Coates-Wiles Theorem: Selmer Groups

Khai-Hoan Nguyen-Dang

Padova University, Italy

August 11, 2023
Euler Systems Seminar

Table of Contents

Table of Contents

Coates-Wiles Theorem

Coates-Wiles '77, Rubin '99

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}$ and the class number is 1. Suppose that E is defined over K and it has complex multiplication by $\mathcal{O}$. If $L(E,1) \neq 0$ then $E(K)$ is finite.

Examples

Consider $E/\mathbb{Q}(i) : y^2 = x^3 - x$, we have $\mathrm{End}_{\mathbb{Q}(i)}(E) = \mathbb{Z}[i]$ (e.g. $[i] : (x, y) \mapsto (-x, iy)$)

Remark

The general framework (e.g the assumption on the class number can be removed) is due to Arthaud and Rubin.

Why Selmer Group?

The starting point

Let K be an imaginary quadratic field of class number 1 with the ring of integers $\mathcal{O}$. Suppose that E has complex multiplication by $\mathcal{O}$ and let $\alpha \in \mathcal{O}$ be an endomorphism. If $E(K)/\alpha E(K) = 0$, then $E(K)$ is finite.

Since E is CM, by Mordell-Weil theorem $E(K)$ is a finitely generated $\mathcal{O}$-module. Using K has class number one, $\mathcal{O}_K$ is PID. The result follows from the structure theorem of finitely generated modules over a PID.

Slogan

Selmer group is the smallest group given by local conditions containing $E(K)/\alpha E(K)$.

Main Result

Let $\mathfrak{p} = \pi\mathcal{O}_K$ be some finite prime of K, $(\mathfrak{p}, N_E) = 1$ and π is its generator.

Vanishing of Selmer Group

The Selmer group $S_\pi(E/K) = 0$ if and only if $\mathrm{Hom}(A, E[\mathfrak{p}])^\Delta = 0$ and $\delta_1(\epsilon) \neq 0$ for all $\epsilon \in \mathcal{O}^\times_{K(E[\mathfrak{p}])}$ where

1. A ideal class group of $K(E[\mathfrak{p}])$
2. $\Delta = \mathrm{Gal}(K(E[\mathfrak{p}]/K))$
3. $\delta_1 : K_\mathfrak{p}(E[\mathfrak{p}])^\times \to E[\mathfrak{p}]$ (reciprocity morphism).

Vanishing of the first term

We have $\mathrm{Hom}(A, E[\mathfrak{p}])^\Delta = 0$ if and only if $A^{\chi_E} = 0$ where χ_E is the Hecke character associated to CM elliptic curve E.

Roadmap

$$\begin{array}{ccc}
\text{Mordell-Weil Group } E(K) & \longrightarrow & \text{Selmer Group } S_\pi(E/K) \\
\big\uparrow & & \big\downarrow \\
\text{Euler System of Elliptic Units} & \longleftarrow & \text{Class Group of } K(E[\mathfrak{p}])
\end{array}$$

Euler Systems

Let $\mathfrak{p} \nmid 6N_E$, $K_n := K(E[\mathfrak{p}^n])$, we fix an ideal $\mathfrak{a}$ of $\mathcal{O}$ coprime to $6N_E\mathfrak{p}$

$$R = \{\text{square free ideals of } \mathcal{O} \text{ prime to } 6N_E\mathfrak{a}\mathfrak{p}\}$$

Definition

Let $r \in R, K_n(r) := K_n(E[r\mathfrak{p}^n])$, an Euler system is a collection

$$\{\eta(n,r) \in K_n(r)^\times : n \geq 1, r \in R\}$$

satisfying

1. $N_{K_n(r)}^{K_n(\mathfrak{q}r)} \eta(n, \mathfrak{q}r) = \eta(n,r)^{1-\mathrm{Frob}_q^{-1}}$
2. $N_{K_n(r)}^{K_{n+1}(r)} \eta(n+1, r) = \eta(n,r)$

Bounding Ideal Class Group

Theorem

If η is an Euler system, χ an irreducible $\mathbb{Z}_p$-representation of Δ then

$$|A^\chi| \leq |(\mathcal{O}^\times_{K(E[\mathfrak{p}])}/C_\eta)^\chi|$$

where C_η is the $\mathbb{Z}[\Delta]$-submodule of $\mathcal{O}_K^\times$ generated by μ_K and $\eta(1, \mathcal{O})$.

Under a certain condition of $\eta(1, \mathcal{O})$ we can obtain $A^\chi = 0$. In our case, elliptic units produce the Euler system.

L-function

If E/K is an elliptic curve with CM, there is a Hecke character on K associated to E

$$\psi : \mathbb{A}_K^\times \to \mathbb{C}^\times$$

Deuring

Let $\psi : \mathbb{A}_K^\times \to \mathbb{C}^\times$ be a Hecke character attached to E, then

$$L(E, s) = L(\psi, s)L(\overline{\psi}, s)$$

Stategy

1. Since $L(E,s) \neq 0$, we have $\dfrac{L(\overline{\psi},1)}{\text{constant}} \neq 0 \mod \mathfrak{p}$ which implies $A^{\chi_E} = 0$.
2. It can be shown that $\eta(1,\mathcal{O})$ generates $\mathcal{O}_{K,\mathfrak{p}}^{\times}$ and $\delta_1(\eta(1,\mathcal{O})) \neq 0$, so is $\delta_1(\epsilon)$ for all $\epsilon \in \mathcal{O}_{K(E[\mathfrak{p}])}^{\times}$.
3. By the main result the Selmer group vanishes, hence the Mordell-Weil group is finite.

Other Aspects

1. (Gross, Rubin, Burungale-Flach) Keep the assumptions above, not only $E(K)$ is finite but also $Ш(E/K)$ is finite and

$$\frac{L(\overline{\psi},1)}{\Omega} = \frac{|Ш(E/K)|_K}{|E(K)|} \cdot \prod_v |\phi_v|_K \cdot \text{constant}$$

It follows that

$$L(E/K,1) = \Omega \frac{|Ш(E/K)|_K}{|E(K)^2|} \cdot \prod_v |\phi_v|_K$$

where ϕ_v is the component group of the Neron model of E/K at the prime v.

Other Aspect

1. Recently, Xin Wan showed a number of explicit infinite families of elliptic curves without complex multiplication for which we can now prove the full Birch and Swinnerton-Dyer conjecture.
2. (Tunnell '83) Congruence Number Problem : Apply Coates-Wiles's theorem for $y^2 = x^3 - n^2x$ and its quadratic twists.
3. (Goldfeld 79): 50% of the quadratic twists of an elliptic curve defined over the rationals have analytic rank zero. Some recent progress is due to Burungale-Tian.

Table of Contents

Fundamental Exact Sequence

We have the fundamental exact sequence of G_K-modules

$$0 \to E[\alpha] \to E(\overline{K}) \xrightarrow{\alpha} E(\overline{K}) \to 0$$

Taking Galois cohomology yields

$$0 \to E[\alpha](K) \to E(K) \xrightarrow{\alpha} E(K) \xrightarrow{\delta} H^1(K, E[\alpha]) \to H^1(K, E) \xrightarrow{\alpha} H^1(K, E)$$

We obtain the following exact sequence

$$0 \to E(K)/\alpha E(K) \xrightarrow{\delta} H^1(K, E[\alpha]) \to H^1(K, E)[\alpha] \to 0$$

Selmer Group

Fix a prime $\mathfrak{p}$ of K and consider that E over $K_\mathfrak{p}$, we also get

$$0 \to E(K_\mathfrak{p})/\alpha E(K_\mathfrak{p}) \xrightarrow{\delta} H^1(K_\mathfrak{p}, E[\alpha]) \to H^1(K_\mathfrak{p}, E)[\alpha] \to 0$$

Giving local conditions by the following

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/\alpha E(K) & \xrightarrow{\delta} & H^1(K, E[\alpha]) & \longrightarrow & H^1(K, E)[\alpha] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(K_\mathfrak{p})/\alpha E(K_\mathfrak{p}) & \longrightarrow & H^1(K_\mathfrak{p}, E[\alpha]) & \longrightarrow & H^1(K_\mathfrak{p}, E)[\alpha] & \longrightarrow & 0 \end{array}$$

Definition

$S_\alpha(E/K) := \ker(H^1(K, E[\alpha]) \to \prod_\mathfrak{p} H^1(K_\mathfrak{p}, E))$

Enlarged Selmer Group

We define the enlarged Selmer group for some $\alpha \in \mathcal{O}$. Write $\alpha\mathcal{O} = \mathfrak{p}^n$ with $\mathfrak{p} \not| 6$ and $n \geq 1$

$$S'_\alpha(E/K) := \ker(H^1(K, E[\alpha]) \to \prod_{\mathfrak{q} \nmid \alpha} H^1(K_\mathfrak{q}, E))$$

Characterization

Suppose that $E[\mathfrak{p}^n] \subset K$. Then

$$S'_\alpha(E/K) = \mathrm{Hom}(\mathrm{Gal}(M/K), E[\mathfrak{p}^n])$$

where M is the maximal abelian extension of K unramified outside above $\mathfrak{p}$, i.e. $\mathfrak{p}^n = (\alpha)$.

Proof

Characterization

Suppose that $E[\mathfrak{p}^n] \subset K$. Then

$$S'_\alpha(E/K) = \mathrm{Hom}(\mathrm{Gal}(M/K), E[\mathfrak{p}^n])$$

where M is the maximal abelian extension of K unramified outside above $\mathfrak{p}$.

By the assumption G_K acts trivially on $E[\mathfrak{p}^n]$, so

$$H^1(K, E[\mathfrak{p}^n]) = \mathrm{Hom}(G_K, E[\mathfrak{p}^n])$$

Let $\mathfrak{q}$ be a prime of K not dividing $\mathfrak{p}$, we have E has good reduction at $\mathfrak{q}$ and $H^1(K_\mathfrak{q}, E[\mathfrak{p}^n]) = \mathrm{Hom}(G_{K_\mathfrak{q}}, E[\mathfrak{p}^n])$. By inflation-restriction sequence, we see that the image of the connecting morphism δ is in

$$E(K_\mathfrak{q})/\alpha E(K_\mathfrak{q}) \xrightarrow{\delta} \mathrm{Hom}(G_{K_\mathfrak{q}}/I_{K_\mathfrak{q}}, E[\mathfrak{p}^n]) = \mathrm{Hom}(\hat{\mathbb{Z}}, E[\mathfrak{p}^n]) = E[\mathfrak{p}^n] = \mathcal{O}/\mathfrak{p}^n$$

Proof

Since E has a good reduction at $\mathfrak{q}$, we see that

$$E(K_\mathfrak{q})/\alpha E(K_\mathfrak{q}) \cong \tilde{E}(k)/\alpha \tilde{E}(k) \cong \mathcal{O}/\mathfrak{p}^n$$

It follows that

$$E(K_\mathfrak{q})/\alpha E(K_\mathfrak{q}) \xrightarrow{\delta} \mathrm{Hom}(G_{K_\mathfrak{q}}/I_{K_\mathfrak{q}}, E[\mathfrak{p}^n])$$

is an isomorphism. The enlarged Selmer group can be rewritten as

$$\begin{aligned} S'_\alpha(E/K) &= \{c \in \mathrm{Hom}(G_K, E[\mathfrak{p}^n]) : \mathrm{res}_\mathfrak{q}(c) \in \mathrm{Hom}(G_{K_\mathfrak{q}}/I_\mathfrak{q}, E[\mathfrak{p}^n]) \ \forall \mathfrak{q} \nmid \alpha\} \\ &= \mathrm{Hom}(\mathrm{Gal}(M/K), E[\mathfrak{p}^n]) \end{aligned}$$

where M is the maximal abelian extension of K unramified outside above $\mathfrak{p}$

Technical Lemma

Let $\mathfrak{p}$ be a prime of K lying above $p \geq 5$. Let $n \geq 0$:

1. If $\mathcal{O}_\mathfrak{p} = \mathbb{Z}_p$ or if $E[\mathfrak{p}] \not\subset E(K)$, the restriction map gives an isomorphism

$$H^1(K, E[\mathfrak{p}^n]) \cong H^1(K(E[\mathfrak{p}^n]), E[\mathfrak{p}^n])^{\mathrm{Gal}(K(E[\mathfrak{p}^n])/K)}$$

2. Suppose K is a finite extension of $\mathbb{Q}_\ell$ for some $\ell \neq p$. Then the restriction map gives an injection

$$H^1(K, E)[\mathfrak{p}^n] \hookrightarrow H^1(K(E[\mathfrak{p}^n]), E)[\mathfrak{p}^n]$$

Characterization of Enlarged Selmer Group

Theorem

Suppose E is defined over K. If we denote by $K_n = K(E[\mathfrak{p}^n])$, then

$$S'_\alpha(E/K) \cong \mathrm{Hom}(M_n/K_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}$$

Here M_n is the maximal abelian extension of K_n unramifield outside primes above $\mathfrak{p}$.

Proof

Apply the above lemma and the characterization of enlarged Selmer group.

Table of Contents

Logarithm Map

Let $\mathfrak{p}$ be a prime of K comprime to $6N$. It follows that E has good reduction at $\mathfrak{p}$. The reduction gives the exact sequence of $\mathcal{O}$-modules

$$0 \to E_1(K_\mathfrak{p}) \to E(K_\mathfrak{p}) \to \tilde{E}(k) \to 0$$

It can be shown that this sequence is split

$$E(K_\mathfrak{p}) \cong E_1(K_\mathfrak{p}) \times \tilde{E}(k)$$

Moreover, the logarithm map gives an isomorphism

$$\log_E : E_1(K_\mathfrak{p}) \cong \mathfrak{p}\mathcal{O}_\mathfrak{p}$$

This map extends to a subjective map

$$\log_E : E(K_\mathfrak{p}) \to \mathfrak{p}\mathcal{O}_\mathfrak{p}$$

whose kernel is finite and has no $\mathfrak{p}$-torsion.

Kummer Pairing

We define

$$\langle , \rangle_{\pi^n} : E(K_{\mathfrak{p}}) \times K_{n,\mathfrak{p}}^{\times} \to E[\mathfrak{p}^n]$$
$$\langle P, x \rangle_{\pi^n} := Q^{\mathrm{Art}(x, K_{n,\mathfrak{p}})} - Q$$

where $Q \in E(\overline{K}_{\mathfrak{p}})$ such that $\pi^n Q = P$ and Art is the local Artin map.

Linearity

Let $P \in E_1(K_{\mathfrak{p}})$, $x \in K_{n,\mathfrak{p}}^{\times}$ and $a \in \mathcal{O}_p$. Then

$$\langle aP, x \rangle_{\pi^n} = a \langle P, x \rangle_{\pi^n}$$

All together

Let $P \in E_1(K_\mathfrak{p}$ such that $\log_E(P) = \pi$. Define $\delta_n : K_{n,\mathfrak{p}}^\times \to E[\mathfrak{p}^n]$ by

$$\delta_n(x) := \langle P, x \rangle_{\pi^n}$$

If $P \in \tilde{E}(k)$, it is a torsion point of order prime to $\mathfrak{p}$, we have

$$\log_E(P) = 0 \text{ and } \langle P, x \rangle_{\pi^n} = 0$$

Theorem

The Galois equivariant morphism (called π^n-reciprocity)

$$\delta_n : K_{n,\mathfrak{p}}^\times \to E[\mathfrak{p}^n]$$

has property: any $P \in E(K_\mathfrak{p})$ and $x \in K_{n,\mathfrak{p}}^\times$

$$\langle P, x \rangle_{\pi^n} = (\pi^{-1} \log_E(P))\delta_n(x)$$

The map δ_n is subjective and $\delta_n(\mathcal{O}_{n,\mathfrak{p}}^\times) = E[\mathfrak{p}^n]$.

Selmer Group

Theorem

Let $K_n = K(E[\mathfrak{p}^n])$ with idele group $\mathbb{A}_{K_n}^\times$. Define

$$W_n = K_n^\times \prod_{v\mid\infty} K_{n,v}^\times \prod_{v\nmid\mathfrak{p}\infty} \mathcal{O}_{n,v}^\times \cdot \ker\delta_n$$

Then $S_{\pi^n}(E/K) \cong \mathrm{Hom}(\mathbb{A}_{K_n}^\times/W_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}$

We can rewrite the enlarged Selmer group

$$S'_{\pi^n}(E/K) = \mathrm{Hom}(\mathbb{A}_{K_n}^\times/W'_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}$$

where $W'_n = K_n^\times \prod_{v\mid\infty} K_{n,v}^\times \prod_{v\nmid\mathfrak{p}\infty} \mathcal{O}_{n,v}^\times$. On the other hand, we have an isomorphism

$$E(K_\mathfrak{p}/\pi^n E(K_\mathfrak{p}) \cong \mathrm{Hom}(K_{n,\mathfrak{p}}^\times/\ker\delta_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}(= \mathcal{O}/\mathfrak{p}^n)$$

Sketch

We have an isomorphism

$$E(K_{\mathfrak{p}}/\pi^n E(K_{\mathfrak{p}}) \cong \mathrm{Hom}(K_{n,\mathfrak{p}}^{\times}/\ker\delta_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}$$

We can rewrite the Selmer group

$$S_{\pi^n}(E/K) \cong \{f \in \mathrm{Hom}(\mathbb{A}_{K_n}^{\times}/W_n', E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)} : \\ \mathrm{res}_{K_{n,\mathfrak{p}}^{\times}} f \in \mathrm{Hom}(K_{n,\mathfrak{p}}^{\times}/\ker\delta_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}\}$$

Hence

$$S_{\pi^n}(E/K) \cong \mathrm{Hom}(\mathbb{A}_{K_n}^{\times}/W_n, E[\mathfrak{p}^n])^{\mathrm{Gal}(K_n/K)}$$

where $W_n = K_n^{\times}\prod_{v|\infty} K_{n,v}^{\times}\prod_{v\nmid\mathfrak{p}\infty}\mathcal{O}_{n,v}^{\times}\cdot\ker\delta_n$

Vanishing of Selmer Group

Apply the previous theorem for $n = 1$.

Theorem

Let $\Delta = \mathrm{Gal}(K(E[\mathfrak{p}])/K)$. The Selmer group $S_\pi(E/K) = 0$ if and only if

$$\mathrm{Hom}(A, E[\mathfrak{p}])^\Delta = 0 \text{ and } \delta_1(\epsilon) \neq 0 \text{ for all } \epsilon \in \mathcal{O}^\times_{K(E[\mathfrak{p}])}$$

Denote by $\overline{\epsilon}$ the closure of ϵ in $\mathcal{O}^\times_{1,\mathfrak{p}}$ and $V = \ker \delta_1 \cap \mathcal{O}^\times_{1,\mathfrak{p}}$, we have Δ-equivariant exact sequence

$$0 \to \mathcal{O}^\times_{K_1,\mathfrak{p}}/V\overline{\epsilon} \to \mathbb{A}^\times_{K_1}/W_1 \to A' \to 0$$

where A' is a certain quotient of A. Applying $\mathrm{Hom}(-, E[\mathfrak{p}])$ and taking Δ-invariant we obtain

$$\mathrm{Hom}(\mathbb{A}^\times_{K_1}/W_1, E[\mathfrak{p}])^\Delta = 0 \text{ iff}$$
$$\mathrm{Hom}(\mathcal{O}^\times_{K_1,\mathfrak{p}}/V\overline{\epsilon}, E[\mathfrak{p}])^\Delta = 0 \text{ and } \mathrm{Hom}(A', E[\mathfrak{p}])^\Delta = 0$$

Isotypical Component

Definition

Let M be a finitely generated Δ module, and hence a $\mathbb{Z}[\Delta]$-module. The p part of M is $M^{(p)} = M \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Given a character $\chi : \Delta \to \mathbb{Z}_p^\times$, we define

$$\epsilon(\chi) = \frac{1}{p-1} \sum_{\sigma \in \Delta} \chi(\sigma)^{-1} \sigma$$

Suppose that χ is an irreducible representation of Δ, we define

$$M^\chi = \epsilon(\chi) M^{(p)}$$

Proposition

Let M be a $\mathbb{Z}[\Delta]$-module. Then

1. $M^\chi = \{m \in M^{(p)} : \sigma m = \chi(\sigma) m \forall \sigma \in \Delta\}$
2. $M^{(p)} = \bigoplus_\chi M^\chi$, where the sum is over all the irreducible representations of Δ.

Vanishing of $\mathrm{Hom}(A, E[\mathfrak{p}])^\Delta = 0$

Corollary

Define χ_E the $\mathbb{F}_p$-representation of Δ induced by the action of Δ on $E[\mathfrak{p}]$, we have

$$E[\mathfrak{p}] = E[\mathfrak{p}]^{\chi_E}$$

We give the last vanishing result of my talk.

Theorem

We have $\mathrm{Hom}(A, E[\mathfrak{p}])^\Delta = 0$ if and only if $A^{\chi_E} = 0$.

Thank you for your attention!