Canad. Math. Bull. 2025, pp. 1–11
http://dx.doi.org/10.4153/S000843952510088X

On the Fitting ideals of anticyclotomic Selmer groups of elliptic curves with good ordinary reduction

Chan-Ho Kim

Abstract. We give a short proof of the anticyclotomic analogue of the "strong" main conjecture of Kurihara on Fitting ideals of Selmer groups for elliptic curves with good ordinary reduction under mild hypotheses. More precisely, we completely determine the initial Fitting ideal of Selmer groups over finite subextensions of an imaginary quadratic field in its anticyclotomic $\mathbb{Z}_p$-extension in terms of Bertolini–Darmon's theta elements.

1 Introduction

1.1 The statement of the main result

Let E be an elliptic curve of conductor N over $\mathbb{Q}$ and $p \geq 5$ be a prime of good ordinary reduction for E such that

(Im) the mod p Galois representation $\overline{\rho} : G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{F}_p}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$ is surjective, and

(Ram) $\overline{\rho}$ is ramified at every prime dividing N, so p does not divide Tamagawa factors of E.

Let K be an imaginary quadratic field of odd discriminant $-D_K < -4$ with $(D_K, Np) = 1$ such that

(Spl) p splits in K, and

(Na) $a_p(E) \not\equiv 1 \pmod{p}$.

Write

$$N = N^+ \cdot N^-,$$

where a prime divisor of N^+ splits in K and a prime divisor of N^- is inert in K.

(Def) Assume that N^- is a square-free product of an odd number of primes.

Let K_∞ be the anticyclotomic $\mathbb{Z}_p$-extension of K and K_n be the subextension of K in K_∞ of degree p^n for $n \geq 0$. Let $\Lambda_n = \mathbb{Z}_p[\mathrm{Gal}(K_n/K)] \simeq \mathbb{Z}_p[X]/((1+X)^{p^n} - 1)$ be the finite layer Iwasawa algebra. Under (Def), denote by

Received by the editors May 7, 2025; revised July 8, 2025; accepted July 8, 2025.
Published online on Cambridge Core July 14, 2025.
AMS subject classification: **11F67, 11G40, 11R23.**
Keywords: Refined Iwasawa theory, anticyclotomic Iwasawa theory, Fitting ideals, Selmer groups.

$$\theta(E/K_n) = \sum_{\sigma \in \mathrm{Gal}(K_n/K)} a_\sigma \cdot \sigma \in \Lambda_n.$$

Bertolini–Darmon's theta element of E over K_n which interpolates the square-roots of $L(E/K, \chi, 1)$ for finite order characters χ on $\mathrm{Gal}(K_n/K)$. It is reviewed in Section 2. For the natural projection map $\pi_{n,n-1} : \Lambda_n \to \Lambda_{n-1}$, let $\nu_{n-1,n} : \Lambda_{n-1} \to \Lambda_n$ be the map defined by $\sigma \mapsto \sum_{\pi_{n,n-1}(\tau)=\sigma} \tau$. For $0 \leq m \leq n$, we write $\nu_{m,n} = \nu_{n-1,n} \circ \nu_{n-2,n-1} \circ \cdots \circ \nu_{m,m+1}$. Then we have the equality of ideals of Λ_n (Lemma 2.1)

$$\left(\theta(E/K_n), \nu_{n-1,n}\left(\theta(E/K_{n-1})\right)\right) = \left(\nu_{m,n}\left(\theta(E/K_m)\right) : 0 \leq m \leq n\right),$$

and it is a principal ideal under (Na) (Lemma 2.2).

The goal of this article is to prove the following anticyclotomic analogue of the "strong" main conjecture of Kurihara [14, Conjecture 0.3], which refines the "weak" main conjecture of Mazur and Tate [15, Conjecture 3].

Theorem 1.1 *Under the assumptions mentioned above, i.e., (Im),(Ram),(Spl),(Na), and (Def), the theta elements over K_m with $0 \leq m \leq n$ generate the initial Fitting ideal of dual Selmer groups over K_n, i.e., we have equality of ideals of Λ_n*

$$\left(\theta(E/K_n), \nu_{n-1,n}\left(\theta(E/K_{n-1})\right)\right)^2 = \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}(K_n, E[p^\infty])^\vee\right),$$

which is indeed a principal ideal, where $\mathrm{Sel}(K_n, E[p^\infty])$ is the classical Selmer group of $E[p^\infty]$ over K_n and $(-)^\vee$ means the Pontryagin dual.

Since theta elements interpolate the *square-roots* of twisted Rankin–Selberg L-values, it is natural that the *square* of the ideal generated by theta elements appears in the equality.

The strategy of our proof follows that given in [11] and we also add some details on the "p-destabilization" process and on the comparison of various anticyclotomic Selmer groups of elliptic curves.

2 Bertolini–Darmon's theta elements and anticyclotomic p-adic L-functions

We quickly review the construction of Gross points of conductor p^n, theta elements, and anticyclotomic p-adic L-functions. See [4, 5, 10] for details.

2.1 Gross points

Let K be the imaginary quadratic field of odd discriminant $-D_K < -4$. Define

$$\vartheta := \frac{D_K - \sqrt{-D_K}}{2}$$

so that $\mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\vartheta$. Let B_{N^-} be the definite quaternion algebra over $\mathbb{Q}$ of discriminant N^-. Then there exists an embedding $\Psi : K \hookrightarrow B_{N^-}$ [20]. More explicitly, we choose a K-basis $(1, J)$ of B_{N^-} so that $B_{N^-} = K \oplus K \cdot J$ such that $\beta := J^2 \in \mathbb{Q}^\times$ with

https://doi.org/10.4153/S000843952510088X Published online by Cambridge University Press

$\beta < 0$, $J \cdot t = \bar{t} \cdot J$ for all $t \in K$, $\beta \in \left(\mathbb{Z}_q^\times\right)^2$ for all $q \mid pN^+$, and $\beta \in \mathbb{Z}_q^\times$ for all $q \mid D_K$. Fix a square root $\sqrt{\beta} \in \overline{\mathbb{Q}}$ of β. For a $\mathbb{Z}$-module A, write $\widehat{A} = A \otimes \widehat{\mathbb{Z}}$. Fix an isomorphism

$$i := \prod i_q : \widehat{B}_{N^-}^{(N^-)} \simeq \mathrm{M}_2(\mathbb{A}^{(N^-\infty)})$$

as follows:

- For each finite place $q \mid N^+p$, the isomorphism $i_q : B_{N^-,q} \simeq \mathrm{M}_2(\mathbb{Q}_q)$ is defined by

$$i_q(\vartheta) = \begin{pmatrix} \mathrm{trd}(\vartheta) & -\mathrm{nrd}(\vartheta) \\ 1 & 0 \end{pmatrix}, \qquad i_q(J) = \sqrt{\beta} \cdot \begin{pmatrix} -1 & \mathrm{trd}(\vartheta) \\ 0 & 1 \end{pmatrix}$$

  where trd and nrd are the reduced trace and the reduced norm on B, respectively.
- For each finite place $q \nmid pN^+$, the isomorphism $i_q : B_{N^-,q} \simeq \mathrm{M}_2(\mathbb{Q}_q)$ is chosen so that $i_q\left(\mathcal{O}_K \otimes \mathbb{Z}_q\right) \subseteq \mathrm{M}_2(\mathbb{Z}_q)$.

Under the fixed isomorphism i, for any rational prime q, the local Gross point $\varsigma_q \in B_{N^-,q}^\times$ is defined as follows:

- $\varsigma_q := 1$ in $B_{N^-,q}^\times$ for $q \nmid pN^+$.
- $\varsigma_q := \frac{1}{\sqrt{D_K}} \cdot \begin{pmatrix} \vartheta & \bar{\vartheta} \\ 1 & 1 \end{pmatrix} \in \mathrm{GL}_2(K_\mathfrak{q}) = \mathrm{GL}_2(\mathbb{Q}_q)$ for $q \mid N^+$ with $q = \mathfrak{q}\bar{\mathfrak{q}}$ in $\mathcal{O}_K$.
- $\varsigma_p^{(n)} = \begin{pmatrix} \vartheta & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} p^n & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(K_\mathfrak{p}) = \mathrm{GL}_2(\mathbb{Q}_p)$ where $p = \mathfrak{p}\bar{\mathfrak{p}}$ splits in K.

Let $\widehat{\Psi} : \widehat{K} \hookrightarrow \widehat{B}_{N^-}$ be the adelic version of Ψ. We define $x_n : \widehat{K}^\times \to \widehat{B}_{N^-}^\times$ by $x_n(a) = \widehat{\Psi}(a) \cdot \varsigma^{(n)} := \widehat{\Psi}(a) \cdot \left(\varsigma_p^{(n)} \times \prod_{q \neq p} \varsigma_q\right)$. The collection $\left\{x_n(a) : a \in \widehat{K}^\times\right\}$ of points is called the **Gross points of conductor** p^n **on** $\widehat{B}_{N^-}^\times$. The fixed embedding $K \hookrightarrow B_{N^-}$ also induces an optimal embedding of $\mathcal{O}_n = \mathbb{Z} + p^n\mathcal{O}_K$ into the Eichler order $B_{N^-} \cap \varsigma^{(n)}\widehat{R}_{N^+}(\varsigma^{(n)})^{-1}$ where R_{N^+} is the Eichler order of level N^+ under the fixed isomorphism i.

2.2 Theta elements

Let $f(z) = \sum_{n \geq 1} a_n q^n \in S_2(\Gamma_0(N))$ be the cuspidal newform of weight two with rational Fourier coefficients corresponding to E via the modularity theorem [3]. Let $\phi_f : B_{N^-}^\times \backslash \widehat{B}_{N^-}^\times / \widehat{R}_{N^+}^\times \to \mathbb{C}$ be the Jacquet–Langlands transfer of f. Since $B_{N^-}^\times \backslash \widehat{B}_{N^-}^\times / \widehat{R}_{N^+}^\times$ is a finite set and f is a Hecke eigenform, we are able to and do normalize

$$\phi_f : B_{N^-}^\times \backslash \widehat{B}_{N^-}^\times / \widehat{R}_{N^+}^\times \to \mathbb{Z}_p,$$

such that the image of ϕ_f does not lie in $p\mathbb{Z}_p$. This integral normalization is related to the congruence ideals [9, 12, 16]. Let

$$\widetilde{\theta}_n(E/K) = \sum_{[a] \in \mathcal{G}_n} \phi_f(x_n(a)) \cdot [a] \in \mathbb{Z}_p[\mathcal{G}_n],$$

where $\mathcal{G}_n = K^\times \backslash \widehat{K}^\times / \widehat{\mathcal{O}}_n^\times$ and $[a]$ is the image of $a \in \widehat{K}^\times$ in $\mathcal{G}_n$. Then **Bertolini–Darmon's theta element** $\theta(E/K_n)$ **of** E **over** K_n is defined by the image of $\widetilde{\theta}_n(E/K)$ in Λ_n

$$\begin{aligned} \mathbb{Z}_p[\mathcal{G}_n] &\longrightarrow \Lambda_n = \mathbb{Z}_p[\mathrm{Gal}(K_n/K)] \\ \widetilde{\theta}_n(E/K) &\longmapsto \theta(E/K_n), \end{aligned}$$

where the map is naturally induced from the quotient map $\mathcal{G}_n \to \mathrm{Gal}(K_n/K)$. It is known that $\theta(E/K_n)$ interpolates "an half of" $L(E,\chi,1)$ where χ runs over characters on $\mathrm{Gal}(K_n/K)$. See [5, Remark (iii) after Theorem A] for the precise meaning of "an half of". Because $\theta(E/K_n)$ depends on the choice of Gross points, $\theta(E/K_n)$ is well-defined only up to multiplication by $\mathrm{Gal}(K_n/K)$.

2.3 *p*-adic *L*-functions

Let α, β be the roots of the Hecke polynomial $X^2 - a_pX + p$ of f at p. Since f is ordinary at p, one of them, say α, is a p-adic unit.

The **p-stabilization** $f_\alpha \in S_2(\Gamma_0(Np))$ **of** f is defined by

$$f_\alpha(z) = f(z) - \beta \cdot f(pz)$$

whose U_p-eigenvalue is α. Then the **theta element of f_α over K_n** is characterized by the following relation:

$$\theta(f_\alpha/K_n) = \frac{1}{\alpha^n} \cdot \left(\theta(E/K_n) - \frac{1}{\alpha} \cdot \nu_{n-1,n}(\theta(E/K_{n-1})) \right). \tag{2.1}$$

It is known that theta elements of E satisfies the three term relation (e.g., [6, Lemma 2.6])

$$\pi_{n+1,n}(\theta(E/K_{n+1})) = a_p \cdot \theta(E/K_n) - \nu_{n-1,n}(\theta(E/K_{n-1})) \tag{2.2}$$

and the theta elements of f_α satisfy the norm compatibility

$$\pi_{n+1,n}(\theta(f_\alpha/K_{n+1})) = \theta(f_\alpha/K_n). \tag{2.3}$$

Let ι be the involution on Λ_n defined by inverting group-like elements, so we have

$$\iota\Big(\sum_{\sigma\in\mathrm{Gal}(K_n/K)} a_\sigma \cdot \sigma\Big) = \sum_{\sigma\in\mathrm{Gal}(K_n/K)} a_\sigma \cdot \sigma^{-1}.$$

We define the **anticyclotomic p-adic L-function of E** by

$$L_p(E/K_\infty) = \varprojlim_n (\theta(f_\alpha/K_n) \cdot \iota(\theta(f_\alpha/K_n))) \in \Lambda = \varprojlim_n \Lambda_n.$$

This element is well-defined. The functional equation for Bertolini–Darmon's theta elements yields the equality of ideals of Λ (e.g., [1, Proposition 2.13], [2, Lemma 1.5])

$$(\theta(f_\alpha/K_n)) = (\iota(\theta(f_\alpha/K_n))). \tag{2.4}$$

We prove two useful lemmas.

Lemma 2.1 *We have an equality of ideals of Λ_n*

$$(\theta(E/K_n), \nu_{n-1,n}(\theta(E/K_{n-1}))) = (\nu_{m,n}(\theta(E/K_m)) : 0 \le m \le n).$$

https://doi.org/10.4153/S000843952510088X Published online by Cambridge University Press

Proof From the three term relation (2.2), we have

$$\nu_{n-1,n}\left(\pi_{n,n-1}\left(\theta(E/K_n)\right)\right) = a_p \cdot \nu_{n-1,n}\left(\theta(E/K_{n-1})\right) - \nu_{n-2,n}\left(\theta(E/K_{n-2})\right)$$

for $n \geq 2$. Since $\nu_{n-1,n}\left(\pi_{n,n-1}\left(\theta(E/K_n)\right)\right) = f_n \cdot \theta(E/K_n)$ for some $f_n \in \Lambda_n$, we have

$$\nu_{n-2,n}\left(\theta(E/K_{n-2})\right) \in \left(\theta(E/K_n), \nu_{n-1,n}\left(\theta(E/K_{n-1})\right)\right) \subseteq \Lambda_n.$$

In the same manner, we can obtain

$$\nu_{n-3,n-1}\left(\theta(E/K_{n-3})\right) \in \left(\theta(E/K_{n-1}), \nu_{n-2,n-1}\left(\theta(E/K_{n-2})\right)\right) \subseteq \Lambda_{n-1}.$$

By taking $\nu_{n-1,n}$, we have

$$\begin{aligned}\nu_{n-3,n}\left(\theta(E/K_{n-3})\right) &\in \left(\nu_{n-1,n}\left(\theta(E/K_{n-1})\right), \nu_{n-2,n}\left(\theta(E/K_{n-2})\right)\right)\\ &\subseteq \left(\theta(E/K_n), \nu_{n-1,n}\left(\theta(E/K_{n-1})\right)\right)\\ &\subseteq \Lambda_n.\end{aligned}$$

By applying this argument recursively, the conclusion follows. ■

Lemma 2.2 *Under (Spl) and (Na), we have an equality of ideals of* Λ_n

$$\left(\theta(E/K_n), \nu_{n-1,n}\left(\theta(E/K_{n-1})\right)\right) = \left(\theta(f_\alpha/K_n)\right).$$

Proof By the definition of the p-stabilization (2.1), we have one inclusion $\supseteq$. Hence, we focus on the opposite inclusion. By the interpolation formula of the anticyclotomic p-adic L-functions [5, Theorem A] under (Spl), we have the comparison of (the square-roots of) L-values

$$\theta(f_\alpha/K) = \left(1 - \frac{1}{\alpha}\right) \cdot \theta(E/K).$$

Under (Na), we have equality in $\mathbb{Z}_p$

$$\left(1 - \frac{1}{\alpha}\right)^{-1} \cdot \theta(f_\alpha/K) = \theta(E/K),$$

so we have $(\theta(E/K)) \subseteq (\theta(f_\alpha/K))$. In fact, they are the same ideal. From (2.1) and (2.3), we have

$$\begin{aligned}\theta(f_\alpha/K_1) &= \frac{1}{\alpha} \cdot \left(\theta(E/K_1) - \frac{1}{\alpha} \cdot \nu_{0,1}(\theta(E/K))\right)\\ &= \frac{1}{\alpha} \cdot \left(\theta(E/K_1) - \frac{1}{\alpha} \cdot \nu_{0,1}(\left(1 - \frac{1}{\alpha}\right)^{-1} \cdot \theta(f_\alpha/K))\right)\\ &= \frac{1}{\alpha} \cdot \left(\theta(E/K_1) - \frac{1}{\alpha} \cdot \left(1 - \frac{1}{\alpha}\right)^{-1} \cdot \nu_{0,1}(\pi_{1,0}(\theta(f_\alpha/K_1)))\right)\\ &= \frac{1}{\alpha} \cdot \left(\theta(E/K_1) - \frac{1}{\alpha} \cdot \left(1 - \frac{1}{\alpha}\right)^{-1} \cdot f_1 \cdot \theta(f_\alpha/K_1)\right)\end{aligned}$$

for some $f_1 \in \Lambda_1$. This shows that $\theta(E/K_1) = g_1 \cdot \theta(f_\alpha/K_1)$ for some $g_1 \in \Lambda_1$.

https://doi.org/10.4153/S000843952510088X Published online by Cambridge University Press

We suppose that $\theta(E/K_{n-1}) = g_{n-1} \cdot \theta(f_\alpha/K_{n-1})$ for some $g_{n-1} \in \Lambda_{n-1}$.

$$\begin{aligned}\theta(f_\alpha/K_n) &= \frac{1}{\alpha^n} \cdot \left(\theta(E/K_n) - \frac{1}{\alpha} \cdot \nu_{n-1,n}(\theta(E/K_{n-1}))\right) \\ &= \frac{1}{\alpha^n} \cdot \left(\theta(E/K_n) - \frac{1}{\alpha} \cdot \nu_{n-1,n}(g_{n-1} \cdot \theta(f_\alpha/K_{n-1}))\right) \\ &= \frac{1}{\alpha^n} \cdot \left(\theta(E/K_n) - \frac{1}{\alpha} \cdot g_{n-1} \cdot \nu_{n-1,n}(\pi_{n,n-1}(\theta(f_\alpha/K_n)))\right) \\ &= \frac{1}{\alpha^n} \cdot \left(\theta(E/K_1) - \frac{1}{\alpha} \cdot g_{n-1} \cdot f_n \cdot \theta(f_\alpha/K_n)\right)\end{aligned}$$

for some $f_n \in \Lambda_n$. This shows that $\theta(E/K_n) = g_n \cdot \theta(f_\alpha/K_n)$ for some $g_n \in \Lambda_n$. By induction, we have inclusion

$$(\theta(E/K_n)) \subseteq (\theta(f_\alpha/K_n)),$$

so we also have

$$(\nu_{n-1,n}(\theta(E/K_{n-1}))) \subseteq (\nu_{n-1,n}(\theta(f_\alpha/K_{n-1}))).$$

Since $\nu_{n-1,n}(\theta(f_\alpha/K_{n-1})) = f_n \cdot \theta(f_\alpha/K_n)$, we have

$$(\nu_{n-1,n}(\theta(f_\alpha/K_{n-1}))) \subseteq (\theta(f_\alpha/K_n)).$$

The conclusion follows. ■

3 Comparison of Selmer groups

3.1 Local properties of Galois representations

Let $\rho : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Q}_p}(V) = \mathrm{GL}_2(\mathbb{Q}_p)$ be the two-dimensional Galois representation associated with E.

- Since E is good ordinary at p, we have

$$\rho|_{G_{\mathbb{Q}_p}} \sim \begin{pmatrix} \chi_\alpha^{-1} \cdot \chi_{\mathrm{cyc}} & * \\ 0 & \chi_\alpha \end{pmatrix}$$

  where χ_α is the unramified character sending the arithmetic Frobenius at p to α.
- For ℓ dividing N exactly, we also have

$$\rho|_{G_{\mathbb{Q}_\ell}} \sim \begin{pmatrix} \pm\chi_{\mathrm{cyc}} & * \\ 0 & \pm\mathbf{1} \end{pmatrix}.$$

For a rational prime v dividing N^-p, we consider the following subspaces:

- For $v = p$, let $F^+V \subseteq V$ be the subspace on which the inertia subgroup I_v acts by χ_{cyc}.
- For a rational prime v dividing N^-, $F^+V \subseteq V$ be the subspace on which the inertia subgroup I_v acts by χ_{cyc} or $\chi_{\mathrm{cyc}}\tau_v$ where τ_v is the non-trivial unramified quadratic character of $G_{\mathbb{Q}_v}$.

https://doi.org/10.4153/S000843952510088X Published online by Cambridge University Press

Let L be an algebraic extension of K. For a prime w of L dividing N^-p, we define the **ordinary local condition of** V **at** w by

$$\mathrm{H}^1_{\mathrm{ord}}(L_w, V) = \ker\left(\mathrm{H}^1(L_w, V) \to \mathrm{H}^1(L_w, V/F^+V)\right).$$

Denote by $T = \varprojlim_k E[p^k]$ the p-adic Tate module of E, so we have $T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = V$, and by $E[p^\infty] = \varinjlim_k E[p^k]$ the p-power torsion points of E. Then the same local conditions for T, T/p^kT, $E[p^\infty]$, and $E[p^k]$ are defined by propagation.

3.2 N^--ordinary (residual) Selmer groups

Let Σ be the finite set of places of $\mathbb{Q}$ consisting of the places dividing $Np\infty$, and K_Σ be the maximal extension of K unramified outside Σ. We write

- $\Sigma^+ \subseteq \Sigma$ to be the subset of Σ consisting of the places not dividing $p\infty$ which split in $K/\mathbb{Q}$, and
- $\Sigma^- \subseteq \Sigma$ to be the subset of Σ consisting of the places not dividing $p\infty$ which are inert in $K/\mathbb{Q}$.

For a place w of K_∞, we write $w \in \Sigma^\pm$ if w divides a rational prime ℓ contained in $\Sigma^\pm$, respectively. For every $k \geq 1$, we define the **N^--ordinary (and N^+-strict) Selmer group of $E[p^k]$** $\mathrm{Sel}_{N^-}(K_\infty, E[p^k])$ by the kernel of the map

$$\mathrm{H}^1(K_\Sigma/K_\infty, E[p^k]) \to \prod_{w \nmid \Sigma^+} \mathrm{H}^1(K_{\infty,w}, E[p^k]) \times \prod_{w \in \Sigma^- \text{ or } w|p} \frac{\mathrm{H}^1(K_{\infty,w}, E[p^k])}{\mathrm{H}^1_{\mathrm{ord}}(K_{\infty,w}, E[p^k])},$$

and define $\mathrm{Sel}_{N^-}(K_\infty, E[p^\infty]) = \varinjlim_k \mathrm{Sel}_{N^-}(K_\infty, E[p^k])$. This is *the* Selmer group used in the bipartite Euler system argument [2, Definition 2.8].

3.3 Minimal and Greenberg Selmer groups

We follow the convention of [16, Section 3.1]. The **minimal Selmer group** $\mathrm{Sel}_{\mathrm{min}}(K_\infty, E[p^\infty])$ **of** $E[p^\infty]$ is defined by the kernel of the map

$$\mathrm{H}^1(K_\infty, E[p^\infty]) \to \prod_{w \nmid p} \mathrm{H}^1(K_{\infty,w}, E[p^\infty]) \times \prod_{w|p} \frac{\mathrm{H}^1(K_{\infty,w}, E[p^\infty])}{\mathrm{H}^1_{\mathrm{ord}}(K_{\infty,w}, E[p^\infty])},$$

and the **Greenberg Selmer group** $\mathrm{Sel}_{\mathrm{Gr}}(K_\infty, E[p^\infty])$ **of** $E[p^\infty]$ is defined by the kernel of the map

$$\mathrm{H}^1(K_\infty, E[p^\infty]) \to \prod_{w \nmid p} \mathrm{H}^1(I_{\infty,w}, E[p^\infty]) \times \prod_{w|p} \frac{\mathrm{H}^1(K_{\infty,w}, E[p^\infty])}{\mathrm{H}^1_{\mathrm{ord}}(K_{\infty,w}, E[p^\infty])},$$

where $I_{\infty,w}$ is the inertia subgroup of $G_{K_{\infty,w}}$. Under (Ram), $\overline{\rho}$ is ramified at every prime dividing N, so p does not divide any Tamagawa factors. Then by using [16, Lemma 3.4], we have an isomorphism

$$\mathrm{Sel}_{\min}(K_\infty, E[p^\infty]) \simeq \mathrm{Sel}_{\mathrm{Gr}}(K_\infty, E[p^\infty]). \tag{3.1}$$

3.4 The comparison

We recall the final displayed equation in the proof of [16, Proposition 3.6]:

$$0 \longrightarrow \mathrm{Sel}_{N^-}(K_\infty, E[p^k]) \longrightarrow \mathrm{Sel}_{\min}(K_\infty, E[p^\infty])[p^k] \longrightarrow \prod_w \frac{(E[p^\infty])^{G_{K_{\infty,w}}}}{p^k (E[p^\infty])^{G_{K_{\infty,w}}}}$$

where w runs over the primes of K_∞ dividing N^+. The local conditions at primes dividing N^- of minimal Selmer groups and N^--ordinary Selmer groups coincide since such primes split completely in K_∞/K. Thus, we have inclusion

$$\mathrm{Sel}_{N^-}(K_\infty, E[p^k]) \subseteq \mathrm{Sel}_{\min}(K_\infty, E[p^\infty])[p^k]$$

which is of finite index and is independent of k.

Proposition 3.1 *If* $\mathrm{Sel}_{N^-}(K_\infty, E[p^\infty])$ *is* Λ*-cotorsion with vanishing of* μ*-invariant, then* $\mathrm{Sel}_{\min}(K_\infty, E[p^\infty])$ *is also* Λ*-cotorsion with vanishing of* μ*-invariant.*

Proof We have $\mathrm{Sel}_{N^-}(K_\infty, E[p^\infty])[p] = \mathrm{Sel}_{N^-}(K_\infty, E[p])$ since N^--ordinary Selmer groups of $E[p^\infty]$ are defined as the injective limit of N^--ordinary Selmer groups of $E[p^k]$. By the assumption, $\mathrm{Sel}_{N^-}(K_\infty, E[p])$ is finite as noted in the proof of [13, Corollary 2.3]. Since the inclusion $\mathrm{Sel}_{N^-}(K_\infty, E[p]) \subseteq \mathrm{Sel}_{\min}(K_\infty, E[p^\infty])[p]$ is of finite index, $\mathrm{Sel}_{\min}(K_\infty, E[p^\infty])[p]$ is also finite. By the same reasoning, the conclusion follows. ■

Proposition 3.2 *Under (Im), if* $\mathrm{Sel}_{\min}(K_\infty, E[p^\infty])$ *is* Λ*-cotorsion, then* $\mathrm{Sel}_{\min}(K_\infty, E[p^\infty])$ *has no proper* Λ*-submodule of finite index. Thus, we have*

$$\mathrm{char}_\Lambda \mathrm{Sel}_{\min}(K_\infty, E[p^\infty]) = \mathrm{Fitt}_\Lambda \mathrm{Sel}_{\min}(K_\infty, E[p^\infty]),$$
$$\mathrm{Sel}_{\min}(K_\infty, E[p^\infty]) \simeq \mathrm{Sel}_{N^-}(K_\infty, E[p^\infty]).$$

Proof This follows from [7, Proposition 4.14], which covers the cyclotomic case actually, but the argument generalizes to our setting as mentioned in the proof of [16, Proposition 3.6]. ■

The following corollary follows from (3.1) and the above two propositions.

Corollary 3.3 *Under (Im) and (Ram), if* $\mathrm{Sel}_{N^-}(K_\infty, E[p^\infty])$ *is* Λ*-cotorsion with vanishing of* μ*-invariant, we have isomorphisms*

$$\mathrm{Sel}_{N^-}(K_\infty, E[p^\infty]) \simeq \mathrm{Sel}_{\min}(K_\infty, E[p^\infty]) \simeq \mathrm{Sel}_{\mathrm{Gr}}(K_\infty, E[p^\infty]).$$

4 The proof of the main theorem via Iwasawa theory

We first gather some tools from Iwasawa theory and give a proof of Theorem 1.1.

4.1 Iwasawa theory

The anticyclotomic main conjecture for (E, p, K) is now completely known for our setting.

Theorem 4.1 *Under (Im),(Ram),(Spl),(Na), and (Def), we have the following statements.*

(1) $L_p(E/K_\infty)$ *is non-zero.*
(2) $\mu(L_p(E/K_\infty)) = 0$.
(3) $\mathrm{Sel}_{N^-}(K_\infty, E[p^\infty])$ *is* Λ*-cotorsion with vanishing of* μ*-invariants.*
(4) $\big(L_p(E/K_\infty)\big) = \mathrm{char}_\Lambda\left(\mathrm{Sel}(K_\infty, E[p^\infty])^\vee\right)$.

Proof

(1) It is proved in [18].
(2) It is proved in [19].
(3) This follows from (1), (2), and the Euler system divisibility

$$\big(L_p(E/K_\infty)\big) \subseteq \mathrm{char}_\Lambda\left(\mathrm{Sel}_{N^-}(K_\infty, E[p^\infty])^\vee\right)$$

obtained from the bipartite Euler system argument [2, 16]. Condition (Na) is implicitly used in the Euler system argument. See [13, Assumption 1.1 and Remark 1.4] for this issue.
(4) By using (3) and Corollary 3.3, we can identify $\mathrm{Sel}_{N^-}(K_\infty, E[p^\infty])$ with the minimal Selmer group. By [7, Proposition 2.1], the minimal Selmer group also coincides with the classical Selmer group. The opposite divisibility

$$\big(L_p(E/K_\infty)\big) \supseteq \mathrm{char}_\Lambda\left(\mathrm{Sel}(K_\infty, E[p^\infty])^\vee\right)$$

follows from [17]. Condition (Spl) is needed only for this last statement to invoke [17]. ■

Corollary 4.2 *Under (Im),(Ram),(Na), and (Def), the classical Selmer group* $\mathrm{Sel}(K_\infty, E[p^\infty])$ *has no proper* Λ*-submodule of finite index; thus,*

$$\mathrm{char}_\Lambda \mathrm{Sel}(K_\infty, E[p^\infty]) = \mathrm{Fitt}_\Lambda \mathrm{Sel}(K_\infty, E[p^\infty]).$$

Proof By Theorem 4.1.(3), $\mathrm{Sel}_{N^-}(K_\infty, E[p^\infty])$ is Λ-cotorsion. By Proposition 3.1, $\mathrm{Sel}_{\min}(K_\infty, E[p^\infty])$ is also Λ-cotorsion. The conclusion follows from Proposition 3.2 and the identification of the minimal Selmer group and the classical Selmer group. ■

We recall the control theorem.

Proposition 4.3 (Control theorem) *Let* $\omega_n = \omega_n(X) = (1+X)^{p^n} - 1 \in \mathbb{Z}_p[\![X]\!] \simeq \Lambda$. *Under (Im), (Na), and (Def), the restriction map*

$$\mathrm{Sel}(K_n, E[p^\infty]) \to \mathrm{Sel}(K_\infty, E[p^\infty])[\omega_n]$$

https://doi.org/10.4153/S000843952510088X Published online by Cambridge University Press

is injective with the finite cokernel whose size is bounded independently of n. If we further assume (Ram), then it is an isomorphism.

Proof See [4, Proposition 1.9] with the identifications of Selmer groups in Corollaries 3.3 and 4.2. ∎

4.2 The proof of Theorem 1.1

By the anticyclotomic main conjecture (Theorem 4.1), we have

$$\left(L_p(E/K_\infty)\right) = \mathrm{char}_\Lambda\left(\mathrm{Sel}(K_\infty, E[p^\infty])^\vee\right).$$

By Corollary 4.2, the above equality becomes

$$\left(L_p(E/K_\infty)\right) = \mathrm{Fitt}_\Lambda\left(\mathrm{Sel}(K_\infty, E[p^\infty])^\vee\right)$$

Under the quotient map $\Lambda \to \Lambda_n = \Lambda/\omega_n$, it becomes

$$\left(\left(\theta(f_\alpha/K_n)\cdot\iota(\theta(f_\alpha/K_n))\right)\right) = \mathrm{Fitt}_{\Lambda_n}\left(\left(\mathrm{Sel}(K_\infty, E[p^\infty])[\omega_n]\right)^\vee\right)$$

since Fitting ideals are compatible with base change. By using the functional equation of theta elements (2.4) and the control theorem (Proposition 4.3), we have

$$\left(\theta(f_\alpha/K_n)\right)^2 = \mathrm{Fitt}_{\Lambda_n}\left(\mathrm{Sel}(K_n, E[p^\infty])^\vee\right).$$

Theorem 1.1 now follows from Lemma 2.2, and the ideal is principal thanks to the above equality.

Acknowledgement I would like to thank Rob Pollack and Masato Kurihara very much. Rob Pollack first suggested me to think about this problem when I was a Ph.D. student and I was able to solve it after having the discussions with Masato Kurihara. In particular, I learned the idea of the proof of Lemma 2.2 on the p-destabilization process from the discussion with Masato Kurihara at his home, January 3, 2017. The main result of this article partially refines that of [8]. We are grateful to thank the referee for pointing out inaccuracies and unrefined writings. The explanation is greatly improved in the revised version following the referee's suggestions.

Funding C.-H.K. was partially supported by research funds for newly appointed professors of Jeonbuk National University in 2024, and by Global-Learning & Academic research institution for Master's Ph.D. Students, and Postdocs (LAMP) Program of the National Research Foundation of Korea (NRF) funded by the Ministry of Education (Grant No. RS-2024-00443714).

References

[1] M. Bertolini and H. Darmon, *Heegner points on Mumford–Tate curves*. Invent. Math. **126**(1996), no. 3, 413–456.

[2] M. Bertolini and H. Darmon, *Iwasawa's main conjectures for elliptic curves over anticyclotomic $\mathbb{Z}_p$-extensions*. Ann. Math. (2) **162**(2005), no. 1, 1–64.

[3] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*. J. Amer. Math. Soc. **14**(2001), no. 4, 843–939.

https://doi.org/10.4153/S000843952510088X Published online by Cambridge University Press

[4] M. Chida and M.-L. Hsieh, *On the anticyclotomic Iwasawa main conjecture for modular forms*. Compos. Math. **151**(2015), no. 5, 863–897.
[5] M. Chida and M.-L. Hsieh, *Special values of anticyclotomic L-functions for modular forms*. J. Reine Angew. Math. **741**(2018), 87–131.
[6] H. Darmon and A. Iovita, *The anticyclotomic main conjecture for elliptic curves at supersingular primes*. J. Inst. Math. Jussieu **7**(2008), no. 2, 291–325.
[7] R. Greenberg, *Iwasawa theory for elliptic curves*. In: C. Viola (ed.), Arithmetic theory of elliptic curves (Cetraro, 1997), volume 1716 of Lecture Notes in Mathematics, Springer-Verlag, Berlin, 1999, pp. 51–144. Centro Internazionale Matematico Estivo (C.I.M.E.), Florence, Lectures from the 3rd C.I.M.E. Session held in Cetraro, July 12–19, 1997.
[8] C.-H. Kim, *An anticyclotomic Mazur–Tate conjecture for modular forms*. Preprint, unpublished, arXiv:1612.03743.
[9] C.-H. Kim, *Anticyclotomic Iwasawa invariants and congruences of modular forms*. Asian J. Math. **21**(2017), no. 3, 499–530.
[10] C.-H. Kim, *Overconvergent quaternionic forms and anticyclotomic p-adic L-functions*. Publ. Mat. **63**(2019), no. 2, 727–767.
[11] C.-H. Kim and M. Kurihara, *On the refined conjectures on Fitting ideals of Selmer groups of elliptic curves with supersingular reduction*. Int. Math. Res. Not. IMRN **2021**(2021), no. 14, 10559–10599.
[12] C.-H. Kim and K. Ota, *On the quantitative variation of congruence ideals and integral periods of modular forms*. Res. Math. Sci. **10**(2023), no. 22, 34.
[13] C.-H. Kim, R. Pollack, and T. Weston, *On the freeness of anticyclotomic Selmer groups of modular forms*. Int. J. Number Theory **13**(2017), no. 6, 1443–1455.
[14] M. Kurihara, *On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I*. Invent. Math. **149**(2002), 195–224.
[15] B. Mazur and J. Tate, *Refined conjectures of the "Birch and Swinnerton-Dyer type"*. Duke Math. J. **54**(1987), no. 2, 711–750.
[16] R. Pollack and T. Weston, *On anticyclotomic μ-invariants of modular forms*. Compos. Math. **147**(2011), 1353–1381.
[17] C. Skinner and E. Urban, *The Iwasawa main conjectures for GL_2*. Invent. Math. **195**(2014), no. 1, 1–277.
[18] V. Vatsal, *Uniform distribution of Heegner points*. Invent. Math. **148**(2002), no. 1, 1–48.
[19] V. Vatsal, *Special values of anticyclotomic L-functions*. Duke Math. J. **116**(2003), no. 2, 219–261.
[20] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, volume 800 of Lecture Notes in Mathematics, Springer, Berlin, 1980.

Department of Mathematics and Institute of Pure and Applied Mathematics, Jeonbuk National University, 567 Baekje-daero, Deokjin-gu, Jeonju, Jeollabuk-do 54896, Republic of Korea
e-mail: chanho.math@gmail.com