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 1
1. Lecture 1: Main conjectures and applications 2
  1.1. Mazur’s main conjecture 2
  1.2. Perrin-Riou’s main conjecture 3
  1.3. BDP main conjecture 5
2. Lecture 2: BDP main conjecture at Eisenstein primes 6
  2.1. Main result 6
  2.2. Anticyclotomic Greenberg–Vatsal method 7
  2.3. Kolyvagin system argument with “error terms” 8
3. Lecture 3: Mazur’s main conjecture at Eisenstein primes 9
  3.1. Main result 9
  3.2. Comparing Iwasawa invariants 10
  3.3. From anticyclotomic to cyclotomic 11
References 12

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 $\text{Re}(s) > 3/2$, 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

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

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

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

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

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

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,
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:

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

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

2. $p$-converse to the theorem of Gross–Zagier and Kolyvagin:

$$\text{corank}_{\mathbb{Z}} \text{Sel}_{p}^{\infty}(E/\mathbb{Q}) = 1 \implies \text{ord}_{s=1} L(E, s) = 1,$$

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

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

3. $p$-part of the BSD formula in analytic rank 1:

$$\text{ord}_{s=1} L(E, s) = 1 \implies \text{ord}_p \left( \frac{L(E, 1)}{\Omega_E \cdot \text{Reg}_E} \right) = \text{ord}_p \left( \frac{\# \text{III}(E/\mathbb{Q}) \cdot \text{Tam}(E/\mathbb{Q})}{\left( \# E(\mathbb{Q})_{\text{tors}} \right)^2} \right),$$

where $\text{Reg}_E$ 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

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

with $\Delta \simeq \text{Gal}(\mathbb{Q}(\mu_{p})/\mathbb{Q})$ 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 $\text{Gal}(\mu_{p^{\infty}})$ by $\Delta$.

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 $\text{Sel}_{p}^{\infty}(E/\mathbb{Q}_n)$ be the usual $p^{\infty}$-Selmer group, defined as

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

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

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 $F_{\infty}/F$).

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

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

have finite kernel and cokernel, of order bounded as $n \to \infty$. 
The original proof of Theorem 1.1 can be found in Mazur [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 $Sel_p^{\infty}(E/Q_\infty)$ is cofinitely generated over $\Lambda$, i.e. the Pontryagin dual

$$X(E/Q_\infty) := \text{Hom}_{\mathbb{Z}_p}(Sel_p^{\infty}(E/Q_\infty), Q_p/\mathbb{Z}_p)$$

is finitely generated over $\Lambda$. Mazur further conjectured that $X(E/Q_\infty)$ is $\Lambda$-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 $Sel_p^{\infty}(E/Q)$ is finite (so in particular, $E(Q)$ 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 $L_p^{\text{MSD}}(E/Q) \in \Lambda \otimes Q_p$ characterized by the property that for every finite order character $\chi : \Gamma \to \mu_p^{\infty}$

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

where $\alpha_p$ is the $p$-adic unit root of $x^2 - a_p(E)x + p$ and $\tau(\chi)$ 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 $L_p^{\text{MSD}}(E/Q)$ is integral, i.e. lies in $\Lambda$.

**Conjecture 1.2** (Mazur’s main conjecture). $X(E/Q_\infty)$ is $\Lambda$-torsion, with

$$\text{char}_\Lambda(X(E/Q_\infty)) = (L_p^{\text{MSD}}(E/Q)).$$

As usual, we identify the Iwasawa algebra $\Lambda$ 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.

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

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

Let $\mathcal{F}(E/Q_\infty) \in \Lambda$ be a characteristic power series of $X(E/Q_\infty)$, i.e. a generator of the principal ideal $\text{char}_\Lambda(X(E/Q_\infty))$. Then by the work of Schneider [Sch88] and Perrin-Riou [PR92] one has

$$\mathcal{F}(E/Q_\infty)(0) \sim_p (1 - \alpha_p^{-1})^2 \cdot \#\text{Sel}_p^{\infty}(E/Q) \cdot \frac{\text{Tam}(E/Q)}{(\#(E/Q)_{\text{tors}})^2}.$$

Since by Conjecture 1.2 the left-hand side of (2) has the same $p$-adic valuation as $L_p^{\text{MSD}}(E/Q)(0)$, 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 $K/Q$ be an imaginary quadratic field satisfying the following Heegner hypothesis:

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

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

Via a fixed modular parametrization
\[ \varphi : X_0(N) \to E, \]
the Kummer images of Heegner points of \( p \)-power conductor yield classes
\[ x_n \in \text{Sel}(K_n^-, T_p E) := \lim_{\to m} \text{Sel}_{p^n}(E/K_n^-), \]
where \( T_p E \) is the \( p \)-adic Tate module of \( E \). Using the ordinary hypotheses on \( p \), these classes can be made compatible under the corestriction maps \( \text{Sel}(K_{n+1}^-, T_p E) \to \text{Sel}(K_n^-, T_p E) \), hence yielding an element
\[ \kappa_{Hg}^{\infty} \in \tilde{S}(E/K_-^\infty) := \lim_{\downarrow n} \text{Sel}(K_n^-, T_p E). \]

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

**Conjecture 1.4** (Perrin-Riou’s main conjecture). \( X(E/K_-^\infty) \) has \( \Lambda^- \)-rank 1, with
\[ \text{char}_{\Lambda^-}(X(E/K_-^\infty)_{\text{tors}}) = \text{char}_{\Lambda^-} \left( \frac{\tilde{S}(E/K_-^\infty)}{\Lambda^- \cdot \kappa_{Hg}^{\infty}} \right)^2 \cdot \frac{1}{u_K c^2}, \]
where the subscript \( \text{tors} \) denotes the maximal \( \Lambda^- \)-torsion submodule, \( u_K := \frac{1}{2} \#(\mathcal{O}_K^\times) \), and \( c \in \mathbb{Q}^\times \) is the Manin constant\(^1\) attached to \( \varphi \).

**Proposition 1.5.** Assume Conjecture 1.4. Then
\[ \text{corank}_{\mathbb{Z}_p} \text{Sel}_{p^n}(E/\mathbb{Q}) = 1 \iff \text{ord}_{s=1} L(E, s) = 1, \]
i.e. the \( p \)-converse to the theorem of Gross–Zagier and Kolyvagin holds.

**Proof.** Suppose \( \text{corank}_{\mathbb{Z}_p} \text{Sel}_{p^n}(E/\mathbb{Q}) = 1 \), 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 \( \# \text{Sel}_{p^n}(E^K/\mathbb{Q}) < \infty \), and so
\[ \text{corank}_{\mathbb{Z}_p} \text{Sel}_{p^n}(E/K) = \text{corank}_{\mathbb{Z}_p} \text{Sel}_{p^n}(E/\mathbb{Q}) = 1. \]

By a variant of Theorem 1.1 for the extension \( K_-^\infty/K \), it follows that the corank_{\mathbb{Z}_p}(X(E/K_-^\infty)_{\Gamma^-}) = 1. By Conjecture 1.4, this implies that
\[ (\gamma - 1) \nmid \text{char}_{\Lambda^-} \left( \frac{\tilde{S}(E/K_-^\infty)}{\Lambda^- \cdot \kappa_{Hg}^{\infty}} \right), \]
where \( \gamma \in \Gamma^- \) is any topological generator (otherwise one would get \( \text{corank}_{\mathbb{Z}_p}(X(E/K_-^\infty)_{\Gamma^-}) \geq 3 \), and so \( \kappa_{Hg}^{\infty} \) has non-torsion image \( \kappa_{0Hg}^{\infty} \) under the natural map
\[ \tilde{S}(E/K_-^\infty) \to \tilde{S}(E/K_-^\infty)_{\Gamma^-} \to \text{Sel}(K, T_p E). \]
But by construction \( \kappa_{0Hg}^{\infty} \) 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 \( \text{ord}_{s=1} L(E, s) = 1 \), as desired. \( \square \)

**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 \( \Lambda^- \)-extension of the BDP formula) allows one to dispense with the assumption that \( \# \text{III}(E/\mathbb{Q})|p^{\infty} \) forced upon in the original approach.

\(^1\)Thus \( \varphi^* \omega_E = c \cdot 2\pi i f(z) dz \) for the Néron differential \( \omega_E \) 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

$$(p) = v \pi \text{splits in } K,$$

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

Put $\Lambda^\text{ur} := \Lambda^\text{ur} \otimes_{\mathbb{Z}_p} \mathbb{Z}_p$, where $\mathbb{Z}_p$ 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 $\Lambda^\text{ur}$-adic extension in [Bra11, CH18], there is a $p$-adic $L$-function $L^\text{BDP}(f/K) \in \Lambda^\text{ur}$ characterized by the property that for every character $\chi : \Gamma^- \to \mathbb{C}_{p}^\times$ crystalline at both $v$ and $\pi$ of weights $(n, -n)$ with $n > 0$ we have

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

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

On the algebraic side, define the BDP Selmer group by

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

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

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). $X_v^\text{BDP}(E/K_\infty)$ is $\Lambda^\text{ur}$-torsion, with

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

as ideals in $\Lambda^\text{ur}$.

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.

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

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

(i) Hypotheses (Heeg) and (spl) hold;

(ii) $L(E/K,1) \neq 0$.

Then $\text{ord}_{s=1} L(E/K,s) = 1$, 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

$$\text{rank}_{\mathbb{Z}} E(K) = 1, \quad \# \text{III}(E/K) < \infty;$$

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

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

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

$$L^\text{BDP}_p(f/K)(0) \sim_p \frac{1}{u_K c_2^2} \cdot \left( 1 - a_p(E) + \frac{p}{p} \right)^2 \cdot \log_{\omega_E}(y_K)^2.$$
Since Conjecture 1.7 implies that $\mathcal{L}_v^{BDP}(f/K)(0) \sim_p \mathcal{F}_v^{BDP}(E/K_\infty)(0)$, combining (4) and (5) we arrive at

$$[E(K) : \mathbb{Z}y_K]^2 \sim_p \#\Xi(E/K) \cdot \prod_{\omega | N} c_\omega(E/K) \cdot u_K^2v^2.$$ 

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

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

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

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

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

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

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 $\Lambda^-$ denotes the anticyclotomic Iwasawa algebra. From the structure theorem for finitely generated $\Lambda^-$-modules and the Weierstrass preparation theorem, one has Iwasawa $\lambda$- and $\mu$-invariants attached to $X_v^{BDP}(E/K_\infty)$ and $\mathcal{L}_v^{BDP}(E/K)$. 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

  $$\mu(X_v^{BDP}(E/K_\infty)) = \mu(\mathcal{L}_v^{BDP}(E/K)) = 0,$$

  $$\lambda(X_v^{BDP}(E/K_\infty)) = \lambda(\mathcal{L}_v^{BDP}(E/K)^2).$$

- **Step 2:** Show that $X_v^{BDP}(E/K_\infty)$ is $\Lambda^-$-torsion, with

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

  as ideals in $\Lambda^u[1/p]$.

Clearly the combination of these two imply the equality

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

in $\Lambda^u$ predicted by Conjecture 1.7. That they also imply Conjecture 1.4 follows from the equivalence between the two conjectures, a consequence of the $\Lambda^-$-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 $\phi$ 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 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 \( N \mu \). Let \( K^\Sigma \) be the Galois group of the maximal extension of \( K \) unramified outside \( \Sigma \), and consider the \( S \)-imprimitive BDP Selmer group

\[
\text{Sel}_{v,S}^{\text{BDP}}(E/K^\infty) := \ker \left\{ H^1(K^\Sigma/K^\infty, E[p^n]) \to \prod_{w} H^1(K^w, E[p^n]) \right\}.
\]

Let \( X_v^{\text{BDP}}(E/K^\infty) \) be the Pontryagin dual of \( \text{Sel}_{v,S}^{\text{BDP}}(E/K^\infty) \). Multiplying \( \mathcal{L}_v^{\text{BDP}}(f/K) \) by certain elements in \( \Lambda^- \) interpolating the local Euler factors of \( L(f/K,\chi,s) \) at \( s = 1 \) at primes \( v \in S \) over \( \chi \in \Gamma^- \), one can define an \( S \)-imprimitive \( \mathcal{L}_v^{\text{BDP}}(f/K) \in \Lambda^\ur \) 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

\[
\text{char}_{\Lambda^-}(X_v^{\text{BDP}}(E/K^\infty)) \cong (\mathcal{L}_v^{\text{BDP}}(f/K))^2,
\]

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 \( \Phi, \Psi : G_Q \to Z^2_p \) be the Teichmüller lifts of \( \phi, \psi \), respectively. Attached to \( \Phi, \Psi \) one has \( \Lambda^- \) cotorsion Selmer groups \( \text{Sel}_{v,S}(\Phi/K^\infty) \), \( \text{Sel}_{v,S}(\Psi/K^\infty) \) (whose definition is recalled in the proof of Proposition 2.3 below) with associated Iwasawa \( \lambda \)-invariants denoted \( \lambda^S_\phi, \lambda^S_\psi \), respectively.

**Proposition 2.3.** Suppose \( p \nmid 2N \) is such that \( E[p]^S \simeq \Gamma(\phi) \oplus \Gamma(\psi) \) as \( G_Q \)-modules with \( \phi|_{G_p} \neq 1, \omega \). Then \( X_v^{\text{BDP}}(E/K^\infty) \) is \( \Lambda^- \)-torsion, with

\[
\mu(X_v^{\text{BDP}}(E/K^\infty)) = 0, \quad \lambda(X_v^{\text{BDP}}(E/K^\infty)) = \lambda^S_\phi + \lambda^S_\psi.
\]

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

\[
\text{Sel}_{v,S}(\Phi/K^\infty) := \ker \left\{ H^1(K^\Sigma/K^\infty, \mathbb{Q}_p/\mathbb{Z}_p(\Phi)) \to \prod_{w} H^1(K^w, \mathbb{Q}_p/\mathbb{Z}_p(\Phi)) \right\}
\]

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

\[
\lambda^S_\phi = \dim_{\mathbb{F}_p} \left( \text{Sel}_{v,S}(\Phi/K^\infty)[p] \right).
\]

From our conditions on \( \phi \), it is easy to see that the natural map

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

gives \( \text{Sel}_{v,S}(\phi/K^\infty) \simeq \text{Sel}_{v,S}(\Phi/K^\infty)[p] \), where \( \text{Sel}_{v,S}(\phi/K^\infty) \) 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 \( \phi \).

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

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

we immediately arrive at the short exact sequence

\[
0 \to \text{Sel}_{v,S}(\phi/K^\infty) \to \text{Sel}_{v,S}^{\text{BDP}}(E[p]/K^\infty) \to \text{Sel}_{v,S}(\psi/K^\infty) \to 0.
\]
Proposition 2.5. \( \Lambda \) in the proof of Proposition 2.4.

Sketch of proof. The same result holds for the opposite divisibilities, and without inverting \( p \), which by virtue of a \( \Lambda \)-invariant of \( \text{Sel}_{v,S}(E/K^\infty) \) can be computed as \( \dim_{\mathbb{F}_p}(\text{Sel}_{v,S}(E/K^\infty)[p]) \), the last claim in the proposition follows from (11) and (9). \( \square \)

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 \( \Phi, \Psi \). From the constructions of \( \mathcal{L}_{v,S}^{\text{BDP}}(f/K) \) 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

\[ \mathcal{L}_{v,S}^{\text{BDP}}(E/K)^2 \equiv \mathcal{L}_{v,S}^{\text{Katz}}(\Phi) \cdot \mathcal{L}_{v,S}^{\text{Katz}}(\Psi) \pmod{p^{\lambda_{\text{ur}}}}, \]

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

\[ \mu(\mathcal{L}_{v,S}^{\text{BDP}}(E/K)) = 0, \quad \lambda(\mathcal{L}_{v,S}^{\text{BDP}}(E/K)^2) = \lambda(\mathcal{L}_{v,S}^{\text{Katz}}(\Phi)) + \lambda(\mathcal{L}_{v,S}^{\text{Katz}}(\Psi)). \]

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. \( X_v^{\text{BDP}}(E/K^\infty) \) is \( \Lambda^{-}\)-torsion, \( \mathcal{L}_v^{\text{BDP}}(f/K) \) is nonzero, and

\[ \text{char}_\Lambda^{-}(X_v^{\text{BDP}}(E/K^\infty)) \supset (\mathcal{L}_v^{\text{BDP}}(f/K)^2) \]

in \( \Lambda^{ur}[1/p] \).

2. \( X(E/K^\infty) \) has \( \Lambda^{-}\)-rank one, \( \kappa_{\Lambda}^{H_8} \) is not \( \Lambda^{-}\)-torsion, and

\[ \text{char}_\Lambda^{-}(X(E/K^\infty)_{\text{tors}}) \supset \text{char}_\Lambda^{-}\left(\frac{\hat{S}(E/K^\infty)}{\Lambda^{-} \cdot \kappa_{\Lambda}^{H_8}}\right)^2 \]

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 \( T_p^\infty E \simeq \mathbb{Z}_p \) 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

\[ \text{Col}_v : \lim_{\xrightarrow{\mathbb{N}}_n} H^1(K_{n,v}, T_p^\infty E) \hookrightarrow \Lambda^{ur}, \]

which by virtue of a \( \Lambda^{-}\)-adic extension of the BDP formula (see [CH18]) sends the natural image of \( \text{res}_v(\kappa_{\Lambda}^{H_8}) \) to \( \mathcal{L}_v^{\text{BDP}}(f/K) \). The result then follows from a double application (one involving \( \text{res}_v \) and another involving \( \text{res}_\tau \)) of Poitou–Tate duality. \( \square \)

Since the fact that \( \kappa_{\Lambda}^{H_8} \) is not \( \Lambda^{-}\)-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 \( \Lambda^{-}\)-rank one, and we have

\[ \text{char}_\Lambda^{-}(X(E/K^\infty)_{\text{tors}}) \supset \text{char}_\Lambda^{-}\left(\frac{\hat{S}(E/K^\infty)}{\Lambda^{-} \cdot \kappa_{\Lambda}^{H_8}}\right)^2 \]

in \( \Lambda^{-}[1/p] \).

\(^2\)Alternatively, it also follows from the \( \Lambda^{-}\)-adic BDP formula and the nonvanishing of \( \mathcal{L}_v^{\text{BDP}}(f/K) \) (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 $κ_{HG}$ and a generalized Cassels–Tate pairing implies the existence of a $Λ^-$-module pseudo-isomorphism

$$X(E/K_∞^γ) \sim Λ^- ⊕ M ⊕ M$$

with $M$ a finitely generated torsion $Λ^-$-module. Thus the task is to compare the characteristic ideal of $M$ with that of $\hat{S}(E/K_∞^γ)/Λ^-.κ_{HG}$. Let $ℙ$ be a height one prime of $Λ^-$ with $ℙ ≠ (p)$, and take a sequence $ℙ_m$ of height one primes of $Λ^-$ with $ℙ_m → ℙ$ as $m → ∞$. Note that each such $ℙ_m$ corresponds to a character $α_m : Γ^− → R_m^Γ$ with $R_m$ a finite extension of $ℤ_p$. By inductively choosing a sequence of Kolyvagin primes as above, but this time exploiting the action of complex conjugation $T_p$-converse to the theorem of Gross–Zagier and Kolyvagin, one arrives at the inequality

$$\text{length}_{R_m}(Mℙ_m) \leq \text{length}_{R_m}(\hat{S}(E/K_∞^γ)ℙ_m/R_m.κ_{HG}ℙ_m) + E_m,$$

where $E_m$ is an “error term” behaving asymptotically like $\text{ord}_p(α_m(γ) − α_m^{-1}(γ))$ as $m → ∞$. Thus $E_m = O(1)$ as long as $ℙ ≠ (γ − 1)$, and hence by a control theorem in the style of Mazur–Rubin [MR04], letting $ℙ$ vary we deduce that the claimed divisibility holds in $Λ^-[1/p, 1/(γ − 1)]$. To handle the prime $ℙ = (γ − 1)$, one takes a sequence $ℙ_m$ with $α_m ≡ 1$ (mod $p^m$), and choosing a sequence of Kolyvagin primes as above, but this time exploiting the action of complex conjugation on $(T_pE ⊗ α_m)/p^m$, a different induction argument yields the inequality

$$\text{length}_{R_m}(Mℙ_m) \leq \text{length}_{R_m}(\hat{S}(E/K_∞^γ)ℙ_m/R_m.κ_{HG}ℙ_m) + E_m,$$

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 $(γ − 1)$. $\Box$

Remark 2.6. For the application to the $p$-converse to the theorem of Gross–Zagier and Kolyvagin, it suffices to have the divisibility “$c$” in Theorem 2.1 (rather than the equality of characteristic ideals) after inverting $(γ − 1)$ and $(p)$; similarly, an ambiguity by powers of $(γ − 1)$ is harmless for the application to the $p$-part of the BSD formula in analytic rank one. However, the final form 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 $E/ℚ$ be an elliptic curve of conductor $N$, and let $p ∤ 2N$ be a good Eisenstein prime for $E$, i.e. such that

$$E[p]^∞ ≃ ℚ_p(φ) ⊕ ℚ_p(ψ)$$

for characters $φ, ψ = ωφ^{-1} : G_ℚ → ℚ^×_p$. Assume that $φ|G_p ≠ 1, ω$. 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]: $X(E/ℚ_∞)$ is $Λ$-torsion, with $\text{char}_Λ(X(E/ℚ_∞)) = (L_p^{MSD}(E/ℚ))$

in $Λ[1/p]$.
- Wüthrich [Wut14]: $L_p^{MSD}(E/ℚ)$ is integral, and Kato’s divisibility holds in $Λ$.
- Greenberg–Vatsal [GV00]: proof in “half” of the cases; more precisely, when

$$φ = \begin{cases} 1 \text{unramified at } p \text{ and odd, or} \\ \text{ramified at } p \text{ and even;} \end{cases}$$

in other words, when $E[p^∞]$ contains no cyclic subgroups of multiplicative type.
The condition on \( \phi \) in the Greenberg–Vatsal result is needed to ensure the vanishing of \( \mu(X(E/Q_{\infty})) \) building on the work of Ferrero–Washington [FW79] and Mazur–Wiles [MW84]. Without this restriction on \( \phi \), it was shown by Greenberg [Gre99] that \( \mu(X(E/Q_{\infty})) \) is positive, and by work of Stevens [Ste89] one similarly knows that \( \mu(L_{p}^{\text{MSD}}(E/Q)) > 0 \) when \( \phi \) 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 \( \mu \), 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

\[
\mu(X(E/Q_{\infty})) = \mu(L_{p}^{\text{MSD}}(E/Q)), \quad \lambda(X(E/Q_{\infty})) = \lambda(L_{p}^{\text{MSD}}(E/Q)),
\]

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 \( p \mid 2N \) of good ordinary reduction for \( E \). Let \( K \) be an imaginary quadratic field satisfying (spl), and let \( K_{\infty}^{+} \) be the cyclotomic \( \mathbb{Z}_{p} \)-extension of \( K \). Following Greenberg [Gre89], we define the ordinary Selmer group of \( E \) over \( K_{\infty}^{\pm} \) by

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

where \( A_{w} := \text{im} \{ E[p^{\infty}] \to E[p^{\infty}] \}_{\text{div}}, \) with \( E[p^{\infty}] \) the kernel of the reduction map at \( p \), and \( I_{w} \subset G_{K_{\infty}^{\pm,w}} \) 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

\[
L_{p}^{\text{PR}}(E/K) \in \Lambda_{K} := \mathbb{Z}_{p}[[\text{Gal}(K_{\infty}^{+}/K)]],
\]

where \( K_{\infty}/K \) 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 \( \chi \) runs over the finite orders characters of \( \Gamma_{K} \).

The action of complex conjugation yields a decomposition \( \Gamma_{K} \simeq \Gamma^{+} \times \Gamma^{-} \) into \( \pm \)-eigenspaces, with \( \Gamma^{+} \) (resp. \( \Gamma^{-} \)) identified with the Galois group of the cyclotomic (resp. anticyclotomic) \( \mathbb{Z}_{p}^{2} \)-extension of \( K \). Denoting by \( L_{p}^{\text{PR}}(E/K)^{\pm} \) the image of \( L_{p}^{\text{PR}}(E/K) \) under the natural projection

\[
\Lambda_{K} \to \Lambda^{\pm} := \mathbb{Z}_{p}[[\text{Gal}(K_{\infty}^{\pm}/K)]] \approx \Lambda.
\]

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

\[
\text{char}_{\Lambda^{\ast}}(X(E/K_{\infty}^{\ast})) \overset{?}{=} (L_{p}^{\text{PR}}(E/K)^{\ast}).
\]

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

\[
\text{char}_{\Lambda^{+}}(X(E/K_{\infty}^{+})) \supset (L_{p}^{\text{PR}}(E/K)^{+}),
\]

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

\[
\mathcal{F}(E/K_{\infty}^{+})(0) \sim_{p} L_{p}^{\text{PR}}(E/K)^{+}(0),
\]

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 \( L_{p}^{\text{PR}}(E/K)^{+}(0) \neq 0.\)
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 \( L_v^{BDP}(E/K)(0) \neq 0 \), 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

\[
\alpha : \Gamma^- \to \mathbb{Z}_p^* 
\]

with \( \alpha \equiv 1 \pmod{p^M} \), for some \( M \gg 0 \) to stay away from any problematic zeroes; in particular, so that \( L_v^{BDP}(E/K)(\alpha) \neq 0 \). 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 \( p \)-indistinquished), and their explicit reciprocity laws, one can deduce from Theorem 2.1 a proof of the \( \alpha \)-twisted variant of conjecture (14) for \( K_\infty/K \):

\[
(17) \quad \text{char}_{A^+}(X(E(\alpha)/K_\infty^+)) \equiv (L_p^{PR}(E(\alpha)/K)^+). 
\]

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

\[
\text{char}_{A^+}(X(E(\alpha)/K_\infty^+)) \equiv \text{char}_{A^+}(X(E/K_\infty^+)) \pmod{p^M},
\]

\[
L_p^{PR}(E(\alpha)/K)^+ \equiv L_p^{PR}(E/K)^+ \pmod{p^M},
\]

it implies the equalities

\[
\mu(X(E(\alpha)/K_\infty^+)) = \mu(L_p^{PR}(E/K)^+), \quad \lambda(X(E/K_\infty^+)) = \lambda(L_p^{PR}(E/K)^+)
\]

(in particular, without knowing the specific value of the \( \mu \)-invariants!). Together with the integral divisibility (15), these equalities yield the proof of conjecture (14) for \( K_\infty/K \), 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 \( E_*/\mathbb{Q} \) is the same isogeny class constructed by Wüthrich [Wut14]. This can be characterized as the elliptic curve whose \( p \)-adic Tate module \( T_{p}E_* \) agrees with the geometric lattice in the \( p \)-adic representation \( V_f \) realized as the maximal quotient of \( H^1_{\text{et}}(Y_1(N)_{\overline{\mathbb{Q}}}, \mathbb{Q}_p(1)) \) on which the Hecke operators acts with the same eigenvalues as \( f \).

Let \( H^1_{Iw}(K_\infty, T_pE_*) \) be the Iwasawa cohomology for the \( \mathbb{Z}_p^2 \)-extension \( K_\infty/K \), which by Shapiro’s lemma can be identified with \( H^1(K, T_pE_* \otimes_{\mathbb{Z}_p} \Lambda_K) \). 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

\[
\text{BF}_\alpha \in H^1_{Iw}(K_\infty, T_pE_*(\alpha))
\]

together with two explicit reciprocity laws:

1. At the prime \( v \), the class \( \text{BF}_\alpha \) naturally lands in the subspace \( H^1(K_v, T_v^+E_*(\alpha)) \) and there is a generalized Coleman power series map

\[
\text{Col}_v : H^1_{Iw}(K_{\infty,v}, T_p^+E_*(\alpha)) \to \mathbb{Z}_p^ur \otimes_{\mathbb{Z}_p} \Lambda_K
\]

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

\[
(L_v^{Gr}(f(\alpha)/K)^-) = (L_v^{BDP}(f(\alpha)/K)^2),
\]

where \( L_v^{BDP}(f(\alpha)/K) \) is the twist of \( L_v^{BDP}(f(\alpha)/K) \) by the anticyclotomic character \( \alpha \).

2. At the prime \( \mathfrak{p} \), there is a generalized Coleman power series map

\[
\text{Col}_{\mathfrak{p}} : H^1_{Iw}(K_{\infty,\mathfrak{p}}, T_p^-E_*(\alpha)) \to \Lambda_K,
\]

where \( T_p^-E_*(\alpha) := T_pE_*(\alpha)/T_p^+E_*(\alpha) \), sending the natural image of \( \text{BF}_\alpha \) to \( L_p^{PR}(E(\alpha)/K) \).
The cyclotomic projection $BF^+_\alpha \in H^1_{Iw}(K_\infty^+, T_pE_\bullet(\alpha))$ is the base class of a cyclotomic Euler system for $T_pE_\bullet(\alpha)$, and for a suitable choice of $\alpha$ 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 $X_{ord, str}(E_\bullet(\alpha)/K_\infty^+)$ (dual to the compact Selmer group $Sel_{ord, rel}(K_\infty^+, T_pE_\bullet(\alpha))$ on which the class $BF^+_\alpha$ lives) is $\Lambda^+$-torsion, with characteristic ideal satisfying the divisibility

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

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

\[
\begin{array}{ccc}
H^1_{Iw}(K_\infty^+, T_pE_\bullet(\alpha)) & \xrightarrow{\text{res}_v} & X(E_\bullet(\alpha)/K_\infty^+) \\
\text{Sel}_{ord, rel}(K_\infty^+, T_pE_\bullet(\alpha)) & \xrightarrow{\text{res}_v} & X_{ord, str}(E_\bullet(\alpha)/K_\infty^+) \\
\Lambda^+ \cdot \text{res}_v(BF^+_\alpha) & \xrightarrow{\text{res}_v} & H^1_v(K_\infty^+, T_pE_\bullet(\alpha)) \\
\Lambda^+ \cdot \text{res}_v(BF^+_\alpha) & \xrightarrow{\text{res}_v} & X_v(E_\bullet(\alpha)/K_\infty^+) \\
\end{array}
\]

this translates into the divisibilities

(18) $\text{char}_{\Lambda^+}(X(E_\bullet(\alpha)/K_\infty^+)) \supset \text{char}_{\Lambda^+} \left( \frac{H^1_{Iw}(K_\infty^+, T_pE_\bullet(\alpha))}{\Lambda^+ \cdot \text{res}_v(BF^+_\alpha)} \right) = (L^\text{pr}(E_\bullet(\alpha)/K)^+)$

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

(19) $\text{char}_{\Lambda^+}(X_v(E_\bullet(\alpha)/K_\infty^+)) \supset \text{char}_{\Lambda^+} \left( \frac{H^1_{Iw}(K_\infty^+, T_pE_\bullet(\alpha))}{\Lambda^+ \cdot \text{res}_v(BF^+_\alpha)} \right) \Lambda^+ = (L^\text{Gr}(E_\bullet(\alpha)/K)^+)$,

similarly using the explicit reciprocity law at $v$. Further choosing $\alpha$ so that $L^\text{BDP}(f/K)(0) \neq 0$ (as is possible by the nonvanishing of $L^\text{BDP}(f/K)$ as an element in $\Lambda^\text{ur}$), 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).

\section*{References}


