an elt of $\mathcal{H}om(E[p], \mu_p)^{G_K}$

But by Weil's pairing, $\mathcal{H}om(E[p], \mu_p) \cong E[p]$ G_K-equiv.

$\rightsquigarrow$ a nontrivial elt of $E[p]^{G_K} = E[p](K)$.

But for $p > 7$ there are no such pts over K and $E[p] = E[\mathfrak{p}] \oplus E[\bar{\mathfrak{p}}]$. $\square$

We have $\delta_1 : F_{\mathfrak{p}}^\times \to E[\mathfrak{p}]$ Δ-equivariant and $\delta_1(\mathcal{O}_{F,\mathfrak{p}}^\times) \neq 0$

Prop. Suppose p splits in K and $\mathrm{Tr}_{K/\mathbb{Q}} \psi(\mathfrak{p}) \neq 1$. Then

1. $\mu_p \not\subseteq F_{\mathfrak{p}}$ 2. $(\mathcal{O}_{F,\mathfrak{p}}^\times)^{\chi_E}$ is free of rk 1 over $\mathbb{Z}_p$

Proof. 1. If $\mu_p \subseteq F_{\mathfrak{p}}$, then $F_{\mathfrak{p}} = K_{\mathfrak{p}}(\mu_p)$. By Local CFT, $[p, \mathbb{Q}_p(\mu_p)/\mathbb{Q}_p] = 1$

Functoriality $\Rightarrow [p, F_{\mathfrak{p}}/K_{\mathfrak{p}}] = 1$. Also $[\psi(\mathfrak{p}), F_{\mathfrak{p}}/K_{\mathfrak{p}}] = 1$ (defs + CM)

$\Rightarrow [\underbrace{p/\psi(\mathfrak{p})}_{\in \mathcal{O}_{\mathfrak{p}}^\times}, F_{\mathfrak{p}}/K_{\mathfrak{p}}] = 1$. Local CFT implies $p/\psi(\mathfrak{p}) \equiv 1 \pmod{\mathfrak{p}}$.

$\mathrm{Tr}\, \psi(\mathfrak{p}) = \psi(\mathfrak{p}) + \overline{\psi(\mathfrak{p})} = \psi(\mathfrak{p}) + p/\psi(\mathfrak{p}) \equiv 1 \pmod{\mathfrak{p}}$.

$|\mathrm{Tr}\, \psi(\mathfrak{p})| \leq 2\sqrt{p} < p - 1 \rightsquigarrow \mathrm{Tr}\, \psi(\mathfrak{p}) = 1$.

2. $\mathcal{U}^{(n)} = 1 + \mathfrak{p}^n \subseteq \mathcal{O}_{F,\mathfrak{p}}^\times$. We have $\mathcal{O}_{F,\mathfrak{p}}^\times \otimes \mathbb{Z}_p \cong \mathcal{U}^{(1)} \otimes \mathbb{Z}_p$

$\uparrow$ enough to show $\mathcal{U}^{(1)\chi_E}$ free of rk 1.

For some n, $\mathcal{U}^{(n)} \cong \mathcal{O}_{F,\mathfrak{p}}$ Δ-equiv. via a logarithm map.

$\mathcal{U}^{(n)} \otimes \mathbb{Q}_p \cong F_{\mathfrak{p}} \overset{\text{normal basis thm}}{\cong} K_{\mathfrak{p}}[\Delta]$. $K_{\mathfrak{p}}[\Delta]^{\chi_E}$ is 1-dimensional.

$$\mathcal{U}^{(n)} \otimes \mathbb{Q}_p \cong F_{\mathfrak{p}} \overset{\text{basis them}}{\cong} K_p[\Delta]. \quad K_p[\Delta]^{\chi_E} \text{ is 1-dimensional.}$$

$\mathcal{U}^{(n)} \otimes \mathbb{Q}_p \cong \mathcal{U}^{(1)} \otimes \mathbb{Q}_p$. So $(\mathcal{U}^{(1)} \otimes \mathbb{Q}_p)^{\chi_E}$ is 1-dim. $\Rightarrow (\mathcal{U}^{(1)} \otimes \mathbb{Z}_p)^{\chi_E}$ is free of rk 1 because it has no p-torsion by 1. $\square$

Cor. If $L(\psi,1)/\Omega \neq 0 \pmod{\mathfrak{p}}$ and $\operatorname{Tr} \psi(\mathfrak{p}) \neq 1$ then $(\mathcal{O}_F^\times)^{\chi_E} \longrightarrow (\mathcal{O}_{F,\mathfrak{p}}^\times)^{\chi_E}$ is an isomorphism.

Proof: Inj. is clear. For surj., first condition gives that $\eta(1,0)^{\chi_E}$ is not a p-th power in $(\mathcal{O}_{F,\mathfrak{p}}^\times)^{\chi_E} \cong \mathbb{Z}_p \Rightarrow$ it generates the whole $\mathbb{Z}_p$-module by previous prop. $\square$.

Proof of thm 1: Suppose $L(\psi,1) \neq 0$. By Chebotarev, we can find p such that:

- $p > 7$
- $p \nmid 6f$
- $L(\psi,1)/\Omega$ is a p-unit
- p splits in K
- $\operatorname{Tr} \psi(\mathfrak{p}) \neq 1$.

We saw before that $A^{\chi_E} = 0$, and we also get $\eta(1,0)^{\chi_E}$ generates $(\mathcal{O}_{F,\mathfrak{p}}^\times)^{\chi_E}$.

Since δ_1 maps this last group onto $E[\mathfrak{p}]$, $\delta_1(\eta(1,0)) = \delta_1(\eta(1,0)^{\chi_E}) \neq 0$.

As explained this gives $S_\pi(E/K) = 0$ and $E(K) = 0$. $\square$