ON THE IWASAWA THEORY OF ELLIPTIC CURVES AT EISENSTEIN PRIMES

FRANCESC CASTELLA

Abstract. These are expanded notes for the mini-course given by the author at the 2022 ICTS workshop 'Elliptic curves and the special values of L-functions'.

Contents

Introduction

Let $E/\mathbb{Q}$ be an elliptic curve and let $L(E,s)$ be its Hasse–Weil L-series. The latter is defined by an Euler product absolutely convergent for complex s in the right-half plane $\mathrm{Re}(s) > 3/2$, but by modularity it can be analytically continued to all $s \in \mathbb{C}$.

By the Mordell–Weil theorem, the group of rational points $E(\mathbb{Q})$ is finitely generated, so

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{\mathrm{tors}},$$

for some $r = \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}) \geq 0$. The Birch–Swinnerton-Dyer conjecture (BSD) is the statement that

$$\mathrm{ord}_{s=1} L(E,s) \stackrel{?}{=} \mathrm{rank}_{\mathbb{Z}} E(\mathbb{Q}).$$

After the groundbreaking works of Coates–Wiles, Rubin, Gross–Zagier, and Kolyvagin in the 1970s and 1980s, the conjecture is known when either $L(E,1) \neq 0$ or $L'(E,1) \neq 0$. In these cases, their results also establish *finiteness* of the Tate–Shafarevich group

$$Ш(E/\mathbb{Q}) := \ker\left\{ \mathrm{H}^1(\mathbb{Q}, E) \to \prod_v \mathrm{H}^1(\mathbb{Q}_v, E) \right\},$$

a statement that is also widely believed to hold in general.

More recently, further progress on the BSD conjecture, and on its refined form predicting an exact formula for the leading Taylor coefficient of $L(E,s)$ around $s = 1$ in terms of arithmetic invariants of E, has been obtained largely through the use of p-adic methods; more specifically,

Date: March 26, 2024.

through various incarnations of Iwasawa theory. More specifically, a large body of work has gone into the proof of the following three implications, which are expected to hold for any prime number p:

(1) *p-part of the BSD formula in analytic rank 0*:

$$L(E,1)\neq 0 \quad\Longrightarrow\quad \mathrm{ord}_p\left(\frac{L(E,1)}{\Omega_E}\right)=\mathrm{ord}_p\left(\frac{\#Ш(E/\mathbb{Q})\cdot \mathrm{Tam}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2}\right),$$

where Ω_E is the positive Néron period of E, and $\mathrm{Tam}(E/\mathbb{Q})=\prod_{\ell|N}c_\ell(E/\mathbb{Q})$ is the product of the Tamagawa factors of $E/\mathbb{Q}$.

(2) *p-converse to the theorem of Gross–Zagier and Kolyvagin*:

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})=1 \quad\Longrightarrow\quad \mathrm{ord}_{s=1}L(E,s)=1,$$

where $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is the p^∞-Selmer group fitting into the descent exact sequence

$$0\to E(\mathbb{Q})\otimes\mathbb{Q}_p/\mathbb{Z}_p\to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q})\to Ш(E/\mathbb{Q})[p^\infty]\to 0.$$

(3) *p-part of the BSD formula in analytic rank 1*:

$$\mathrm{ord}_{s=1}L(E,s)=1 \quad\Longrightarrow\quad \mathrm{ord}_p\left(\frac{L'(E,1)}{\Omega_E\cdot \mathrm{Reg}_E}\right)=\mathrm{ord}_p\left(\frac{\#Ш(E/\mathbb{Q})\cdot \mathrm{Tam}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2}\right),$$

where Reg_E is the regulator of the Néron–Tate canonical height pairing on $E(\mathbb{Q})\otimes\mathbb{R}$.

The goal of these lectures is to explain the proof of (1)–(3) for good ordinary primes, with a special emphasis in the case of (the most recently established) *Eisenstein primes* p, i.e. primes p for which E admits a rational p-isogeny, or equivalently, such that $E[p]$ is reducible as a $G_{\mathbb{Q}}$-module.

Acknowledgements. It is a pleasure to heartily thank the organizers of the 2022 ICTS workshop 'Elliptic curves and the special values of L-functions, Ashay Burungale, Haruzo Hida, Somnath Jha, and Ye Tian, for their invitation to deliver these lectures, and the opportunity to contribute to these proceedings.

1. Lecture 1: Main conjectures and applications

The purpose of this lecture is to explain how, for any *good ordinary prime* (either Eisenstein or not) the implications (1), (2), and (3) from the Introduction follow from certain (three different, but not completely unrelated) "main conjectures" in Iwasawa theory.

1.1. Mazur's main conjecture.

Let $p>2$ be a good ordinary prime for E. Let $\mathbb{Q}(\mu_{p^\infty})$ be the field obtained by adjoining to $\mathbb{Q}$ of p-power roots of unity; then

$$\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})=\Delta\times\Gamma$$

with $\Delta\simeq\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ a cyclic group of order $p-1$, and $\Gamma\simeq\mathbb{Z}_p$. Let $\mathbb{Q}_\infty/\mathbb{Q}$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$, defined as the fixed of $\mathbb{Q}(\mu_{p^\infty})$ by Δ.

For every $n\geq 0$, denote by $\mathbb{Q}_n$ the unique subfield of $\mathbb{Q}_\infty$ with $[\mathbb{Q}_n:\mathbb{Q}]=p^n$. Let $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n)$ be the usual p^∞-Selmer group, defined as

$$\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n)=\ker\left\{\mathrm{H}^1(\mathbb{Q}_n,E[p^\infty])\to\prod_v \mathrm{H}^1(\mathbb{Q}_v,E)\right\},$$

where v runs over all primes of $\mathbb{Q}$, and put $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)=\varinjlim_n \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n)$.

The following is a special case of Mazur's control theorem (which applies to abelian varieties defined over a number field F more generally, and arbitrary $\mathbb{Z}_p$-extensions F_∞/F).

Theorem 1.1 (Mazur)**.** *The restriction maps*

$$\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n)\to\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)^{\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}_n)}$$

have finite kernel and cokernel, of order bounded as $n\to\infty$.

The original proof of Theorem 1.1 can be found in [Maz72]; an alternative and highly influential proof of the same result is given (for elliptic curves) in [Gre99].

Let $\Lambda = \mathbb{Z}_p[[\Gamma]]$ be the cyclotomic Iwasawa algebra. It follows easily from Theorem 1.1 together with the weak Mordell–Weil theorem, that $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty)$ is cofinitely generated over Λ, i.e. the Pontryagin dual

$$X(E/\mathbb{Q}_\infty) := \mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_\infty), \mathbb{Q}_p/\mathbb{Z}_p)$$

is finitely generated over Λ. Mazur further conjectured that $X(E/\mathbb{Q}_\infty)$ is Λ-torsion (see Conjecture 1.2 below), a condition that can be easily verified (using a topological version of Nakayama's lemma) when the classical Selmer group $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is finite (so in particular, $E(\mathbb{Q})$ is finite), but which lies much deeper in general.

On the analytic side, using modular symbols (assuming E is parametrized by modular functions) Mazur and Swinnerton-Dyer [MSD74] attached to E a p-adic L-function $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q}) \in \Lambda \otimes \mathbb{Q}_p$ characterized by the property that for every finite order character $\chi : \Gamma \to \mu_{p^\infty}$:

$$\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})(\chi) = \begin{cases} (1-\alpha_p^{-1})^2 \cdot \frac{L(E,1)}{\Omega_E} & \text{if } \chi = 1, \\ \frac{p^n}{\tau(\overline{\chi})\alpha_p^n} \cdot \frac{L(E,\overline{\chi},1)}{\Omega_E} & \text{if } \mathrm{cond}(\chi) = p^n > 1, \end{cases} \tag{1}$$

where α_p is the p-adic unit root of $x^2 - a_p(E)x + p$ and $\tau(\overline{\chi})$ is the Gauss sum.

Motivated by Iwasawa's main conjecture for class groups of number fields, Mazur formulated the following (see [MSD74, §9.5, Conj. 3]). Note that implicit in the conjecture is the statement that $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})$ is integral, i.e. lies in Λ.

Conjecture 1.2 (Mazur's main conjecture)**.** *$X(E/\mathbb{Q}_\infty)$ is Λ-torsion, with*

$$\mathrm{char}_\Lambda(X(E/\mathbb{Q}_\infty)) = \big(\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})\big).$$

As usual, we identify the Iwasawa algebra Λ with the one-variable power series ring $\mathbb{Z}_p[[T]]$ upon the choice of a topological generator $\gamma \in \Gamma$ by setting $T = \gamma - 1$. Under this identification, the evaluation of an element $\mathcal{L} \in \Lambda$ at a character $\chi : \Gamma \to \mathbb{C}_p^\times$ corresponds to the specialization of the power series expression of $\mathcal{L}$ at $T = \chi(\gamma) - 1$. In particular, evaluation at $\chi = 1$ corresponds to specialization at $T = 0$.

Henceforth we shall use $a \sim_p b$ to denote the equality $a = ub$ with $u \in \mathbb{Z}_p$.

Proposition 1.3. *Assume Conjecture 1.2. Then the p-part of the BSD formula holds in analytic rank 0, i.e.*

$$L(E,1) \neq 0 \quad \Longrightarrow \quad \mathrm{ord}_p\left(\frac{L(E,1)}{\Omega_E}\right) = \mathrm{ord}_p\left(\frac{\#Ш(E/\mathbb{Q}) \cdot \mathrm{Tam}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2}\right).$$

Proof. Suppose $L(E,1) \neq 0$. Then $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})(0) \neq 0$ by the interpolation property. By Mazur's main conjecture, it follows that the Γ-coinvariants $X(E/\mathbb{Q}_\infty)_\Gamma$ are finite, and so $\#\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) < \infty$ by Pontryagin duality and Mazur's control theorem. In particular, $\#\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) = \#Ш(E/\mathbb{Q})[p^\infty]$.

Let $\mathcal{F}(E/\mathbb{Q}_\infty) \in \Lambda$ be a characteristic power series of $X(E/\mathbb{Q}_\infty)$, i.e. a generator of the principal ideal $\mathrm{char}_\Lambda(X(E/\mathbb{Q}_\infty))$. Then by the work of Schneider [Sch85] and Perrin-Riou [PR92] one has

$$\mathcal{F}(E/\mathbb{Q}_\infty)(0) \sim_p (1-\alpha_p^{-1})^2 \cdot \#\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \cdot \frac{\mathrm{Tam}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2}. \tag{2}$$

Since by Conjecture 1.2 the left-hand side of (2) has the same p-adic valuation as $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})(0)$, the combination of (1) and (2) yields the result. □

1.2. **Perrin-Riou's main conjecture.** We keep the assumption that p is an odd prime of good ordinary reduction for E. Let $K/\mathbb{Q}$ be an imaginary quadratic field satisfying the following *Heegner hypothesis*:

(Heeg) every prime $\ell | N$ splits in K.

Let K_∞^-/K be the anticyclotomic $\mathbb{Z}_p$-extension, characterized as the unique $\mathbb{Z}_p$-extension of K that is Galois over $\mathbb{Q}$ with $\tau\sigma\tau = \sigma^{-1}$ for all $\sigma \in \mathrm{Gal}(K_\infty^-/K)$, where τ is the non-trivial automorphism of $K/\mathbb{Q}$. Let K_n^- be the unique subextension of K_∞^- with $[K_n^- : K] = p^n$.

Via a fixed modular parametrization

$$\varphi : X_0(N) \to E,$$

the Kummer images of Heegner points of p-power conductor yield classes

$$x_n \in \mathrm{Sel}(K_n^-, T_pE) := \varprojlim_m \mathrm{Sel}_{p^m}(E/K_n^-),$$

where T_pE is the p-adic Tate module of E. Using the ordinary hypotheses on p, these classes can be made compatible under the corestriction maps $\mathrm{Sel}(K_{n+1}^-, T_pE) \to \mathrm{Sel}(K_n^-, T_pE)$, hence yielding an element

$$\kappa_\infty^{\mathrm{Hg}} \in \check{S}(E/K_\infty^-) := \varprojlim_n \mathrm{Sel}(K_n^-, T_pE).$$

Denote by $X(E/K_\infty^-)$ the Pontryagin dual of $\mathrm{Sel}_{p^\infty}(E/K_\infty^-)$; this is a finitely generated module over the anticyclotomic Iwasawa algebra $\Lambda^- = \mathbb{Z}_p[[\Gamma^-]]$, where we put $\Gamma^- = \mathrm{Gal}(K_\infty^-)/K)$.

Conjecture 1.4 (Perrin-Riou's main conjecture)**.** *$X(E/K_\infty^-)$ has Λ^--rank 1, with*

$$\mathrm{char}_{\Lambda^-}(X(E/K_\infty^-)_{\mathrm{tors}}) = \mathrm{char}_{\Lambda^-}\left(\frac{\check{S}(E/K_\infty^-)}{\Lambda^- \cdot \kappa_\infty^{\mathrm{Hg}}}\right)^2 \cdot \frac{1}{u_K^2 c^2},$$

where the subscript tors *denotes the maximal Λ^--torsion submodule, $u_K := \frac{1}{2}\#(\mathcal{O}_K^\times)$, and $c \in \mathbb{Q}^\times$ is the Manin constant*[1] *attached to φ.*

Proposition 1.5. *Assume Conjecture 1.4. Then*

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) = 1 \quad \Longrightarrow \quad \mathrm{ord}_{s=1}L(E,s) = 1,$$

i.e. the p-converse to the theorem of Gross–Zagier and Kolyvagin holds.

Proof. Suppose $\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) = 1$, and choose an imaginary quadratic field K such that:

(i) Hypothesis (Heeg) holds;
(ii) $L(E^K, 1) \neq 0$,

where $E^K/\mathbb{Q}$ is the twist of E by the quadratic character corresponding to K. By Kato's work [Kat04], condition (ii) implies that $\#\mathrm{Sel}_{p^\infty}(E^K/\mathbb{Q}) < \infty$, and so

$$\mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E/K) = \mathrm{corank}_{\mathbb{Z}_p}\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) = 1.$$

By a variant of Theorem 1.1 for the extension K_∞^-/K, it follows that the $\mathrm{corank}_{\mathbb{Z}_p}(X(E/K_\infty^-)_{\Gamma^-}) = 1$. By Conjecture 1.4, this implies that

$$(\gamma - 1) \nmid \mathrm{char}_{\Lambda^-}\left(\frac{\check{S}(E/K_\infty^-)}{\Lambda^- \cdot \kappa_\infty^{\mathrm{Hg}}}\right),$$

where $\gamma \in \Gamma^-$ is any topological generator (otherwise one would get $\mathrm{corank}_{\mathbb{Z}_p}(X(E/K_\infty^-)_{\Gamma^-}) \geq 3$), and so $\kappa_\infty^{\mathrm{Hg}}$ has non-torsion image κ_0^{Hg} under the natural map

$$\check{S}(E/K_\infty^-) \twoheadrightarrow \check{S}(E/K_\infty^-)_{\Gamma^-} \hookrightarrow \mathrm{Sel}(K, T_pE).$$

But by construction κ_0^{Hg} is the Kummer image of the classical Heegner point $y_K \in E(K)$ in the Gross–Zagier formula [GZ86], and therefore $L'(E/K, 1) \neq 0$. Finally, the factorization $L(E/K, s) = L(E, s)L(E^K, s)$ together with condition (ii) implies that $\mathrm{ord}_{s=1}L(E, s) = 1$, as desired. □

Remark 1.6. The first general p-converse to the theorem of Gross–Zagier and Kolyvagin for good ordinary primes p is due to Skinner [Ski20] and independently W. Zhang [Zha14]. The above proof of Proposition 1.5 is closely related to the approach in [Ski20] and is essentially contained in the work of X. Wan [Wan21a], which by using the Iwasawa theory of Heegner points (and their ensuing Λ^--extension of the BDP formula) allows one to dispense with the assumption that $\#Ш(E/\mathbb{Q})[p^\infty]$ forced upon in the original approach.

[1] Thus $\varphi^*\omega_E = c \cdot 2\pi i f(z)dz$ for the Néron differential ω_E and the newform f attached to E.

1.3. **BDP main conjecture.** In this section we assume that, in addition to (Heeg), the imaginary quadratic field K satisfies the condition that

$$(p) = v\overline{v} \text{ splits in } K, \tag{spl}$$

with v the prime of K above p induced by our fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$. On the other hand, the condition that p is a prime of good ordinary reduction for E is *not* necessary here.

Put $\Lambda^{\mathrm{ur}} := \Lambda^- \hat{\otimes}_{\mathbb{Z}_p} \mathbb{Z}_p^{\mathrm{ur}}$, where $\mathbb{Z}_p^{\mathrm{ur}}$ is the completion of the ring of integers of the maximal unramified extension of $\mathbb{Q}_p$. By the work of Bertolini–Darmon–Prasanna [BDP13] and its Λ^--adic extension in [Bra11, CH18], there is a p-adic L-function $\mathcal{L}_v^{\mathrm{BDP}}(f/K) \in \Lambda^{\mathrm{ur}}$ characterized by the property that for every character $\chi : \Gamma^- \to \mathbb{C}_p^\times$ crystalline at both v and $\overline{v}$ of weights $(n, -n)$ with $n > 0$ we have

$$\mathcal{L}_v^{\mathrm{BDP}}(f/K)^2(\chi) = C(f/K, \chi) \cdot L^{\mathrm{alg}}(f/K, \chi, 1),$$

where $C(f/K, \chi)$ is a nonzero term depending on f/K and χ, and $L^{\mathrm{alg}}(f/K, \chi, 1)$ is the "algebraic part" of the central Rankin–Selberg L-value $L(f/K, \chi, 1)$.

On the algebraic side, define the *BDP Selmer group* by

$$\mathrm{Sel}_v^{\mathrm{BDP}}(E/K_\infty^-) := \ker\left\{ \mathrm{H}^1(K_\infty^-, E[p^\infty]) \to \prod_{w \nmid v} \mathrm{H}^1(K_{\infty,w}^-, E[p^\infty]) \right\}.$$

In particular, classes in $\mathrm{Sel}_v^{\mathrm{BDP}}(E/K_\infty^-)$ are trivial at the primes above $\overline{v}$. Denote by $X_v^{\mathrm{BDP}}(E/K_\infty^-)$ the Pontryagin dual of $\mathrm{Sel}_v^{\mathrm{BDP}}(E/K_\infty^-)$.

The following can be viewed as a special case of Greenberg's Iwasawa main conjectures [Gre94] for p-adic deformations of motives.

Conjecture 1.7 (BDP main conjecture)**.** *$X_v^{\mathrm{BDP}}(E/K_\infty^-)$ is Λ^--torsion, with*

$$\mathrm{char}_{\Lambda^-}(X_v^{\mathrm{BDP}}(E/K_\infty^-)) = \left(\mathcal{L}_v^{\mathrm{BDP}}(f/K)^2\right)$$

as ideals in Λ^{ur}.

Proposition 1.8. *Suppose the p-part of the BSD formula holds in analytic rank 0. Then Conjecture 1.7 implies the p-part of the BSD formula in analytic rank 1, i.e.*

$$\mathrm{ord}_{s=1} L(E, s) = 1 \quad \Longrightarrow \quad \mathrm{ord}_p\left(\frac{L'(E,1)}{\Omega_E \cdot \mathrm{Reg}_E}\right) = \mathrm{ord}_p\left(\frac{\#Ш(E/\mathbb{Q}) \cdot \mathrm{Tam}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\mathrm{tors}})^2}\right).$$

Proof. Suppose $\mathrm{ord}_{s=1} L(E, s) = 1$, and choose an imaginary quadratic field K such that:

(i) Hypotheses (Heeg) and (spl) hold;
(ii) $L(E^K, 1) \neq 0$.

Then $\mathrm{ord}_{s=1} L(E/K, s) = 1$, which by the work of Gross–Zagier and Kolyvagin [Kol88] implies that the classical Heegner point $y_K \in E(K)$ is non-torsion, and we have

$$\mathrm{rank}_{\mathbb{Z}} E(K) = 1, \quad \#Ш(E/K) < \infty; \tag{3}$$

in particular, the index $[E(K) : \mathbb{Z}y_K]$ is finite. Let $\mathcal{F}_v^{\mathrm{BDP}}(E/K_\infty^-) \in \Lambda^-$ be a characteristic power series for $X_v^{\mathrm{BDP}}(E/K_\infty^-)$. Then by the work of Jetchev–Skinner–Wan [JSW17] we have the equality up to a p-adic unit

$$\mathcal{F}_v^{\mathrm{BDP}}(E/K_\infty^-)(0) \sim_p \left(\frac{1 - a_p(E) + p}{p}\right)^2 \cdot \prod_{w|N} c_w(E/K) \cdot \#Ш(E/K) \cdot \frac{\log_{\omega_E}(y_K)^2}{[E(K) : \mathbb{Z}y_K]^2}, \tag{4}$$

where $a_p(E) = p + 1 - \#E(\mathbb{F}_p)$, $c_w(E/K)$ is the Tamagawa factor of E at w, and $\log_{\omega_E} : E(K_v) \to \mathbb{Q}_p$ is the formal group logarithm. On the other hand, the formula of Bertolini–Darmon–Prasanna [BDP13] yields

$$\mathcal{L}_p^{\mathrm{BDP}}(f/K)(0) \sim_p \frac{1}{u_K^2 c^2} \cdot \left(\frac{1 - a_p(E) + p}{p}\right)^2 \cdot \log_{\omega_E}(y_K)^2. \tag{5}$$

Since Conjecture 1.7 implies that $\mathcal{L}_v^{\mathrm{BDP}}(f/K)(0) \sim_p \mathcal{F}_v^{\mathrm{BDP}}(E/K_\infty^-)(0)$, combining (4) and (5) we arrive at

$$[E(K) : \mathbb{Z}y_K]^2 \sim_p \#Ш(E/K) \cdot \prod_{w|N} c_w(E/K) \cdot u_K^2 c^2.$$

By Gross–Zagier formula [GZ86], this last relation is *equivalent* to the p-part of the BSD formula when $\mathrm{ord}_{s=1} L(E/K) = 1$. Thus using from the factorization

$$L(E/K, s) = L(E, s)L(E^K, s)$$

and the assumption that the p-part of the BSD formula holds for $L(E^K, 1)$, the result follows. □

2. Lecture 2: BDP main conjecture at Eisenstein primes

2.1. **Main result.** Let $p \nmid 2N$ be a prime of good ordinary reduction for E. When the residual representation

$$\rho_{E,p} : G_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{F}_p}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$$

has "big image" (and satisfies some mild ramification hypotheses), Conjectures 1.4 and 1.7 are known by combining:

- Euler/Kolyvagin system methods using Heegner points ([MR04], [How04]);
- A vast generalization of Ribet's methods ([SU14], [Wan20, Wan21b]).

Now we put ourselves in the opposite case where $E[p]$ is *reducible* as a $G_{\mathbb{Q}}$-module, say

$$E[p]^{ss} \simeq \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi), \tag{6}$$

where $\phi, \psi : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$ are characters. Note that $\psi = \omega\phi^{-1}$ by the Weil pairing, where $\omega : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$ is the mod p cyclotomic character. The goal of this lecture is to outline the proof of the following result from [CGLS22] (in the rank one case) and [CGS23].

Theorem 2.1. *Let K be an imaginary quadratic field of odd discriminant $-D_K \neq -3$, and satisfying hypotheses (Heeg) and (spl). Suppose $p > 2$ is a good Eisenstein prime for E with*

$$\phi|_{G_p} \neq 1, \omega,$$

where $G_p \subset G_{\mathbb{Q}}$ is a decomposition group at p. Then the BDP main conjecture (Conjecture 1.7) and Perrin-Riou's main conjecture (Conjecture 1.4) both hold.

Recall that Λ^- denotes the anticyclotomic Iwasawa algebra. From the structure theorem for finitely generated Λ^--modules and the Weierstrass preparation theorem, one has Iwasawa λ- and μ-invariants attached to $X_v^{\mathrm{BDP}}(E/K_\infty^-)$ and $\mathcal{L}_v^{\mathrm{BDP}}(E/K)$. An understanding of these invariants is a key in Theorem 2.1, whose proof is naturally divided into 2 steps:

- *Step 1*: Exploit the congruence (6) to show that
$$\mu(X_v^{\mathrm{BDP}}(E/K_\infty^-)) = \mu(\mathcal{L}_v^{\mathrm{BDP}}(E/K)) = 0,$$
$$\lambda(X_v^{\mathrm{BDP}}(E/K_\infty^-)) = \lambda(\mathcal{L}_v^{\mathrm{BDP}}(E/K)^2).$$
- *Step 2*: Show that $X_v^{\mathrm{BDP}}(E/K_\infty^-)$ is Λ^--torsion, with
$$\mathrm{char}_{\Lambda^-}(X_v^{\mathrm{BDP}}(E/K_\infty^-)) \supset \left(\mathcal{L}_v^{\mathrm{BDP}}(f/K)^2\right)$$
as ideals in $\Lambda^{\mathrm{ur}}[1/p]$.

Clearly the combination of these two imply the equality

$$\mathrm{char}_{\Lambda^-}(X_v^{\mathrm{BDP}}(E/K_\infty^-)) = \left(\mathcal{L}_v^{\mathrm{BDP}}(f/K)^2\right)$$

in Λ^{ur} predicted by Conjecture 1.7. That they also imply Conjecture 1.4 follows from the *equivalence* between the two conjectures, a consequence of the Λ^--adic analogue of the BDP formula [BDP13] obtained in [CH18].

Remark 2.2. In a recent work [KY24], T. Keller and M. Yin have removed the hypothesis on ϕ in Theorem 2.1. They have also extended the result to higher weight modular forms, and (using Hida theory in the style of Skinner [Ski16]) even to the case of multiplicative Eisenstein primes.

In the next two subsections we outline the main ideas that go into the proofs of the above *Step 1* and *Step 2*, respectively.

2.2. **Anticyclotomic Greenberg–Vatsal method.** Denote by S the set of primes of K dividing N, and by $\Sigma \supset S$ the set of primes of K dividing $Np\infty$. Let K^Σ be the Galois group of the maximal extension of K unramified outside Σ, and consider the *S-imprimitive* BDP Selmer group

$$\mathrm{Sel}^{\mathrm{BDP}}_{v,S}(E/K^-_\infty) := \ker\left\{ \mathrm{H}^1(K^\Sigma/K^-_\infty, E[p^\infty]) \to \prod_{w|\overline{v}} \mathrm{H}^1(K^-_{\infty,w}, E[p^\infty]) \right\}. \tag{7}$$

Let $X^{\mathrm{BDP}}_{v,S}(E/K^-_\infty)$ be the Pontryagin dual of $\mathrm{Sel}^{\mathrm{BDP}}_{v,S}(E/K^-_\infty)$. Multiplying $\mathcal{L}^{\mathrm{BDP}}_v(f/K)$ by certain elements in Λ^- interpolating the local Euler factors of $L(f/K,\chi,s)$ at $s=1$ at primes $v \in S$ over characters χ of Γ^-, one can define an S-imprimitive $\mathcal{L}^{\mathrm{BDP}}_{v,S}(f/K) \in \Lambda^{\mathrm{ur}}$ interpolating the central L-values of $L(f/K,\chi,s)$ at $s=1$ with the Euler factors at the primes in S stripped out.

The principle to be exploited is that Conjecture 1.7 should be equivalent to its S-imprimitive counterpart, so in particular

$$\mathrm{char}_{\Lambda^-}(X^{\mathrm{BDP}}_{v,S}(E/K_\infty)) \stackrel{?}{=} \big(\mathcal{L}^{\mathrm{BDP}}_{v,S}(f/K)^2\big),$$

with the latter having the advantage (first noticed by Greenberg in the context of classical Iwasawa theory [Gre77]) that the objects involved are better-behaved with respect to congruences.

Let $\Phi, \Psi : G_{\mathbb{Q}} \to \mathbb{Z}_p^\times$ be the Teichmüller lifts of ϕ, ψ, respectively. Attached to Φ, Ψ one has Λ^--cotorsion Selmer groups $\mathrm{Sel}_{v,S}(\Phi/K^-_\infty), \mathrm{Sel}_{v,S}(\Psi/K^-_\infty)$ (whose definition is recalled in the proof of Proposition 2.3 below) with associated Iwasawa λ-invariants denoted $\lambda^S_\phi, \lambda^S_\psi$, respectively.

Proposition 2.3. *Suppose $p \nmid 2N$ is such that $E[p]^{ss} \simeq \mathbb{F}(\phi) \oplus \mathbb{F}(\psi)$ as $G_{\mathbb{Q}}$-modules with $\phi|_{G_p} \neq 1, \omega$. Then $X^{\mathrm{BDP}}_{v,S}(E/K^-_\infty)$ is Λ^--torsion, with*

$$\mu(X^{\mathrm{BDP}}_{v,S}(E/K^-_\infty)) = 0, \qquad \lambda(X^{\mathrm{BDP}}_{v,S}(E/K^-_\infty)) = \lambda^S_\phi + \lambda^S_\psi.$$

Proof. Let K_ϕ is the fixed field of $\ker(\phi|_{G_K})$, and let M_∞ be the maximal abelian pro-p extension of $K^-_\infty K_\phi$ unramfied outside v and S. By standard arguments, the Selmer group

$$\begin{aligned} \mathrm{Sel}_{v,S}(\Phi/K^-_\infty) &:= \ker\left\{ \mathrm{H}^1(K^\Sigma/K^-_\infty, \mathbb{Q}_p/\mathbb{Z}_p(\Phi)) \to \prod_{w|\overline{v}} \mathrm{H}^1(K^-_{\infty,w}, \mathbb{Q}_p/\mathbb{Z}_p(\Phi)) \right\} \\ &\simeq \mathrm{Hom}_{\mathrm{cts}}(\mathrm{Gal}(M_\infty/K^-_\infty K_\phi), \mathbb{Q}_p/\mathbb{Z}_p) \end{aligned} \tag{8}$$

is Λ^--cotorsion and with no proper Λ^--submodules of finite index. On the other hand, by Hida's result on the vanishing of the μ-invariant of anticyclotomic Katz p-adic L-functions [Hid10] together with Rubin's proof of the Iwasawa main conjecture for K [Rub91], we have $\mu(\mathrm{Sel}_{v,S}(\Phi/K^-_\infty)^\vee) = 0$. Thus we see that $\mathrm{Sel}_{v,S}(\Phi/K^-_\infty)$ is p-divisible, and therefore the λ-invariant of its Pontryagin dual $\mathrm{Sel}_{v,S}(\Phi/K^-_\infty)^\vee$ is given by

$$\lambda^S_\phi = \dim_{\mathbb{F}_p}\big(\mathrm{Sel}_{v,S}(\Phi/K^-_\infty)[p]\big). \tag{9}$$

From our conditions on ϕ, it is easy to see that the natural map

$$\mathrm{H}^1(K^-_\infty, \mathbb{Q}_p/\mathbb{Z}_p(\phi)) \to \mathrm{H}^1(K^-_\infty, \mathbb{Q}_p/\mathbb{Z}_p(\Phi))[p]$$

gives $\mathrm{Sel}_{v,S}(\phi/K^-_\infty) \simeq \mathrm{Sel}_{v,S}(\Phi/K^-_\infty)[p]$, where $\mathrm{Sel}_{v,S}(\phi/K^-_\infty)$ is the *residual Selmer group* defined as in (8) with $\mathbb{F}_p(\phi)$ in place of $\mathbb{Q}_p/\mathbb{Z}_p(\Phi)$. Of course, the same results apply with $\psi = \omega\phi^{-1}$ in place of ϕ.

Letting $\mathrm{Sel}^{\mathrm{BDP}}_{v,S}(E[p]/K^-_\infty)$ be the Selmer group defined as in (7) with $E[p^\infty]$ replaced by $E[p]$, from the short exact sequence

$$0 \to \mathbb{F}_p(\phi) \to E[p] \to \mathbb{F}_p(\psi) \to 0 \tag{10}$$

we immediately arrive at the short exact sequence

$$0 \to \mathrm{Sel}_{v,S}(\phi/K^-_\infty) \to \mathrm{Sel}^{\mathrm{BDP}}_{v,S}(E[p]/K^-_\infty) \to \mathrm{Sel}_{v,S}(\psi/K^-_\infty) \to 0. \tag{11}$$

The above thus shows that $\mathrm{Sel}_{v,S}(E[p]/K_\infty^-) \simeq \mathrm{Sel}_{v,S}^{\mathrm{BDP}}(E/K_\infty^-)[p]$ is finite, and so $X_{v,S}^{\mathrm{BDP}}(E/K_\infty^-)$ is Λ^--torsion with $\mu = 0$. Since similarly as before the λ-invariant of $\mathrm{Sel}_{v,S}^{\mathrm{BDP}}(\Phi/K_\infty^-)^\vee$ can be computed as $\dim_{\mathbb{F}_p}(\mathrm{Sel}_{v,S}^{\mathrm{BDP}}(E/K_\infty^-)[p])$, the last claim in the proposition follows from (11) and (9). □

On the analytic side, (10) implies a congruence

$$f \equiv E_{\phi,\psi} \pmod{p}$$

between the newform f attached to E and a weight 2 Eisenstein series $E_{\phi,\psi}$ attached to the Dirichlet characters Φ, Ψ. From the constructions of $\mathcal{L}_{v,S}^{\mathrm{BDP}}(f/K)$ and of the Katz p-adic L-function for characters of K [Kat78, HT93], building on work of Kriz [Kri16] one then deduces a congruence

$$\mathcal{L}_{v,S}^{\mathrm{BDP}}(E/K)^2 \equiv \mathcal{L}_{v,S}^{\mathrm{Katz}}(\Phi) \cdot \mathcal{L}_{v,S}^{\mathrm{Katz}}(\Psi) \pmod{p\Lambda^{\mathrm{ur}}},$$

which together with the aforementioned vanishing result of Hida yields the equalities

$$\mu(\mathcal{L}_{v,S}^{\mathrm{BDP}}(E/K)) = 0, \qquad \lambda(\mathcal{L}_{v,S}^{\mathrm{BDP}}(E/K)^2) = \lambda(\mathcal{L}_{v,S}^{\mathrm{Katz}}(\Phi)) + \lambda(\mathcal{L}_{v,S}^{\mathrm{Katz}}(\Psi)).$$

By Rubin's proof of the Iwasawa main conjecture for K, these last two equalities and Proposition 2.3 yield the proof of *Step 1*.

2.3. **Kolyvagin system argument with "error terms".** As noted in §2.1, the proof of Theorem 2.1 exploits the following interplay between Conjectures 1.7 and Conjecture 1.4.

Proposition 2.4. *Suppose $E(K)[p] = 0$. Then the following are equivalent:*

(1) $X_v^{\mathrm{BDP}}(E/K_\infty^-)$ is Λ^--torsion, $\mathcal{L}_v^{\mathrm{BDP}}(f/K)$ is nonzero, and

$$\mathrm{char}_{\Lambda^-}(X_v^{\mathrm{BDP}}(E/K_\infty^-)) \supset \left(\mathcal{L}_v^{\mathrm{BDP}}(f/K)^2\right)$$

in $\Lambda^{\mathrm{ur}}[1/p]$.

(2) $X(E/K_\infty^-)$ has Λ^--rank one, $\kappa_\infty^{\mathrm{Hg}}$ is not Λ^--torsion, and

$$\mathrm{char}_{\Lambda^-}(X(E/K_\infty^-)_{\mathrm{tors}}) \supset \mathrm{char}_{\Lambda^-}\left(\frac{\check{S}(E/K_\infty^-)}{\Lambda^- \cdot \kappa_\infty^{\mathrm{Hg}}}\right)^2$$

in $\Lambda^-[1/p]$.

The same result holds for the opposite divisibilities, and without inverting p.

Sketch of proof. By p-ordinarity, there is a unique quotient $T_p^- E \simeq \mathbb{Z}_p$ of $T_p E$ where the G_p-action is unramified. From the two-variable extension (due to Loeffler–Zerbes [LZ14]) of the cyclotomic Perrin-Riou big logarithm map [PR94] one can deduce the existence of an injective generalized Coleman power series map with pseudo-null cokernel

$$\mathrm{Col}_v : \varprojlim_n \mathrm{H}^1(K_{n,v}^-, T_p^- E) \hookrightarrow \Lambda^{\mathrm{ur}},$$

which by virtue of a Λ^--adic extension of the BDP formula (see [CH18]) sends the natural image of $\mathrm{res}_v(\kappa_\infty^{\mathrm{Hg}})$ to $\mathcal{L}_v^{\mathrm{BDP}}(f/K)$. The result then follows from a double application (one involving res_v and another involving $\mathrm{res}_{\overline{v}}$) of Poitou–Tate duality. □

Since the fact that $\kappa_\infty^{\mathrm{Hg}}$ is not Λ^--torsion follows from the work of Cornut–Vatsal [Cor02, Vat03][2], the proof of *Step 2*, and hence of Theorem 2.1, is thus reduced to the following.

Proposition 2.5. *Suppose $E(K)[p] = 0$. Then $X(E/K_\infty^-)$ has Λ^--rank one, and we have*

$$\mathrm{char}_{\Lambda^-}(X(E/K_\infty^-)_{\mathrm{tors}}) \supset \mathrm{char}_{\Lambda^-}\left(\frac{\check{S}(E/K_\infty^-)}{\Lambda^- \cdot \kappa_\infty^{\mathrm{Hg}}}\right)^2$$

in $\Lambda^-[1/p]$.

[2] Alternatively, it also follows from the Λ^--adic BDP formula and the nonvanishing of $\mathcal{L}_v^{\mathrm{BDP}}(f/K)$ (see [Hsi14]) via Hida's methods.

Proof. This follows from a refinement of Kolyvagin's methods building on some of the techniques developed by Howard and Nekovář (see [How04, Nek07]) in related settings. The difficulty in the present case lies in the fact that no "big image" hypotheses on T_pE is being made.

By standard arguments, the non-triviality of $\kappa_\infty^{\mathrm{Hg}}$ and a generalized Cassels–Tate pairing implies the existence of a Λ^--module pseudo-isomorphism

$$X(E/K_\infty^-) \sim \Lambda^- \oplus M \oplus M$$

with M a finitely generated torsion Λ^--module. Thus the task is to compare the characteristic ideal of M with that of $\check{S}(E/K_\infty^-)/\Lambda^- \cdot \kappa_\infty^{\mathrm{Hg}}$. Let $\mathfrak{P}$ be a height one prime of Λ^- with $\mathfrak{P} \neq (p)$, and take a sequence $\mathfrak{P}_m$ of height one primes of Λ^- with $\mathfrak{P}_m \to \mathfrak{P}$ as $m \to \infty$. Note that each such $\mathfrak{P}_m$ corresponds to a character $\alpha_m : \Gamma^- \to R_m^\times$ with R_m a finite extension of $\mathbb{Z}_p$. By inductively choosing a sequence of Kolyvagin primes (of "depth k" for $k \gg 0$) using Cebotarev, one arrives at the inequality

$$\mathrm{length}_{R_m}(M_{\mathfrak{P}_m}) \leq \mathrm{length}_{R_m}\big(\check{S}(E/K_\infty)_{\mathfrak{P}_m}/R_m \cdot \kappa^{\mathrm{Hg}}_{\infty,\mathfrak{P}_m}\big) + E_m,$$

where E_m is an "error term" behaving asymptotically like $\mathrm{ord}_p(\alpha_m(\gamma) - \alpha_m^{-1}(\gamma))$ as $m \to \infty$. Thus $E_m = O(1)$ as long as $\mathfrak{P} \neq (\gamma - 1)$, and hence by a control theorem in the style of Mazur–Rubin [MR04], letting $\mathfrak{P}$ vary we deduce that the claimed divisibility holds in $\Lambda^-[1/p, 1/(\gamma-1)]$. To handle the prime $\mathfrak{P} = (\gamma - 1)$, one takes a sequence $\mathfrak{P}_m$ with $\alpha_m \equiv 1 \pmod{p^m}$, and choosing a sequence of Kolyvagin primes as above, but this time exploiting the action of complex conjugation on $(T_pE \otimes \alpha_m)/p^m$, a different induction argument yields the inequality

$$\mathrm{length}_{R_m}(M_{\mathfrak{P}_m}) \leq \mathrm{length}_{R_m}\big(\check{S}(E/K_\infty)_{\mathfrak{P}_m}/R_m \cdot \kappa^{\mathrm{Hg}}_{\infty,\mathfrak{P}_m}\big) + E_m,$$

with an error term E_m now bounded independently of m, which by a control theorem yields the desired divisibility also at the augmentation ideal $(\gamma - 1)$. □

Remark 2.6. For the application to the p-converse to the theorem of Gross–Zagier and Kolyvagin, it suffices to have the divisibility "$\subset$" in Theorem 2.1 (rather than the equality of characteristic ideals) after inverting $(\gamma - 1)$ and (p); similarly, an ambiguity by powers of $(\gamma - 1)$ is harmless for the application to the p-part of the BSD formula in analytic rank one. However, the final from of the result of Theorem 2.1 obtained in [CGS23] is essential to the proof of Mazur's main conjecture at Eisenstein primes explained in the next lecture.

3. Lecture 3: Mazur's main conjecture at Eisenstein primes

3.1. Main result.

In this lecture we explain the proof of the following result from [CGS23].

Theorem 3.1. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N, and let $p \nmid 2N$ be a good Eisenstein prime for E, i.e. such that*

$$E[p]^{ss} \simeq \mathbb{F}_p(\phi) \oplus \mathbb{F}_p(\psi)$$

for characters $\phi, \psi = \omega\phi^{-1} : G_{\mathbb{Q}} \to \mathbb{F}_p^\times$. Assume that $\phi|_{G_p} \neq 1, \omega$. Then Mazur's main conjecture (Conjecture 1.2) holds for E.

Previously, the following results were known towards Conjecture 1.2 for good Eisenstein primes p:

- Rubin [Rub91]: proof in the CM case.
- Kato [Kat99]: $X(E/\mathbb{Q}_\infty)$ is Λ-torsion, with
$$\mathrm{char}_\Lambda(X(E/\mathbb{Q}_\infty)) = \big(\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})\big)$$
in $\Lambda[1/p]$.
- Wüthrich [Wut14]: $\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})$ is integral, and Kato's divisibility holds in Λ.
- Greenberg–Vatsal [GV00]: proof in "half" of the cases; more precisely, when
$$\phi = \begin{cases} \text{unramified at } p \text{ and odd, or} \\ \text{ramified at } p \text{ and even;} \end{cases} \tag{12}$$
in other words, when $E[p^\infty]$ contains no cyclic subgroups of multiplicative type.

The condition on ϕ in the Greenberg–Vatsal result is needed to ensure the vanishing of $\mu(X(E/\mathbb{Q}_\infty))$ building on the work of Ferrero–Washington [FW79] and Mazur–Wiles [MW84]. Without this restriction on ϕ, it was shown by Greenberg [Gre99] that $\mu(X(E/\mathbb{Q}_\infty))$ is positive, and by work of Stevens [Ste89] one similarly knows that $\mu(\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q}))>0$ when ϕ doesn't satisfy (12).

Thus to extend the Greenberg–Vatsal method beyond the cases covered by (12) one is faced with the challenge of determining the exact value of the algebraic and analytic invariants, which seems to be a very difficult problem (but see [BP19] and [PW24] for interesting recent works in this direction).

The proof of Theorem 3.1 is based on a different method to compare Iwasawa invariants. The method is insensitive to the value of μ, and in particular gives a new proof of the Greenberg–Vatsal result in the cases they considered.

3.2. **Comparing Iwasawa invariants.** In this section we explain the strategy from [CGS23] to arrive at the equalities

$$\mu(X(E/\mathbb{Q}_\infty))=\mu(\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})),\quad \lambda(X(E/\mathbb{Q}_\infty))=\lambda(\mathcal{L}_p^{\mathrm{MSD}}(E/\mathbb{Q})), \tag{13}$$

which combined with Kato's divisibility (as integrally refined by Wüthrich [Wut14]) yields Theorem 3.1. Some of the details on how the strategy is carried out are given in the next subsection.

The following discussion applies to any prime $p\nmid 2N$ of good ordinary reduction for E. Let K be an imaginary quadratic field satisfying (spl), and let K_∞^+ be the cyclotomic $\mathbb{Z}_p$-extension of K. Following Greenberg [Gre89], we define the ordinary Selmer group of E over K_∞^+ by

$$\mathrm{Sel}_{p^\infty}(E/K_\infty^+):=\ker\left\{\mathrm{H}^1(K_\infty^+,E[p^\infty])\to\prod_{w\mid p}\frac{\mathrm{H}^1(K_{\infty,w}^+,E[p^\infty])}{A_w}\times\prod_{w\nmid p}\mathrm{H}^1(I_w,E[p^\infty])\right\},$$

where $A_w:=\mathrm{im}\{E^+[p^\infty]\to E[p^\infty]\}_{\mathrm{div}}$, with $E^+[p^\infty]$ the kernel of the reduction map at p, and $I_w\subset G_{K_{\infty,w}^+}$ the inertia subgroup at w. On the analytic side, Hida's p-adic Rankin method [Hid85] (as studied by Perrin-Riou [PR88] in detail in the case of Rankin–Selberg convolution of f with theta series of K) yields the construction of a 2-variable p-adic L-function

$$\mathcal{L}_p^{\mathrm{PR}}(E/K)\in\Lambda_K:=\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/K)]],$$

where K_∞/K is the $\mathbb{Z}_p^2$-extension of K, interpolating the algebraic part of the central L-values $L(f/K,\chi,1)$ (with a normalized period depending on E), as χ runs over the finite orders characters of Γ_K.

The action of complex conjugation yields a decomposition $\Gamma_K\simeq\Gamma^+\times\Gamma^-$ into $\pm$-eigenspaces, with Γ^+ (resp. Γ^-) idenfitied with the Galois group of the cyclotomite (resp. anticyclotomic) $\mathbb{Z}_p$-extension of K. Denoting by $\mathcal{L}_p^{\mathrm{PR}}(E/K)^+$ the image of $\mathcal{L}_p^{\mathrm{PR}}(E/K)$ under the natural projection

$$\Lambda_K\to\Lambda^+:=\mathbb{Z}_p[[\mathrm{Gal}(K_\infty^+/K)]]\simeq\Lambda,$$

Greenberg's Iwasawa Main Conjecture for general p-ordinary representations [Gre89] predicts that for $\star\in\{+,\emptyset\}$, the Pontryagin dual $X(E/K_\infty^\star)=\mathrm{Hom}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(E/K_\infty^\star),\mathbb{Q}_p/\mathbb{Z}_p)$ is $\Lambda^\star$-torsion, with

$$\mathrm{char}_{\Lambda^\star}(X(E/K_\infty^\star))\stackrel{?}{=}\big(\mathcal{L}_p^{\mathrm{PR}}(E/K)^\star\big). \tag{14}$$

As a motivation for the general argument, we note that the aforementioned results, together with Theorem 2.1, already imply a proof of this conjecture in some cases. Indeed, denote by E^K the twist of E by the quadratic character corresponding to K. Kato's integral divisibility towards Conjecture 1.2 for E and E^K yields the divisibility

$$\mathrm{char}_{\Lambda^+}(X(E/K_\infty^+))\supset\big(\mathcal{L}_p^{\mathrm{PR}}(E/K)^+\big), \tag{15}$$

while from Theorem 2.1 and the fact that $K_\infty^-\cap K_\infty^+=K$ one can show the equality up to a p-adic unit

$$\mathcal{F}(E/K_\infty^+)(0)\sim_p\mathcal{L}_p^{\mathrm{PR}}(E/K)^+(0), \tag{16}$$

where $\mathcal{F}(E/K_\infty^+)\in\Lambda^+$ is any characteristic power series for $X(E/K_\infty^+)$. It is easy to see that the combination of (15) and (16) implies (14), and hence Conjecture 1.2, *provided* $\mathcal{L}_p^{\mathrm{PR}}(E/K)^+(0)\neq 0$.

Unfortunately, hypothesis (Heeg) forces this value to vanish for sign reasons. Using Beilinson–Flach classes and their explicit reciprocity laws (as described in more detail in the next subsection), the same conclusion applies *provided* $\mathcal{L}_v^{\mathrm{BDP}}(E/K)(0) \neq 0$, which by the main result of [BDP13] amounts to the requirement that the Heegner point $y_K \in E(K)$ is non-torsion.

To treat the general case, the idea is to take an anticyclotomic character

$$\alpha : \Gamma^- \to \mathbb{Z}_p^\times$$

with $\alpha \equiv 1 \pmod{p^M}$, for some $M \gg 0$ to stay away from any problematic zeroes; in particular, so that $\mathcal{L}_v^{\mathrm{BDP}}(E/K)(\alpha) \neq 0$. From a refinement [BSTW23] of the Beilinson–Flach classes constructed by Lei–Loeffler–Zerbes [LLZ14, LLZ15] and Kings–Loeffler–Zerbes [KLZ20, KLZ17] (allowing one of the forms to be residually reducible and p-indistinguished), and their explicit reciprocity laws, one can deduce from Theorem 2.1 a proof of the α-twisted variant of conjecture (14) for K_∞^+/K:

$$\mathrm{char}_{\Lambda^+}(X(E(\alpha)/K_\infty^+)) \stackrel{?}{=} \big(\mathcal{L}_p^{\mathrm{PR}}(E(\alpha)/K)^+\big). \tag{17}$$

Establishing (17) for a suitable choice of α as above is the key to the proof of Theorem 3.1, since from the easy congruences

$$\begin{aligned}\mathrm{char}_{\Lambda^+}(X(E(\alpha)/K_\infty^+)) &\equiv \mathrm{char}_{\Lambda^+}(X(E/K_\infty^+)) \pmod{p^M},\\ \mathcal{L}_p^{\mathrm{PR}}(E(\alpha)/K)^+ &\equiv \mathcal{L}_p^{\mathrm{PR}}(E/K)^+ \pmod{p^M},\end{aligned}$$

it implies the equalities

$$\mu(X(E/K_\infty^+)) = \mu(\mathcal{L}_p^{\mathrm{PR}}(E/K)^+), \quad \lambda(X(E/K_\infty^+)) = \lambda(\mathcal{L}_p^{\mathrm{PR}}(E/K)^+)$$

(in particular, without knowing the specific value of the μ-invariants!). Together with the integral divisibility (15), these equalities yield the proof of conjecture (14) for K_∞^+/K, from where the proof of Theorem 3.1 can be deduced from Kato's work.

3.3. **From anticyclotomic to cyclotomic.** It remains to outline the proof of (17).

Since Conjecture 1.2 is known to be isogeny invariant, we replace E by the elliptic curve $E_\bullet/\mathbb{Q}$ is the same isogeny class constructed by Wüthrich [Wut14]. This can be characterized as the elliptic curve whose p-adic Tate module $T_pE_\bullet$ agrees with the geometric lattice in the p-adic representation V_f realized as the maximal quotient of $\mathrm{H}^1_{\text{ét}}(Y_1(N)_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(1))$ on which the Hecke operators acts with the same eigenvalues as f.

Let $\mathrm{H}^1_{\mathrm{Iw}}(K_\infty, T_pE_\bullet)$ be the Iwasawa cohomology for the $\mathbb{Z}_p^2$-extension K_∞/K, which by Shapiro's lemma can be identified with $\mathrm{H}^1(K, T_pE_\bullet \hat{\otimes}_{\mathbb{Z}_p}\Lambda_K)$. By the work of Lei–Loeffler–Zerbes and Kings–Loeffler–Zerbes, as refined in the case of interest in recent work of Burungale–Skinner–Tian–Wan, there exists a class

$$\mathrm{BF}_\alpha \in \mathrm{H}^1_{\mathrm{Iw}}(K_\infty, T_pE_\bullet(\alpha))$$

together with two explicit reciprocity laws:

(1) At the prime v, the class BF_α naturally lands in the subspace $\mathrm{H}^1(K_v, T_p^+E_\bullet(\alpha))$ and there is a generalized Coleman power series map

$$\mathrm{Col}_v : \mathrm{H}^1_{\mathrm{Iw}}(K_{\infty,v}, T_p^+E_\bullet(\alpha)) \hookrightarrow \mathbb{Z}_p^{\mathrm{ur}}\hat{\otimes}_{\mathbb{Z}_p}\Lambda_K$$

sending $\mathrm{res}_v(\mathrm{BF}_\alpha)$ to $\mathcal{L}_v^{\mathrm{Gr}}(f(\alpha)/K)$, where $\mathcal{L}_v^{\mathrm{Gr}}(f(\alpha)/K)$ is a two-variable Rankin–Selberg p-adic L-function with the property that its natural image $\mathcal{L}_v^{\mathrm{Gr}}(f(\alpha)/K)^-$ in Λ^{ur} satisfies (as can be checked by comparing their respective interpolation properties)

$$\big(\mathcal{L}_v^{\mathrm{Gr}}(f(\alpha)/K)^-\big) = \big(\mathcal{L}_v^{\mathrm{BDP}}(f(\alpha)/K)^2\big),$$

where $\mathcal{L}_v^{\mathrm{BDP}}(f(\alpha)/K)$ is the twist of $\mathcal{L}_v^{\mathrm{BDP}}(f(\alpha)/K)$ by the anticyclotomic character α.

(2) At the prime $\overline{v}$, there is a generalized Coleman power series map

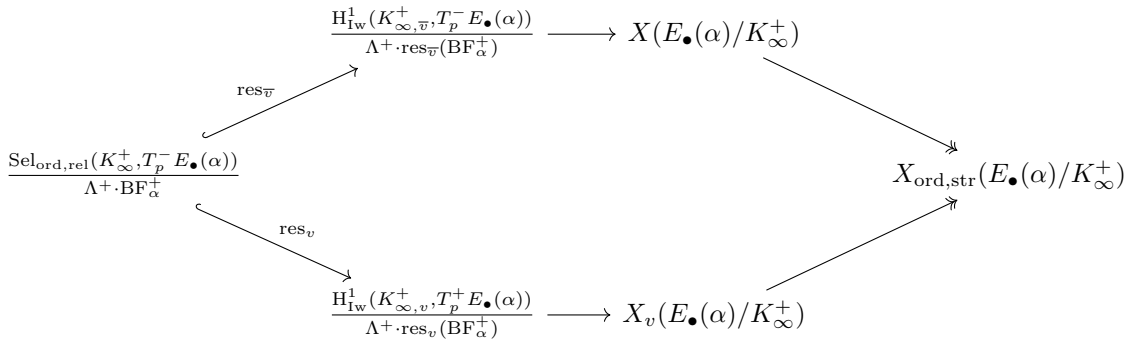
$$\mathrm{Col}_{\overline{v}} : \mathrm{H}^1_{\mathrm{Iw}}(K_{\infty,\overline{v}}, T_p^-E_\bullet(\alpha)) \hookrightarrow \Lambda_K,$$

where $T_p^-E_\bullet(\alpha) := T_pE_\bullet(\alpha)/T_p^+E_\bullet(\alpha)$, sending the natural image of BF_α to $\mathcal{L}_p^{\mathrm{PR}}(E(\alpha)/K)$.

The cyclotomic projection $\mathrm{BF}_\alpha^+ \in \mathrm{H}^1_{\mathrm{Iw}}(K_\infty^+, T_pE_\bullet(\alpha))$ is the base class of a cyclotomic Euler system for $T_pE_\bullet(\alpha)$, and for a suitable choice of α it can be shown to be nonzero as a consequence of Rohrlich's nonvanishing results [Roh84] and the second of the above explicit reciprocity laws. By the Euler system machinery [Rub00], one thus obtains that a certain dual Selmer group $X_{\mathrm{ord,str}}(E_\bullet(\alpha)/K_\infty^+)$ (dual to the compact Selmer group $\mathrm{Sel}_{\mathrm{ord,rel}}(K_\infty^+, T_pE_\bullet(\alpha))$ on which the class BF_α^+ lives) is Λ^+-torsion, with characteristic ideal satisfying the divisibility

$$\mathrm{char}_{\Lambda^+}\big(X_{\mathrm{ord,str}}(E_\bullet(\alpha)/K_\infty^+)\big) \supset \mathrm{char}_{\Lambda^+}\left(\frac{\mathrm{Sel}_{\mathrm{ord,rel}}(K_\infty^+, T_pE_\bullet(\alpha))}{\Lambda^+\cdot \mathrm{BF}_\alpha^+}\right)$$

in $\Lambda^+[1/p]$. By the commutative hexagon deduced from Poitou–Tate duality:



this translates into the divisibilities

$$\mathrm{char}_{\Lambda^+}(X(E_\bullet(\alpha)/K_\infty^+)) \supset \mathrm{char}_{\Lambda^+}\left(\frac{\mathrm{H}^1_{\mathrm{Iw}}(K^+_{\infty,\overline{v}}, T_p^- E_\bullet(\alpha))}{\Lambda^+\cdot \mathrm{res}_{\overline{v}}(\mathrm{BF}_\alpha^+)}\right) = \big(\mathcal{L}_p^{\mathrm{PR}}(E_\bullet(\alpha)/K)^+\big) \tag{18}$$

with the equality following from the explicit reciprocity law at $\overline{v}$ (using that $\mathrm{Col}_{\overline{v}}$ has pseudo-null cokernel), and

$$\mathrm{char}_{\Lambda^+}(X_v(E_\bullet(\alpha)/K_\infty^+))\tilde{\Lambda}^+ \supset \mathrm{char}_{\Lambda^+}\left(\frac{\mathrm{H}^1_{\mathrm{Iw}}(K^+_{\infty,v}, T_p^+ E_\bullet(\alpha))}{\Lambda^+\cdot \mathrm{res}_v(\mathrm{BF}_\alpha^+)}\right)\tilde{\Lambda}^+ = \big(\mathcal{L}_v^{\mathrm{Gr}}(E_\bullet(\alpha)/K)^+\big), \tag{19}$$

similarly using the explicit reciprocity law at v. Further choosing α so that $\mathcal{L}_v^{\mathrm{BDP}}(f/K)(0) \neq 0$ (as is possible by the nonvanishing of $\mathcal{L}_v^{\mathrm{BDP}}(f/K)$ as an element in Λ^{ur}), we deduce from Theorem 3.1 that both sides of the divisibility (19) agree at $T = 0$ and are nonzero, hence they are equal. From the commutative hexagon, it follows that the divisibility in (18) is also an equality, concluding the proof of (17).

References

[BDP13] Massimo Bertolini, Henri Darmon, and Kartik Prasanna. Generalized Heegner cycles and p-adic Rankin L-series. *Duke Math. J.*, 162(6):1033–1148, 2013. With an appendix by Brian Conrad.

[BP19] Joël Bellaïche and Robert Pollack. Congruences with Eisenstein series and μ-invariants. *Compos. Math.*, 155(5):863–901, 2019.

[Bra11] Miljan Brakočević. Anticyclotomic p-adic L-function of central critical Rankin-Selberg L-value. *Int. Math. Res. Not. IMRN*, (21):4967–5018, 2011.

[BSTW23] Ashay Burungale, Christopher Skinner, Ye Tian, and Xin Wan. Zeta elements for elliptic curves and applications. 2023. preprint.

[CGLS22] Francesc Castella, Giada Grossi, Jaehoon Lee, and Christopher Skinner. On the anticyclotomic Iwasawa theory of rational elliptic curves at Eisenstein primes. *Invent. Math.*, 227:517–580, 2022.

[CGS23] Francesc Castella, Giada Grossi, and Christopher Skinner. Mazur's main conjecture at Eisenstein primes. 2023. preprint, arXiv:2303.04373.

[CH18] Francesc Castella and Ming-Lun Hsieh. Heegner cycles and p-adic L-functions. *Math. Ann.*, 370(1-2):567–628, 2018.

[Cor02] Christophe Cornut. Mazur's conjecture on higher Heegner points. *Invent. Math.*, 148(3):495–523, 2002.

[FW79] Bruce Ferrero and Lawrence C. Washington. The Iwasawa invariant μ_p vanishes for abelian number fields. *Ann. of Math. (2)*, 109(2):377–395, 1979.

[Gre77] Ralph Greenberg. On p-adic L-functions and cyclotomic fields. II. *Nagoya Math. J.*, 67:139–158, 1977.

[Gre89] Ralph Greenberg. Iwasawa theory for p-adic representations. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 97–137. Academic Press, Boston, MA, 1989.

[Gre94] Ralph Greenberg. Iwasawa theory and p-adic deformations of motives. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 193–223. Amer. Math. Soc., Providence, RI, 1994.

[Gre99] Ralph Greenberg. Iwasawa theory for elliptic curves. In *Arithmetic theory of elliptic curves (Cetraro, 1997)*, volume 1716 of *Lecture Notes in Math.*, pages 51–144. Springer, Berlin, 1999.

[GV00] Ralph Greenberg and Vinayak Vatsal. On the Iwasawa invariants of elliptic curves. *Invent. Math.*, 142(1):17–63, 2000.

[GZ86] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[Hid85] Haruzo Hida. A p-adic measure attached to the zeta functions associated with two elliptic modular forms. I. *Invent. Math.*, 79(1):159–195, 1985.

[Hid10] Haruzo Hida. The Iwasawa μ-invariant of p-adic Hecke L-functions. *Ann. of Math. (2)*, 172(1):41–137, 2010.

[How04] Benjamin Howard. The Heegner point Kolyvagin system. *Compos. Math.*, 140(6):1439–1472, 2004.

[Hsi14] Ming-Lun Hsieh. Special values of anticyclotomic Rankin-Selberg L-functions. *Doc. Math.*, 19:709–767, 2014.

[HT93] H. Hida and J. Tilouine. Anti-cyclotomic Katz p-adic L-functions and congruence modules. *Ann. Sci. École Norm. Sup. (4)*, 26(2):189–259, 1993.

[JSW17] Dimitar Jetchev, Christopher Skinner, and Xin Wan. The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one. *Camb. J. Math.*, 5(3):369–434, 2017.

[Kat78] Nicholas M. Katz. p-adic L-functions for CM fields. *Invent. Math.*, 49(3):199–297, 1978.

[Kat99] Kazuya Kato. Euler systems, Iwasawa theory, and Selmer groups. *Kodai Math. J.*, 22(3):313–372, 1999.

[Kat04] Kazuya Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:117–290, 2004.

[KLZ17] Guido Kings, David Loeffler, and Sarah Livia Zerbes. Rankin-Eisenstein classes and explicit reciprocity laws. *Camb. J. Math.*, 5(1):1–122, 2017.

[KLZ20] Guido Kings, David Loeffler, and Sarah Livia Zerbes. Rankin-Eisenstein classes for modular forms. *Amer. J. Math.*, 142(1):79–138, 2020.

[Kol88] Victor Kolyvagin. The Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves (Russian). *Izvestiya Akademii Nauk SSSR. Seriya Matematicheskaya*, 52(6):1154–1180, 1327, 1988. translation in Mathematics of the USSR-Izvestiya **33** (1989), no. 3, 473–499.

[Kri16] Daniel Kriz. Generalized Heegner cycles at Eisenstein primes and the Katz p-adic L-function. *Algebra Number Theory*, 10(2):309–374, 2016.

[KY24] Timo Keller and Mulun Yin. On the anticyclotomic Iwasawa theory of newforms at Eisenstein primes of semistable reduction. 2024. preprint, arXiv:2402.12781.

[LLZ14] Antonio Lei, David Loeffler, and Sarah Livia Zerbes. Euler systems for Rankin-Selberg convolutions of modular forms. *Ann. of Math. (2)*, 180(2):653–771, 2014.

[LLZ15] Antonio Lei, David Loeffler, and Sarah Livia Zerbes. Euler systems for modular forms over imaginary quadratic fields. *Compos. Math.*, 151(9):1585–1625, 2015.

[LZ14] David Loeffler and Sarah Livia Zerbes. Iwasawa theory and p-adic L-functions over $\mathbb{Z}_p^2$-extensions. *Int. J. Number Theory*, 10(8):2045–2095, 2014.

[Maz72] Barry Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.*, 18:183–266, 1972.

[MR04] Barry Mazur and Karl Rubin. Kolyvagin systems. *Mem. Amer. Math. Soc.*, 168(799):viii+96, 2004.

[MSD74] Barry Mazur and Peter Swinnerton-Dyer. Arithmetic of Weil curves. *Invent. Math.*, 25:1–61, 1974.

[MW84] B. Mazur and A. Wiles. Class fields of abelian extensions of $\mathbf{Q}$. *Invent. Math.*, 76(2):179–330, 1984.

[Nek07] Jan Nekovář. The Euler system method for CM points on Shimura curves. In *L-functions and Galois representations*, volume 320 of *London Math. Soc. Lecture Note Ser.*, pages 471–547. Cambridge Univ. Press, Cambridge, 2007.

[PR88] Bernadette Perrin-Riou. Fonctions L p-adiques associées à une forme modulaire et à un corps quadratique imaginaire. *J. London Math. Soc. (2)*, 38(1):1–32, 1988.

[PR92] Bernadette Perrin-Riou. Théorie d'Iwasawa et hauteurs p-adiques. *Invent. Math.*, 109(1):137–185, 1992.

[PR94] Bernadette Perrin-Riou. Théorie d'Iwasawa des représentations p-adiques sur un corps local. *Invent. Math.*, 115(1):81–161, 1994. With an appendix by Jean-Marc Fontaine.

[PW24] Robert Pollack and Preston Wake. Iwasawa invariants in residually reducible Hida families. 2024. preprint, arXiv:2401.14518.

[Roh84] David E. Rohrlich. On L-functions of elliptic curves and anticyclotomic towers. *Invent. Math.*, 75(3):383–408, 1984.

[Rub91] Karl Rubin. The "main conjectures" of Iwasawa theory for imaginary quadratic fields. *Invent. Math.*, 103(1):25–68, 1991.

[Rub00] Karl Rubin. *Euler systems*, volume 147 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2000. Hermann Weyl Lectures. The Institute for Advanced Study.

[Sch85] Peter Schneider. p-adic height pairings. II. *Invent. Math.*, 79(2):329–374, 1985.

[Ski16] Christopher Skinner. Multiplicative reduction and the cyclotomic main conjecture for GL_2. *Pacific J. Math.*, 283(1):171–200, 2016.

[Ski20] Christopher Skinner. A converse to a theorem of Gross, Zagier, and Kolyvagin. *Ann. of Math. (2)*, 191(2):329–354, 2020.

[Ste89] Glenn Stevens. Stickelberger elements and modular parametrizations of elliptic curves. *Invent. Math.*, 98(1):75–106, 1989.

[SU14] Christopher Skinner and Eric Urban. The Iwasawa main conjectures for GL_2. *Invent. Math.*, 195(1):1–277, 2014.

[Vat03] Vinayak Vatsal. Special values of anticyclotomic L-functions. *Duke Math. J.*, 116(2):219–261, 2003.

[Wan20] Xin Wan. Iwasawa main conjecture for Rankin-Selberg p-adic L-functions. *Algebra Number Theory*, 14(2):383–483, 2020.

[Wan21a] Xin Wan. Heegner Point Kolyvagin System and Iwasawa Main Conjecture. *Acta Math. Sin. (Engl. Ser.)*, 37(1):104–120, 2021.

[Wan21b] Xin Wan. Heegner point Kolyvagin system and Iwasawa main conjecture. *Acta Math. Sin. (Engl. Ser.)*, 37(1):104–120, 2021.

[Wut14] Christian Wuthrich. On the integrality of modular symbols and Kato's Euler system for elliptic curves. *Doc. Math.*, 19:381–402, 2014.

[Zha14] Wei Zhang. Selmer groups and the indivisibility of Heegner points. *Camb. J. Math.*, 2(2):191–253, 2014.

Department of Mathematics, University of California, Santa Barbara, CA 93106, USA
Email address: castella@ucsb.edu