LECTURES ON THE IWASAWA THEORY OF ELLIPTIC CURVES

CHRISTOPHER SKINNER

Abstract. These are a preliminary set ot notes for the author's lectures for the 2018 Arizona Winter School on Iwasawa Theory.

Contents

1. Introduction 2
2. Selmer groups 3
2.1. Selmer groups of elliptic curves 3
2.2. Bloch–Kato Selmer groups 9
2.3. Selmer structures 12
3. Iwasawa modules for elliptic curves 13
3.1. The extension F_∞/F 13
3.2. Selmer groups over F_∞ 15
3.3. $S_?(E/F_\infty)$ as a Λ-module 17
3.4. Control theorems 19
4. Main Conjectures 22
4.1. p-adic L-functions 23
4.2. The Main Conjectures 27
4.3. Main Conjectures without L-functions 28
5. Theorems and ideas of their proofs 30
5.1. Cyclotomic Main Conjectures: the ordinary case 30
5.2. The Main Conjectures for $S_{\mathrm{Gr}}(E/K_\infty)$ and $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ 32
5.3. Cyclotomic Main Conjectures: the supersingular case 34
5.4. Perrin-Riou's Heegner point Main Conjecture 35
6. Arithmetic consequences 36

6.1. Results when $L(E,1) \neq 0$ 36
6.2. Results when $L(E,1) = 0$ 36
6.3. Results when $\mathrm{ord}_{s=1} L(E,s) = 1$ 37
6.4. Converses to Gross–Zagier/Kolyvagin 39
References 40

1. Introduction

Iwasawa theory was introduced around 1960 in the context of class groups of cyclotomic and other $\mathbb{Z}_p$-extensions of number fields. The Main Conjecture of Iwasawa theory proposed a remarkable connection between the p-adic L-functions of Kubota and Leopoldt and these class groups [19, §1], [12, §5], including among its consequences certain refined class number formulas for values of Dirichlet L-functions. This Main Conjecture was proved by Mazur and Wiles [47] in the early 1980's.

Beginning with work of Mazur and Swinnerton-Dyer [45] in the 1970's and especially in subsequent papers of Greenberg [20] [21] [22], the ideas of Iwasawa theory were extended to elliptic curves and – having been suitably recast in the language of Selmer groups – other p-adic Galois representations. Each instance has its own Main Conjecture (at least conjecturally!) relating certain Galois cohomology groups (the algebraic side) with p-adic L-functions (the analytic side). And like the original Main Conjecture of Iwasawa, these Main Conjectures have consequences for the (expected) related special value formulas. In the case of an elliptic curve E this can include the p-part of the Birch–Swinnerton-Dyer formula when the analytic rank is at most one.

The aim of these lectures is to describe the Iwasawa theory of elliptic curves, stating the associated Main Conjectures and reporting on some of the progress that has been made toward proving these conjectures and especially some of the arithmetic consequences.

Prerequisites. These notes are prepared with the expectation that the reader will have a solid background in algebraic number theory and be comfortable with Galois cohomology and Tate's duality theorems ([49, I] is a good reference for the latter). These notes focus on the case of elliptic curves, but this course was chosen with the expectation that the reader will be more comfortable with this case than with that of a general eigenform and because this is probably the case of most interest (and it also simplifies some notation). While very little specific to elliptic curves is used, it could also be helpful to have a familiarity with their basic arithmetic ([61] would be more than sufficient).

Additional readings for details. Those seeking more details should be able to easily find some in the literature. In particular, in addition to the earlier cited papers of Greenberg, [23], [24], and [25] contain a wealth of foundational material (and many examples). Kato's paper [33] is an introduction to the circle of ideas carried out in [34] for elliptic curves and modular forms, while [59], [60], and [14] help illuminate aspects of [34]. However, for details of the proofs of many of the more recent results (such as [64]) the best current resources may be the original papers themselves.

Some notational preliminaries. We let $\overline{\mathbb{Q}}$ be a fixed separable algebraic closure of $\mathbb{Q}$. Given a subfield $F \subset \overline{\mathbb{Q}}$ we let $G_F = \mathrm{Gal}(\overline{\mathbb{Q}}/F)$. For a set Σ of places of F, we write $G_{F,\Sigma}$ for the Galois group $\mathrm{Gal}(F_\Sigma/F)$ of the maximal extension $F_\Sigma \subset \overline{\mathbb{Q}}$ of F that is unramified outside Σ. If $F = \mathbb{Q}$ then we may drop the subscript '$\mathbb{Q}$' from our notation (writing G_Σ for $G_{\mathbb{Q},\Sigma}$). For a place v of F we let $\overline{F}_v$ be a separable algebraic closure of the completion F_v and let $G_{F_v} = \mathrm{Gal}(\overline{F}_v/F_v)$. We let $I_v \subset G_{F_v}$ be the inertia subgroup and, when the residue field of F_v is finite, $\mathrm{Frob}_v \in G_{F_v}/I_v$ an arithmetic Frobenius. Generally, we will assume that we have chosen an F-embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{F}_v$, which identifies G_{F_v} as a subgroup of G_F.

We fix conventions for the reciprocity laws of class field theory as follows: For a number field F and a place v of F we let $\mathrm{rec}_{F_v} : F_v^\times \to G_{F_v}^{ab}$ be the reciprocity map of local class field theory, normalized so that uniformizers map to lifts of the arithmetic Frobenius. Similarly, we let $\mathrm{rec}_F : F^\times \backslash \mathbb{A}_F^\times \to G_F^{ab}$ be the reciprocity map of global class field theory, normalized so that $\mathrm{rec}_F|_{F_v^\times} = \mathrm{rec}_{F_v}$.

Throughout, p is a prime number (usually assumed > 2). We let $\epsilon : G_\mathbb{Q} \to \mathbb{Z}_p^\times$ be the p-adic cyclotomic character.

At times it will be useful to view elements of $\overline{\mathbb{Q}}$ as both complex numbers and p-adic numbers. To this end we fix embeddings $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ which will be tacitly in use in all that follows.

Finally, one last bit of general notation about modules: Suppose M is a module for a ring R. If $\phi : M \to M$ is an R-linear endomorphism of M, then we write $M[\phi]$ to mean the kernel of ϕ. A commonly used variation of this will be to write $M[r]$ for $M[\phi]$ when ϕ is just the multiplication by r map.

Acknowledgments. It is a pleasure to thank all those who provided feedback and corrections to these notes, particulary Francesc Castella – who carefully read earlier drafts – as well as Kim Tuan Do. The author's work has been supported by grants from the National Science Foundation and a Simons Investigator grant.

2. Selmer groups

We begin by recalling the usual Selmer groups of an elliptic curve as well as some generalizations.

2.1. Selmer groups of elliptic curves.

Let E be an elliptic curve over a number field F.

2.1.1. *The Weak Mordell–Weil Theorem.* One of the fundamental results about the arithmetic of E is the celebrated theorem of Mordell and Weil:

$$E(F) \text{ is a finitely-generated abelian group.}$$

An important step in the proof of this theorem is the Weak Mordell–Weil Theorem: for any positive integer $m \geq 2$, $E(F)/mE(F)$ is a finite group. This yields the Mordell–Weil Theorem when combined with the theory of heights on elliptic curves, especially Tate's canonical height.

The Weak Mordell–Weil Theorem is generally proved by realizing $E(F)/mE(F)$ as a subgroup of another group that is more readily recognized as having finite order. This makes use of the Kummer map for elliptic curves. Let $P \in E(F)$ be a point and let $Q \in E(\overline{F})$ be a point such that $mQ = P$. The map $\phi_Q : G_F \to E[m]$, $\sigma \mapsto \sigma(Q) - Q$, is a 1-cocycle. Let $c_P = [\phi_Q]$ be

the class of ϕ_Q in the Galois cohomology group $H^1(F, E[m])$. If Q' is another point such that $mQ' = P$, then the difference $\phi_Q - \phi_{Q'}$ is a coboundary, so c_P depends only on P. The map $E(F) \to H^1(F, E[m])$, $P \mapsto c_P$, is clearly a homomorphism. A point $P \in E(F)$ is in the kernel of this homomorphism if and only if c_P is a coboundary, that is, if and only if there exists $R \in E[m]$ such that $\sigma(Q) - Q = \sigma(R) - R$ for all $\sigma \in G_F$. But this is so if and only if $\sigma(Q - R) = Q - R$ for all $\sigma \in G_F$, and so if and only if $Q - R \in E(F)$. But then $P = m(Q - R) \in mE(F)$. This shows that there is in fact an injection

$$E(F)/mE(F) \overset{\kappa}{\hookrightarrow} H^1(F, E[m]), \quad \kappa(P) = c_P.$$

The map κ is the Kummer map for the multiplication by m endomorphism of E. It is just the boundary map in the long exact Galois cohomology sequence associated with the short exact sequence $0 \to E[m] \to E \overset{m}{\to} E \to 0$. However, we have not yet achieved what we wanted: the group $H^1(F, E[m])$ is infinite. We seem to have gone in the wrong direction! To finish the proof of the Weak Mordell–Weil Theorem one makes a closer analysis of the image of κ.

Let v be a finite place of F not dividing m and such that E has good reduction at v. This only excludes a finite subset Σ of all the places of F. Let k_v be the residue field of v and let ℓ be the characteristic of k_v. Let $\overline{E}$ be the reduction of E modulo v; this is an elliptic curve over k_v. As $\ell \nmid m$, the reduction map is an isomorphism on m-torsion: $E[m] \overset{\sim}{\to} \overline{E}[m]$. Let $\sigma \in I_v$. Then σ acts trivially on $\overline{E}$ and so $\sigma(Q)$ and Q have the same image in $\overline{E}$. In particular, $\sigma(Q) - Q$ reduces to the origin in $\overline{E}$. But $\sigma(Q) - Q \in E[m]$ and so it follows from the injectivity of the reduction map on $E[m]$ that $\sigma(Q) - Q = 0$. In particular, the restriction of c_Q to the inertia group I_v is a coboundary. This means that the image of κ is contained in

$$\ker \left\{ H^1(F, E[m]) \overset{res}{\to} \prod_{v \notin \Sigma} H^1(I_v, E[m]) \right\},$$

the kernel of the product of the restriction maps to the inertia subgroups of all the places v not in the finite set Σ. Another way of writing this kernel is $H^1(G_{F,\Sigma}, E[m])$. So we have

$$E(F)/mE(F) \overset{\kappa}{\hookrightarrow} H^1(G_{F,\Sigma}, E[m]), \quad \kappa(P) = c_P.$$

This is better: the group $H^1(G_{F,\Sigma}, E[m])$ is finite (and hence $E(F)/mE(F)$ is also finite). The finiteness of $H^1(G_{F,\Sigma}, E[m])$ can be seen as follows. Let $L = F(E[m]) \subset F_\Sigma$ be the finite Galois extension of F obtained by adjoining the coordinates of points in $E[m]$. The inflation restriction sequence gives a left-exact sequence

$$0 \to H^1(\mathrm{Gal}(L/F), E[m]^{G_L}) \to H^1(G_{F,\Sigma}, E[m]) \overset{res}{\to} H^1(\mathrm{Gal}(F_\Sigma/L), E[m]).$$

The group $H^1(\mathrm{Gal}(L/F), E[m]^{G_L})$ is clearly finite (as both $\mathrm{Gal}(L/F)$ and $E[m]$ are finite groups). Since $\mathrm{Gal}(F_\Sigma/L)$ acts trivially on $E[m]$, $H^1(\mathrm{Gal}(F_\Sigma/L), E[m]) = \mathrm{Hom}(\mathrm{Gal}(F_\Sigma/L), E[m])$. Any element of $\mathrm{Hom}(\mathrm{Gal}(F_\Sigma/L), E[m])$ factors through the Galois group over L of the maximal abelian extension of L of exponent m that is unramified outside the finitely many places of L dividing a place in Σ. This extension is finite, and hence so is $\mathrm{Hom}(\mathrm{Gal}(F_\Sigma/L), E[m])$. We have sandwiched $H^1(G_{F,\Sigma}, E[m])$ between two finite groups.

By realizing $E(F)/mE(F)$ as a subgroup of $H^1(G_{F,\Sigma}, E[m])$ we reduced its finiteness to the ostensibly easier problem of the finiteness of certain extensions of number fields. This demonstrates one utility of cohomology groups.

2.1.2. *The Selmer group for multiplication by m.* The Selmer group for the multiplication by m map on E refines the inclusion $E(F)/mE(F) \hookrightarrow H^1(G_{F,\Sigma}, E[m])$. It is essentially the smallest subgroup of $H^1(F, E[m])$ containing the image of $E(F)/mE(F)$ that can be defined by more-or-less obvious local constraints ('local conditions') on the cohomology classes.

The Kummer map $P \overset{\kappa}{\mapsto} c_P$ that we recalled earlier makes sense for E over any field and in particular over the completion F_v of F at a place of F.

For each place v of F the inclusion of F in the completion F_v induces a commutative diagram

$$\begin{array}{ccc} E(F)/mE(F) & \xrightarrow{\kappa} & H^1(F, E[m]) \\ \downarrow & & \downarrow res \\ E(F_v)/mE(F_v) & \xrightarrow{\kappa_v} & H^1(F_v, E[m]), \end{array}$$

where κ_v is just the Kummer map for E over F_v. The Selmer group $\mathrm{Sel}_m(E/F)$ for the multiplication by m on E is

$$\mathrm{Sel}_m(E/F) = \left\{ c \in H^1(F, E[m]) \ : \ res_v(c) \in \mathrm{im}(\kappa_v) \ \forall v \right\}.$$

This clearly contains the image of κ. Furthermore, by the argument explained above, if v does not divide m and E has good reduction at v then $\mathrm{im}(\kappa_v) \subset \ker\left\{ H^1(F_v, E[m]) \overset{res}{\to} H^1(I_v, E[m]) \right\}$. In particular, $\mathrm{Sel}_m(E/F) \subseteq H^1(G_{F,\Sigma}, E[m])$.

The maps κ and κ_v are part of short exact sequences

$$0 \to E(F)/mE(F) \overset{\kappa}{\to} H^1(F, E[m]) \to H^1(F, E)[m] \to 0$$

and

$$0 \to E(F_v)/mE(F_v) \overset{\kappa_v}{\to} H^1(F_v, E[m]) \to H^1(F_v, E)[m] \to 0$$

that come from the long exact Galois cohomology sequences associated with the short exact sequence $0 \to E[m] \to E \overset{m}{\to} E \to 0$. In particular, we can rewrite the definition of $\mathrm{Sel}_m(E/F)$ as

$$\mathrm{Sel}_m(E/F) = \ker\left\{ H^1(F, E[m]) \overset{res}{\to} \prod_v H^1(F_v, E) \right\}.$$

And we see that the image of κ is just $\ker\left\{ \mathrm{Sel}_m(E/F) \to H^1(F, E) \right\}$. In particular, there is a fundamental exact sequence

$$0 \to E(F)/mE(F) \overset{\kappa}{\to} \mathrm{Sel}_m(E/F) \to Ш(E/F)[m] \to 0,$$

where

$$Ш(E/F) = \ker\left\{ H^1(F, E) \overset{res}{\to} \prod_v H^1(F_v, E) \right\}$$

is the Tate-Shafarevich group of E over F.

If $m \mid m'$ then the inclusion $E[m] \subset E[m']$ induces a surjection $H^1(F, E[m]) \twoheadrightarrow H^1(F, E[m'])[m]$ and so a surjection $\mathrm{Sel}_m(E/F) \to \mathrm{Sel}_{m'}(E/F)[m]$. The kernel is just $E[\frac{m'}{m}](F)/mE[m'](F)$. If F'/F is a finite extension, then the restriction map $H^1(F, E[m]) \to H^1(F', E[m])$ induces a homomorphism $\mathrm{Sel}_m(E/F) \to \mathrm{Sel}_m(E/F')$. Furthermore, if F'/F is a Galois extension, then the action of $\mathrm{Gal}(F'/F)$ on $H^1(F', E[m])$ defines an action on $\mathrm{Sel}_m(E/F')$, and the maximal $\mathrm{Gal}(F'/F)$-fixed subgroup contains the image of $\mathrm{Sel}_m(E/F)$.

Remark 2.1.2.a. Suppose that $m = p$. It is expected that $Ш(E/F)[p^\infty]$ is finite, in which case it is known that $Ш(E/F)[p]$ has even dimension as a vector space over $\mathbb{F}_p$. It then follows from the fundamental exact sequence that

$$\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/F) \equiv \dim_{\mathbb{F}_p} E(F)/pE(F) \bmod 2.$$

In particular, if $\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/F) = 1$, then is expected that $\dim_{\mathbb{F}_p} E(F)/pE(F) = 1$. If $\dim_{F_p} E(F)/pE(F) = 1$ but $E[p](F) = 0$, then $\mathrm{rank}_{\mathbb{Z}} E(F) = 1$. This suggests

$$(\dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/F) = 1 \text{ and } E[p](F) = 0) \overset{?}{\Longrightarrow} \mathrm{rank}_{\mathbb{Z}} E(F) = 1.$$

2.1.3. *Vista: Selmer groups of Abelian varieties and their isogenies.* The group $\mathrm{Sel}_m(E/F)$ is a special case of a definition that can be made for any non-zero isogeny

$$A \overset{\phi}{\to} B$$

of abelian varieties over F. The natural generalization of the Kummer map yields an injection $A(F)/\phi(B(F)) \hookrightarrow H^1(F, A[\phi])$, which leads to the definition of a Selmer group $\mathrm{Sel}_\phi(A/F) \subset H^1(G_{F,\Sigma}, A[\phi])$ (for Σ containing all places that divide $\#A[\phi]$ and at which A – and so also B – has bad reduction). These Selmer groups play an equally important role in our understanding of the arithmetic of the abelian varieties A and B.

Elliptic curves can have isogenies that are not just multiplication by an integer m. For example, if E has an F-rational point $P \in E[m]$, then the quotient map $E \to E' = E/\langle P \rangle$ is an isogeny. And if E is an elliptic curve with complex multiplication by an order in an imaginary quadratic field K contained in F, then E will have many F-rational endomorphisms that are not just multiplication by an integer. The Selmer groups for these endomorphisms have featured prominently in most efforts to understand the arithmetic of elliptic curves with complex multiplication, such as the Coates–Wiles theorem [13] or Rubin's proof of the first known cases of elliptic curves with a finite Tate-Shafarevich group [57].

2.1.4. *The p^∞-Selmer group.* The p^∞-Selmer group of E is obtained by taking the direct limits over n of the p-power Selmer groups $\mathrm{Sel}_{p^n}(E/F)$:

$$\mathrm{Sel}_{p^\infty}(E/F) = \varinjlim_n \mathrm{Sel}_{p^n}(E/F).$$

Since $\varinjlim_n H^1(F, E[p^n]) = H^1(F, E[p^\infty])$ the p^∞-Selmer group can also be directly defined as

$$\mathrm{Sel}_{p^\infty}(E/F) = \ker \left\{ H^1(F, E[p^\infty]) \overset{res}{\to} \prod_v H^1(F_v, E) \right\}.$$

The natural surjection $H^1(F, E[p^n]) \twoheadrightarrow H^1(F, E[p^\infty])[p^n]$ induces a surjection $\mathrm{Sel}_{p^n}(E/F) \twoheadrightarrow \mathrm{Sel}_{p^\infty}(E/F)[p^n]$ with kernel $E[p^\infty](F)/p^n E[p^\infty](F)$.

Taking the direct limit over the fundamental exact sequences for the multiplication by p^n maps yields the fundamental exact sequence for the p^∞-Selmer groups:

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

Remark 2.1.4.b. The group $Ш(E/F)[p^\infty]$ is expected to be finite, in which case it follows from the fundamental exact sequence for $\mathrm{Sel}_{p^\infty}(E/F)$ that

$$\mathrm{rank}_{\mathbb{Z}} E(F) \overset{?}{=} \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/F),$$

the $\mathbb{Z}_p$-corank of a discrete module S being the $\mathbb{Z}_p$-rank of its Pontryagin dual $\mathrm{Hom}_{cts}(S, \mathbb{Q}_p/\mathbb{Z}_p)$.

2.1.5. *The p^∞-Selmer group in terms of $E[p^\infty]$ only.* The p^∞-Selmer group of E can be defined solely in terms of the p-divisible group $E[p^\infty]$. We start by noting that if $v \nmid p$, then $\varinjlim_n E(F_v)/p^nE(F_v) = E(F_v)\otimes\mathbb{Q}_p/\mathbb{Z}_p = 0$. The key point here is that $E(F_v)/p^nE(F_v)$ has order either 1 or 2 if $v \mid \infty$ and if $v \nmid \infty$ then $E(F_v)$ contains a pro-ℓ-subgroup of finite index, where ℓ is the residue characteristic of v. It follows that the local condition at v defining a class in $\mathrm{Sel}_{p^\infty}(E/F)$ is just that its restriction to $H^1(F_v, E[p^\infty])$ is 0. If in addition v is a prime of good reduction, then the kernel of the restriction map $H^1(F_v, E[p^\infty]) \to H^1(I_v, E[p^\infty])$ is $H^1(G_{F_v}/I_v, E[p^\infty]) \cong E[p^\infty]/(\mathrm{Frob}_v - 1)E[p^\infty] = 0$ (since $E[p^\infty]$ is divisible and 1 is not an eigenvalue for the action of Frob_v on the p-adic Tate module of the elliptic curve E/k_v). So for such v, vanishing in $H^1(F_v, E[p^\infty])$ is equivalent to vanishing in $H^1(I_v, E[p^\infty])$, that is, the local condition at v defining a class in $\mathrm{Sel}_{p^\infty}(E/F)$ can also be expressed as the class being unramified at v. Already, this means

$$\begin{aligned}\mathrm{Sel}_{p^\infty}(E/F) &= \ker\left\{H^1(F, E[p^\infty]) \overset{res}{\to} \prod_{v\nmid p} H^1(F_v, E[p^\infty]) \times \prod_{v\mid p} H^1(F_v, E)\right\}\\ &= \ker\left\{H^1(G_{F,\Sigma}, E[p^\infty]) \overset{res}{\to} \prod_{v\in\Sigma, v\nmid p} H^1(F_v, E[p^\infty]) \times \prod_{v\mid p} H^1(F_v, E[p^\infty])/\mathrm{im}(\kappa_v)\right\}.\end{aligned}$$

The situation for $v \mid p$ is more complicated. We want to express $\mathrm{im}(\kappa_v)$ in terms of $E[p^\infty]$ only (without reference to the full curve E). Let $T = T_pE = \varprojlim_n E[p^n]$ be the p-adic Tate-module of E (really just of the p-divisible group $E[p^\infty]$). Note that there is a canonical isomorphism $T_pE \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \overset{\sim}{\to} E[p^\infty]$ (given by $(P_n)\otimes\frac{1}{p^m} \mapsto P_m$).

Suppose first that E has good ordinary or multiplicative reduction at v. Then T has a G_{F_v}-filtration $0 \subset T_v^+ \subset T$ with T_v^+ a rank-one $\mathbb{Z}_p$-summand such that T/T_v^+ is unramified with Frob_v acting as multiplication by the unit root α_p of $x^2 - a_v(E)x + p$ (if E has good reduction at v) or by $a_v(E)$ (if E has multiplicative reduction at v). Then

$$\begin{aligned}\mathrm{im}(\kappa_v) &= \mathrm{im}\left\{H^1(F_v, T_v^+\otimes\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(F_v, E[p^\infty])\right\}_{\mathrm{div}}\\ &= \ker\left\{H^1(F_v, E[p^\infty]) \to H^1(F_v, T/T_v^+ \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p)\right\}_{\mathrm{div}},\end{aligned}$$

where the subscript 'div' denotes the maximal divisible subgroup. In the case of good reduction, the divisible subgroup is the whole group unless $a_v(E) \equiv 1 \bmod p$ (the index of the divisible subgroup is $\#\mathbb{Z}_p/(\alpha_p - 1)\mathbb{Z}_p$). In the case of split multiplicative reduction, the divisible subgroup is everything. In the case of non-split multiplicative reduction, the divisible subgroup is everything if $p > 2$, and if $p = 2$ then the index of the divisible subgroup is either 1 or 2 (and equals the 2-part of the Tamagawa factor for E/F_v). All this follows from analyzing $E[p^\infty]$ and its cohomology using the formal group when E has good reduction at v and using the Tate parameterization in the cases of multiplicative reduction.

More generally, Bloch and Kato [5, Ex. 3.11] described the image of κ_v, $v \mid p$, in a manner that also covers the cases of supersingular and additive reduction. Let $V = T\otimes\mathbb{Q}_p$. This is a two-dimensional $\mathbb{Q}_p$-representation of G_F. Note that $V/T = T\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p \overset{\sim}{\to} E[p^\infty]$. Letting

$$H^1_f(F_v, V) = \ker\left\{H^1(F_v, V) \to H^1(F_v, V\otimes_{\mathbb{Q}_p} B_{\mathrm{cris}})\right\},$$

they show that

$$\mathrm{im}(\kappa_v) = \mathrm{im}\left\{H^1_f(F_v, V) \to H^1(F_v, E[p^\infty])\right\}.$$

It is a good exercise of one's understanding of basic p-adic Hodge theory to deduce the description of $\mathrm{im}(\kappa_v)$ given above in the cases of ordinary and multiplicative reduction from that of Bloch and Kato.

Remark 2.1.5.c. The question of whether the Selmer group $\mathrm{Sel}_{p^n}(E/F)$ is determined by the Galois module $E[p^n]$ has been studied by Česnavičius [11]; a positive answer is given in terms of flat cohomology under mild conditions on p.

2.1.6. *Selmer groups and The Birch–Swinnerton-Dyer Conjecture.* As already noted, the Selmer groups $\mathrm{Sel}_m(E/F)$ and $\mathrm{Sel}_{p^\infty}(E/F)$ encapsulate information about the Mordell–Weil group $E(F)$ and the Tate–Shafarevich group $Ш(E/F)$. Information about both these groups should also be encoded in the L-function $L(E/F,s)$ of E, as explained in the Birch–Swinnerton-Dyer Conjecture. Combining this we can extract some expected connections between $L(E/F,s)$ and Selmer groups of E.

The Birch and Swinnerton-Dyer Conjecture, as stated by Tate [68]:

Conjecture 1 (Birch and Swinnerton-Dyer Conjecture)**.** *Let F be a number field and let E/F be an elliptic curve.*

(a) *The Hasse–Weil L-function $L(E/F,s)$ has analytic continuation to the entire complex plane and*

$$\mathrm{ord}_{s=1}L(E/F,s) = \mathrm{rk}_{\mathbb{Z}}\, E(F). \tag{BSD}$$

(b) *The Tate–Shafarevich group $Ш(E/F)$ has finite order, and*

$$\frac{L^{(r)}(E/F,1)}{r!\cdot \Omega_{E/F}\cdot \mathrm{Reg}(E/F)\cdot |\Delta_F|^{-1/2}} = \frac{\#Ш(E/F)\cdot \prod_{v\nmid\infty} c_v(E/F)}{(\#E(F)_{\mathrm{tors}})^2}, \tag{BSD-f}$$

where $r=\mathrm{ord}_{s=1}L(E/F,s)$, $c_v(E/F)=[E(F_v):E^0(F_v)]$ is the Tamagawa number at v for a finite place v of F, $\mathrm{Reg}(E/F)$ is the regulator of the Néron-Tate height pairing on $E(F)$, Δ_F is the discriminant of F, and $\Omega_{E/F}\in\mathbb{C}^\times$ is the period defined by

$$\Omega_{E/F} = \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{a}_\omega)\cdot \prod_{\substack{v|\infty\\ v\text{-real}}} \int_{E(F_v)} |\omega| \cdot \prod_{\substack{v|\infty\\ v\text{-complex}}} \left(2\cdot \int_{E(F_v)} \omega\wedge\overline{\omega}\right). \tag{Ω}$$

Here $\omega\in\Omega^1(\tilde{E}/\mathcal{O}_F)$ is any non-zero differential on the Néron model $\tilde{E}$ of E over $\mathcal{O}_F$, and $\mathfrak{a}_\omega\subset F$ is the fractional ideal such that $\mathfrak{a}_\omega\cdot\omega=\Omega^1(\tilde{E}/\mathcal{O}_F)$. Also, for a finite place v, $E^0(F_v)\subset E(F_v)$ denotes the subgroup of local points that specialize to the identity component of the Néron model of E at the place v.

When $F=\mathbb{Q}$ we will write Ω_E for $\Omega_{E/\mathbb{Q}}$.

As already noted, the finiteness of $Ш(E/F)$ (or even of just the p-primary part $Ш(E/F)[p^\infty]$) implies that the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/F)$ equals the rank of $E(F)$. So one expects

$$\mathrm{ord}_{s=1}L(E/F,s) \overset{?}{=} \mathrm{corank}_{\mathbb{Z}_p}\,\mathrm{Sel}_{p^\infty}(E/F). \tag{BSD-crk}$$

This suggests that one might first ask:

$$L(E/F,1)=0 \overset{?}{\iff} \#\mathrm{Sel}_{p^\infty}(E/F)=\infty. \tag{Sel-van}$$

It also suggests the question:

$$\text{(Sel-par)} \qquad \operatorname{ord}_{s=1} L(E/F,s) \equiv \frac{1-w(E/F)}{2} \stackrel{?}{\equiv} \operatorname{corank}_{\mathbb{Z}_p} \operatorname{Sel}_{p^\infty}(E/F) \bmod 2.$$

Here $w(E/F) \in \{\pm 1\}$ is the root number of E/F (the sign of the expected functional equation of $L(E/F)$). If $L^{\mathrm{alg}}(E/F,1) = L(E/F,1)/\Omega_{E/F}|\Delta_F|^{-1/2}$ is a rational number, then a refined form of (Sel-van), incorporating the BSD formula (BSD-f) when $r=0$, is

$$\text{(BSDp-0)} \qquad \left|L^{\mathrm{alg}}(E/F,1)\right|_p \stackrel{?}{=} \left| \frac{\#\operatorname{Sel}_{p^\infty}(E/F) \cdot \prod_{v \nmid \infty} c_v(E/F)}{(\#E(F)_{\mathrm{tors}})^2} \right|_p .$$

Here we understand the right-hand side to equal 0 if $\#\operatorname{Sel}_{p^\infty}(E/F) = \infty$. As explained below, some progress has been made on all these problems (and a few others) for an elliptic curve $E/\mathbb{Q}$.

2.2. **Bloch–Kato Selmer groups.** Bloch and Kato [5] actually defined Selmer groups in a very general setting, starting with a p-adic Galois representation of G_F.

In keeping with our arithmetic conventions for class field theory, we also adopt arithmetic conventions for p-adic Hodge–Tate weights. In particular, the p-adic cyclotomic character has Hodge–Tate weight 1.

2.2.1. *The definition.* Let L be a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}$. Let V be a finite-dimensional L-space equipped with a continuous L-linear action of G_F. We assume that V is a *geometric* representation of G_F. This means that the action of G_F on V is unramified away from a finite set of places and that for each place $v \mid p$ the representation of G_{F_v} on V is potentially semistable (equivalently, de Rham). Let $T \subset V$ be a G_F-stable $\mathcal{O}$-lattice (so in particular, $V = T \otimes_{\mathcal{O}} L$). Such a lattice always exists by a simple compactness argument. Let $W = V/T$. Bloch and Kato defined subgroups (Selmer groups) $H^1_f(F,V) \subset H^1(F,V)$, $H^1_f(F,T) \subset H^1(F,T)$, and $H^1_f(F,W) \subset H^1(F,W)$ as follows.

First they defined local subgroups for a place v of F:

$$H^1_f(F_v,V) = \begin{cases} H^1(\mathrm{Gal}(F_v^{\mathrm{ur}}/F_v), V^{I_v}) = \ker\left\{H^1(F_v,V) \to H^1(I_v,V)\right\} & v \nmid p \\ \ker\left\{H^1(F_v,V) \to H^1(F_v, V \otimes_{\mathbb{Q}_p} B_{\mathrm{cris}})\right\} & v \mid p. \end{cases}$$

The exact sequence $0 \to T \to V \to W \to 0$ yields an exact sequence

$$H^1(F_v,T) \stackrel{i}{\to} H^1(F_v,V) \stackrel{j}{\to} H^1(F_v,W),$$

and $H^1_f(F_v,T)$ and $H^1_f(F_v,W)$ are defined to be

$$H^1_f(F_v,T) = i^{-1}(H^1_f(F_v,V)) \ \text{ and } \ H^1_f(F_v,W) = j(H^1_f(F_v,V)).$$

Note that $H^1_f(F_v,W)$ is L-divisible, being the image of the L-space $H^1_f(F_v,V)$.

The Bloch–Kato Selmer groups are then defined by

$$H^1_f(F,?) = \ker\left\{ H^1(F,?) \stackrel{res}{\to} \prod_v H^1(F_v,?)/H^1_f(F_v,?) \right\}, \quad ? = T, V, \text{ or } W.$$

The Bloch–Kato analog of the Tate–Shafarevich group is

$$Ш_f(W/F) = H^1_f(F,W)/H^1_f(F,W)_{\mathrm{div}},$$

the quotient of $H^1_f(F,W)$ by its maximal divisible subgroup.

2.2.2. *Examples.* We describe some examples, a few of which figure in subsequent results:

Example 2.2.2.a (Elliptic curves: $V = V_pE$). Then $T = T_pE$ is a G_F-stable $\mathbb{Z}_p$-lattice and $W \cong E[p^\infty]$. If $v \nmid p$ then it is relatively easy to see that $H^1_f(F_v, V) = 0$. Then $H^1_f(F_v, W) = 0$, which agrees with $\mathrm{im}(\kappa_v)$. As already noted above, Bloch and Kato proved that $H^1(F_v, W) = \mathrm{im}(\kappa_v)$ even when $v \mid p$. It follows that $H^1_f(F, W) = \mathrm{Sel}_{p^\infty}(E/F)$. The group $Ш_f(E[p^\infty]/F)$ is then the quotient of the p-primary part $Ш(E/F)[p^\infty]$ of the usual Tate–Shafarevich group by its maximal divisible subgroup. In particular, $Ш_f(E[p^\infty]/F)$ equals $Ш(E/F)[p^\infty]$ if and only if the latter is finite.

Example 2.2.2.b (Algebraic Hecke characters). Let $\psi : F^\times \backslash \mathbb{A}_F^\times \to \mathbb{C}^\times$ be an algebraic Hecke character. This means that there exists an algebraic character $\rho : F^\times \to \overline{\mathbb{Q}}^\times$ such that the restriction of ψ to the identity component $(F \otimes \mathbb{R})_1^\times \subset (F \otimes \mathbb{R})^\times$ is given by ρ. Concretely, this is so if and only if there exist $[F : \mathbb{Q}]$ integers $(n_\tau)_\tau$, indexed by the embeddings $\tau : F \hookrightarrow \mathbb{C}$, such that for $\alpha = \sum_i x_i \otimes r_i \in (F \otimes \mathbb{R})_1^\times$, $\psi(\alpha) = \prod_\tau (\sum_i \tau(x_i) r_i)^{n_\tau}$. The character $\mathbb{A}_F^\times \to \mathbb{C}^\times$, $\alpha \mapsto \rho(\alpha_\infty)^{-1}\psi(\alpha)$ takes values in $\overline{\mathbb{Q}}^\times$ (and even in a finite extension of $\mathbb{Q}$). The p-adic Galois character associated with ψ is just

$$\rho_\psi : G_F \to \overline{\mathbb{Q}}_p^\times, \quad \rho_\psi(\sigma) = \rho(x_p)\rho(x_\infty)^{-1}\psi(x) \ \text{ for } \ \sigma = \mathrm{rec}_F(x).$$

Note that if $\psi = |\mathrm{N}_{F/\mathbb{Q}}(\cdot)|_{\mathbb{Q}}^{-1}$, then $\sigma_\psi = \epsilon$, the p-adic cyclotomic character.

Serre proved that $\psi \mapsto \sigma_\psi$ is a bijection between algebraic Hecke characters of F and p-adic characters $\chi : G_F \to \overline{\mathbb{Q}}_p^\times$ that are unramified outside a finite set of places and Hodge–Tate at each $v \mid p$.

The Hodge–Tate weights of ρ_ψ can be read off from the algebraic representation ρ. The simplest case is when p splits completely in F. Then the places of v are indexed by the embeddings τ. In particular, if v is the place determined by the embedding $F \xhookrightarrow{\tau} \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$, then the Hodge–Tate weight of $\sigma_\psi|_{G_{F_v}}$ is $-n_\tau$. Let $n_v = n_\tau$. Let $L \subset \overline{\mathbb{Q}}$ be a finite extension of $\mathbb{Q}_p$ containing the values of ρ_ψ. It follows that in this case

$$H^1_f(F_v, L(\rho_\psi)) = \begin{cases} H^1(F_v, L(\rho_\psi)) & n_v < -1 \\ 0 & n_v > 0. \end{cases}$$

In particular, for $W = L/\mathcal{O}(\rho_\psi)$ with each n_v either > 0 or < -1,

$$H^1_f(F, W) = \ker\left\{ H^1(F, W) \overset{res}{\to} \prod_{v \nmid p} \frac{H^1(F_v, W)}{H^1_f(F_v, W)} \prod_{v \mid p, n_v > 0} H^1(F_v, W) \times \prod_{v \mid p, n_v < -1} \frac{H^1(F_v, W)}{H^1(F_v, W)_{\mathrm{div}}} \right\}.$$

Example 2.2.2.c (Twists of V_pE by characters). Suppose $\chi : G_F \to \overline{\mathbb{Q}}_p^\times$ is a continuous character that is unramified away from finitely many places and Hodge–Tate at all places $v \mid p$. Let $L = \mathbb{Q}_p[\chi]$ be the finite extension of $\mathbb{Q}_p$ obtained by adjoining the values of χ. Then χ takes values in $\mathcal{O}^\times$. Let $V = V_pE \otimes_{\mathbb{Q}_p} L(\chi)$ and $T = T_pE \otimes_{\mathbb{Z}_p} \mathcal{O}(\chi)$ (so if ρ denotes the action of G_F on T_pE, then G_F acts on T as $\rho \otimes \chi$). We then let

$$\mathrm{Sel}(E/F, \chi) = H^1_f(F, W).$$

It will be useful to have a description of $H^1(F_v, V)$, $v \mid p$, in some cases. Suppose first that all the Hodge-Tate weights of $\chi|_{G_{F_v}}$ are zero (equivalently, the restriction $\chi|_{I_v}$ has finite order).

Suppose also that E has good ordinary or multiplicative reduction at v. Then

$$H^1_f(F_v, V) = \ker\left\{H^1(F_v, V) \to H^1(I_v, V/V_v^+)\right\},$$

where V_v^+ is $(V_pE)_v^+ \otimes_{\mathbb{Q}_p} L(\chi)$. It follows that $H^1_f(F_v, W)$ is just the maximal divisible subgroup of $\ker\left\{H^1(F_v, W) \to H^1(I_v, W/W_v^+)\right\}$, where $W_v^+ = T_v^+ \otimes \mathbb{Q}_p/\mathbb{Z}_p$.

If all the Hodge–Tate weights of $\chi|_{G_{F_v}}$ are > 1, then all the Hodge–Tate weights of V at v are > 1 and so $H^1_f(F_v, V) = H^1(F_v, V)$. But if all the Hodge–Tate weights of $\chi|_{G_{F_v}}$ are < -1, then all the Hodge–Tate weights of V at v are < 0 and so $H^1_f(F_v, V) = 0$. Suppose then that for each $v \mid p$ the Hodge–Tate weights of $\chi|_{G_{F_v}}$ are either all > 1 or all < -1, and let $S_p^{\pm}$ denote the set of $v \mid p$ such that the Hodge–Tate weight of χ at v has sign $\pm$. Then

$$H^1_f(F, W) = \ker\left\{H^1(F, W) \overset{res}{\to} \prod_{v\nmid p} \frac{H^1(F_v, W)}{H^1_f(F_v, W)} \times \prod_{v\in S_p^-} H^1(F_v, W) \times \prod_{v\in S_p^+} \frac{H^1(F_v, W)}{H^1(F_v, W)_{\mathrm{div}}}\right\}.$$

In particular, the reduction type of E at v does not really intervene in the description of the Bloch–Kato Selmer groups in this case.

Example 2.2.2.d (Eigenforms). Let $f \in S_k(N, \chi)$ be a newform of weight k, level N, and character χ. Let $f = \sum_{n=0}^{\infty} a_n q^n$ be the q-expansion of f at the cusp at infinity. The coefficients a_n (equivalently, the eigenvalues of the action of the usual Hecke operators on f) are algebraic integers and generate a (possibly non-maximal) order in the ring of integers of the finite extension $\mathbb{Q}(f) \subset \mathbb{C}$ obtained by adjoining the a_n's. Let $L \subset \overline{\mathbb{Q}}_p$ be a finite extension of $\mathbb{Q}_p$ containing the image of $\mathbb{Q}(f)$. Let $\mathcal{O} \subset L$ be the ring of integers of L.

Associated with f and L (and the embedding $\mathbb{Q}(f) \hookrightarrow L$) is a two-dimensional L-space V_f and an absolutely irreducible continuous $G_{\mathbb{Q}}$-representation $\rho_f : G_{\mathbb{Q}} \to \mathrm{Aut}_L(V_f)$ such that ρ_f is unramified at all primes $\ell \nmid Np$ and $\det(1 - X \cdot \rho_f(\mathrm{frob}_\ell)) = 1 - a_\ell X + \chi(\ell)\ell^{k-1}X^2$ for such ℓ. In particular, $\mathrm{trace}\,\rho_f(\mathrm{frob}_\ell) = a_\ell(f)$ if $\ell \nmid pN$, and $\det \rho_f = \chi\epsilon^{k-1}$.

Suppose $k \geq 2$ and $a_p \in \mathcal{O}^\times$. Let $\alpha_p \in \mathbb{Q}^\times$ be the unit root of $x^2 - a_p x + \chi(p)p^{k-1}$ if $p \nmid N$ and otherwise let $\alpha_p = a_p$. Then V has a $G_{\mathbb{Q}_p}$-filtration $V^+ \subset V$, with $\dim_L V^+ = 1$ and $G_{\mathbb{Q}_p}$ acting on V via the character $\epsilon^{k-1}\alpha^{-1}$, where $\alpha : G_{\mathbb{Q}_p} \to \mathcal{O}^\times$ is unramified and $\alpha(\mathrm{frob}_p) = \alpha_p$. Let $V^- = V/V^+$. In this case

$$H^1_f(\mathbb{Q}_p, V) = \ker\left\{H^1(\mathbb{Q}_p, V) \to H^1(\mathbb{Q}_p, V^-)\right\}.$$

Letting $T \subset V$ be any $G_{\mathbb{Q}}$-stable $\mathcal{O}$-lattice and $W = V/T$, we let $T^+ = T \cap V^+$, $T^- = T/T^+$, $W^+ = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ and $W^- = W/W^+$. Then

$$H^1_f(\mathbb{Q}_p, W) = \ker\left\{H^1(\mathbb{Q}_p, W) \to H^1(\mathbb{Q}_p, W^-)\right\}_{\mathrm{div}} = \mathrm{im}\left\{H^1(\mathbb{Q}_p, W^+) \to H^1(\mathbb{Q}_p, W)\right\}_{\mathrm{div}}.$$

Example 2.2.2.e (Twists of Eigenforms). Let V be the Galois representation associated to some newform of weight k, and let $\chi : G_F \to L^\times$ be a character as in Example 2.2.2.c. Everything in that example carries over to the G_F-representations $V(\chi)$ with the only change being that we now require the Hodge–Tate weights to be either > 1 or $< 1 - k$ in the latter part.

2.2.3. *Vista: The Bloch–Kato conjectures for L-functions and Selmer groups.* In addition to defining Selmer groups very generally, Bloch and Kato [5] also formulated conjectures generalizing (BSD-crk) and (BSDp-0) (see also [18]).

2.3. **Selmer structures.** Mazur and Rubin [48, Ch. 2] introduced a general setup for Selmer groups.

2.3.1. *The structures.* Let $\mathcal{O}$ be the ring of integers of a finite extension $L/\mathbb{Q}_p$. Let M be a topological $\mathcal{O}$-module equipped with a continuous $\mathcal{O}$-linear action of G_F that is unramified outside a finite set of places.

A Selmer structure for M is a collection of $\mathcal{O}$-submodules

$$\mathcal{L} = (\mathcal{L}_v)_v, \quad \mathcal{L}_v \subset H^1(F_v, M),$$

indexed by the places v of M. To be a Selmer structure this collection must satisfy

$$\mathcal{L}_v = H^1_{\mathrm{ur}}(F_v, M) = \ker\left\{H^1(F_v, M) \to H^1(I_v, M)\right\} \quad \text{for almost all } v.$$

The asssociated Selmer group is then defined to be

$$H^1_{\mathcal{L}}(F, M) = \left\{c \in H^1(F, M) \ : \ res_v(c) \in \mathcal{L}_v \ \forall v\right\}.$$

If Σ is any finite set of places containing all those at which M is ramified or for which $\mathcal{L}_v \neq H^1_{\mathrm{ur}}(F_v, M)$, then

$$H^1_{\mathcal{L}}(F, M) = \ker\left\{H^1(G_{F,\Sigma}, M) \stackrel{res}{\to} \prod_{v \in \Sigma} H^1(F_v, M)/\mathcal{L}_v\right\}.$$

Let $M^* = \mathrm{Hom}_{cts}(M, \mathbb{Q}_p/\mathbb{Z}_p(1)) = \mathrm{Hom}_{cts}(M, \mu_{p^\infty})$ be the arithmetic dual of M, equipped with the natural $\mathcal{O}$-module structure (so $(a \cdot f)(m) = f(am)$ for $a \in \mathcal{O}$, $f \in M^\vee$, and $m \in M$). Suppose M is either a direct or projective limit of finite-order G_F-stable $\mathcal{O}$-modules. The same is then true of M^* (the dual of a direct limit is an inverse limit, etc.). In this case, local Tate duality provides us with a perfect pairing

$$(\cdot,\cdot)_v : H^i(F_v, M) \times H^{2-i}(F_v, M^*) \to \mathbb{Q}_p/\mathbb{Z}_p, \quad i = 0, 1, 2.$$

This is just the cup-product combined with the canonical pairing $M \otimes M^* \to \mu_{p^\infty}$ and the identification $H^2(F_v, \mu_{p^\infty}) = \mathbb{Q}_p/\mathbb{Z}_p$. Furthermore, if $v \nmid p\infty$, then $H^1_{\mathrm{ur}}(F_v, M)$ and $H^1_{\mathrm{ur}}(F_v, M^*)$ are mutual annihilators under $(\cdot,\cdot)_v$. It follows that if $\mathcal{L} = (\mathcal{L}_v)$ is a Selmer structure for M, then

$$\mathcal{L}^* = (\mathcal{L}_v^*), \quad \mathcal{L}_v^* \text{ the annihilator of } \mathcal{L}_v \text{ under } (\cdot,\cdot)_v,$$

is a Selmer structure for M^*.

2.3.2. *Examples.* The Selmer groups we have considered so far are all defined by Selmer structures.

Example 2.3.2.a ($\mathrm{Sel}_{p^n}(E/F)$). Take $\mathcal{O} = \mathbb{Z}_p$, $M = E[p^n]$, and

$$\mathcal{L}_v = \mathrm{im}(E(F_v)/p^n E(F_v) \stackrel{\kappa_v}{\to} H^1(F_v, E[p^n]).$$

As noted before, if $v \nmid p$ is a prime of good reduction, then $\mathrm{im}(\kappa_v) = H^1_{\mathrm{ur}}(F_v, E[p^n])$, so $(\mathcal{L}_v)_v$ is a Selmer structure for $E[p^n]$.

The Weil pairing $(\cdot,\cdot)_{\mathrm{Weil}} : E[p^n] \times E[p^n] \to \mu_{p^n}$ identifies M^* with $E[p^n]$. Furthermore, for each place v, $\mathrm{im}(\kappa_v)$ is its own annihilator under $(\cdot,\cdot)_v$, and so $\mathcal{L}^* = \mathcal{L}$.

Example 2.3.2.b ($H^1_f(F,T)$ and $H^1_f(F,W)$). The Bloch–Kato Selmer groups $H^1_f(F,?)$, $? = T, W$, are just the Selmer groups for the Selmer structures

$$\mathcal{L}_f = (H^1_f(F_v, ?)).$$

To see that $\mathcal{L}_f$ is a Selmer structure, it suffices to note that if V is unramified at some $v \nmid p$, then $H^1_f(F_v,?) = H^1_{\mathrm{ur}}(F_v,?)$. For $? = T$ this is so since $H^1(F_v,T)_{\mathrm{tor}}$ is the image of $W^{G_{F_v}} = W^{G_{F_v}/I_v}$ and so belongs to $H^1_{\mathrm{ur}}(F_v,T)$. And for $? = W$, $H^1_{\mathrm{ur}}(F_v,W) = H^1(G_{F_v}/I_v, W)$ is the image of $H^1_{\mathrm{ur}}(F_v,V) = H^1(G_{F_v}/I_v,V)$ as $H^2(G_{F_v}/I_v,T) = 0$, the pro-cyclic group $G_{F_v}/I_v \cong \widehat{\mathbb{Z}}$ having cohomological dimension 1.

2.3.3. *An important exact sequence.* We impose a partial ordering on the Selmer structures on M, writing $\mathcal{L}_1 \leq \mathcal{L}_2$ if $\mathcal{L}_{1,v} \subseteq \mathcal{L}_{2,v}$ for all v. In this case $H^1_{\mathcal{L}_1}(F,M) \subseteq H^1_{\mathcal{L}_2}(F,M)$. Note that we also have $\mathcal{L}_2^* \leq \mathcal{L}_1^*$.

Let $\mathcal{L}_1 \leq \mathcal{L}_2$ be Selmer structures for M and let S be the finite set of places where $\mathcal{L}_{1,v} \neq \mathcal{L}_{2,v}$. Then global duality implies that there is an exact sequence [48, Thm. 2.3.4]:

$$\text{(SES)} \qquad 0 \to H^1_{\mathcal{L}_1}(F,M) \to H^1_{\mathcal{L}_2}(F,M) \overset{res}{\to} \prod_{v\in S} \frac{\mathcal{L}_{2,v}}{\mathcal{L}_{1,v}} \overset{res^\vee}{\to} H^1_{\mathcal{L}_1^*}(F,M^*)^\vee \to H^1_{\mathcal{L}_2}(F,M^*)^\vee \to 0.$$

The map $res^\vee$ is the dual of

$$H^1_{\mathcal{L}^*}(F,M^*) \overset{res}{\to} \prod_{v\in S} \mathcal{L}_v^* = \prod_{v\in S} \left(\frac{H^1(F_v,M)}{\mathcal{L}_v} \right)^\vee,$$

where the final identification comes via Tate local duality.

2.3.4. *An important formula.* Suppose that M has finite order. Let $\mathcal{L}$ be a Selmer structure for M. Then by combining the exact sequence (SES) with global duality and the global Euler characteristic yields (cf. [15, Thm. 2.19] and [48, Prop. 2.3.5]):

$$\text{(SF)} \qquad \frac{\#H^1_{\mathcal{L}}(F,M)}{\#H^1_{\mathcal{L}^*}(F,M^*)} = \frac{\#H^0(F,M)}{\#H^0(F,M^*)} \prod_v \frac{\#\mathcal{L}_v}{\#H^1(F_v,M)}.$$

3. Iwasawa modules for elliptic curves

For simplicity we assume from hereon that

$$\text{(odd)} \qquad p > 2.$$

Among other things this ensures the triviality of all the H^1-cohomology groups for all archimedean local fields that appear herein.

3.1. **The extension F_∞/F.** Let F_∞/F be a $\mathbb{Z}_p^d$-extension of F, $d \geq 1$. This is an (infinite) pro-finite abelian extension of F such that $\Gamma = \mathrm{Gal}(F_\infty/F)$ (which is a $\widehat{\mathbb{Z}}$-module) is isomorphic to $\mathbb{Z}_p^d$. Let

$$\Lambda = \mathbb{Z}_p[\![\Gamma]\!],$$

be the completed group ring of Γ over $\mathbb{Z}_p$. If $\gamma_1, ..., \gamma_d \in \Gamma$ are topological generators, then the map $\Lambda \overset{\sim}{\to} \mathbb{Z}_p[\![T_1, ..., T_d]\!]$, $\gamma_1 \mapsto 1 + T_i$, identifies Λ with the power series ring in d variables over $\mathbb{Z}_p$. In particular, Λ is a $d+1$-dimensional regular complete local ring. The maximal ideal of Λ is $\mathfrak{m} = (p, \gamma_1 - 1, ..., \gamma_d - 1)$. If $d = 1$, then we will just write γ for a topological generator of Γ.

The examples of most interest to us will be:

3.1.1. $F = \mathbb{Q}$. In this case there is exactly one possibility for F_∞, namely the cyclotomic $\mathbb{Z}_p$-extension, which we will denote by $\mathbb{Q}_\infty$. This is defined as follows.

For each $n \geq 1$ let ζ_{p^n} be a primitive p^nth root of unity. The field $\mathbb{Q}(\zeta_{p^{n+1}})$ is a Galois extension of $\mathbb{Q}$ with Galois group $G_n = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q})$ canonically isomorphic to $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$, the isomorphism being $\sigma \mapsto a \bmod p^{n+1}$ for $\sigma(\zeta_{p^{n+1}}) = \zeta_{p^{n+1}}^a$. The groups G_n decompose compatibly as $G_n = \Delta \times \Gamma_n$ with Δ cyclic of order $p-1$ and Γ_n cyclic of order p^n. The subgroup Δ projects isomorphically onto $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^\times$. Put $\mathbb{Q}(\zeta_{p^\infty}) = \cup_{n=0}^\infty \mathbb{Q}(\zeta_{p^{n+1}})$. Then there is a canonical isomorphism of profinite groups:

$$G = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}) = \varprojlim_n G_n \xrightarrow{\sim} \varprojlim_n (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times = \mathbb{Z}_p^\times.$$

The Galois group G then decomposes as $G = \Delta \times \Gamma$ with $\Gamma = \varprojlim_n \Gamma_n$. The group Γ is a cyclic pro-p-group and identified with $1 + p\mathbb{Z}_p \subset \mathbb{Z}_p^\times$ while Δ is just the subgroup $\mu_{p-1} \subset \mathbb{Z}_p^\times$. The cyclotomic $\mathbb{Z}_p$-extension is just $\mathbb{Q}_\infty = \mathbb{Q}(\mu_{p^\infty})^\Delta$. The group Γ projects isomorphically onto $\Gamma_\mathbb{Q} = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$, which indentifies these two groups. Note that a convenient topological generator of Γ (and hence of $\Gamma_\mathbb{Q}$) is the element γ identified with $1 + p \in 1 + p\mathbb{Z}_p$ (since $p > 2$, $1 + p\mathbb{Z}_p = (1+p)^{\mathbb{Z}_p}$).

3.1.2. $F = K$, *an imaginary quadratic extension of* $\mathbb{Q}$. In this case there are three extensions of interest to us. The first of these is the unique $\mathbb{Z}_p^2$-extension K_∞/K; this is maximal among the $\mathbb{Z}_p^d$-extensions of K (for all d). The other two are the cyclotomic $\mathbb{Z}_p$-extension $K_\infty^{\mathrm{cyc}}/K$ and the anticyclotomic $\mathbb{Z}_p$-extension K_∞^{ac}.

The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ acts on $\Gamma_K = \mathrm{Gal}(K_\infty/K)$ by conjugation. In particular, Γ_K decomposes under the action of the non-trivial automorphism $c \in \mathrm{Gal}(K/\mathbb{Q})$ as $\Gamma_K = \Gamma_K^+ \times \Gamma_K^-$ with c acting on $\Gamma_K^\pm$ as $c^{-1}gc = g^{\pm 1}$. Then $K_\infty^{\mathrm{cyc}} = K_\infty^{\Gamma_K^-}$ and $K_\infty^{\mathrm{ac}} = K_\infty^{\Gamma_K^+}$. In particular, the canonical projections $\mathrm{Gal}(K_\infty/K) \twoheadrightarrow \mathrm{Gal}(K_\infty^?/K)$ induce isomporphisms

$$\Gamma_K^+ \xrightarrow{\sim} \Gamma_K^{\mathrm{cyc}} = \mathrm{Gal}(K_\infty^{\mathrm{cyc}}/K) \ \text{ and } \ \Gamma_K^- \xrightarrow{\sim} \Gamma_K^{\mathrm{ac}} = \mathrm{Gal}(K_\infty^{\mathrm{ac}}/K).$$

Of course, the cyclotomic $\mathbb{Z}_p$-extension is just $K_\infty^{\mathrm{cyc}} = K \cdot \mathbb{Q}_\infty$, and the canonical projection $\Gamma_K^{\mathrm{cyc}} = \mathrm{Gal}(K_\infty^{\mathrm{cyc}}/K) \xrightarrow{\sim} \Gamma_\mathbb{Q} = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ is an isomorphism.

3.1.3. *Back to the general case.* In general, the extension F_∞/F is unramified at each place $v \nmid p$ of F, and the finiteness of the class group of F implies that it must be ramified at at least one place $v \mid p$. For simplicity we will assume that

(p-ram) $\qquad\qquad$ F_∞ is ramified at each place $v \mid p$.

This is true of each of our examples of interest. However, there are many $\mathbb{Z}_p$-extensions of arithmetic interest for which this hypothesis does not hold. Another nice property that an extension F_∞/F can have is

(fs) $\qquad$ there are only finitely many places of F_∞ over each finite place of F.

This can only hold for $\mathbb{Z}_p$-extensions (that is, for $d = 1$), and even then it does not always hold. Property (fs) holds for the cyclotomic $\mathbb{Z}_p$-extensions $\mathbb{Q}_\infty$ and K_∞^{cyc}. It does not hold for the anticyclotomic extension K_∞^{ac}: while each prime that splits in K has only finitely many places over it in K_∞^{ac}, every prime that is inert in K splits completely in K_∞^{ac}.

3.2. **Selmer groups over F_∞.** Perhaps the most natural way to define a Selmer group over F_∞ is

$$S(E/F_\infty) = \varinjlim_{F \subseteq F' \subset F_\infty} \mathrm{Sel}_{p^\infty}(E/F'),$$

where F' runs over the finite extensions of F in F_∞. This realizes $S(E/F_\infty)$ as a subgroup of $H^1(F_\infty, E[p^\infty])$. However, for our purposes it is convenient to take a slightly different point of view. Following Greenberg, instead of varying the fields F', we enlarge the Galois module $E[p^\infty]$.

As before let $T = T_pE = \varprojlim_n E[p^n]$ be the p-adic Tate-module of E. Then T is a free $\mathbb{Z}_p$-module of rank two with a continuous $\mathbb{Z}_p$-linear action of G_F. We denote this action by ρ. Let $\Lambda^\vee = \mathrm{Hom}_{cts}(\Lambda, \mathbb{Q}_p/\mathbb{Z}_p)$ be the Pontryagin dual of Λ with the Λ-action given by $(x \cdot f)(y) = f(xy) = f(yx)$. Let

$$\Psi : G_F \twoheadrightarrow \mathrm{Gal}(F_\infty/F) = \Gamma \subset \Lambda^\times$$

be the canonical projection. Put

$$M = T \otimes \Lambda^\vee$$

and let G_F act via $\rho \otimes \Psi^{-1}$. Note that the canonical isomorphism $T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \xrightarrow{\sim} E[p^\infty]$ induces an isomorphism $M \xrightarrow{\sim} \mathrm{Hom}_{cts}(\Lambda, E[p^\infty])$, and this is a G_F-equivariant isomorphism if we let G_F act on Λ via Ψ. The module M can be viewed as built out of the W arising from twist of T_pE as in Example 2.2.2.c. If $\chi : G_\mathbb{Q} \twoheadrightarrow \Gamma \to \mathcal{O}^\times$ is a character, $\mathcal{O}$-being the ring of integers of a finite extension L of $\mathbb{Q}_p$, then

$$(M \otimes_{\mathbb{Z}_p} \mathcal{O})[\gamma - \chi(\gamma)] = T_pE \otimes_{\mathbb{Z}_p} (\Lambda^\vee \otimes_{\mathbb{Z}_p} \mathcal{O})[\gamma - \chi(\gamma)] = T_p \otimes_{\mathbb{Z}_p} L/\mathcal{O}(\chi^{-1}).$$

3.2.1. $S(E/F_\infty)$. Let Σ be a finite set of places of F containing all those divide p or at which E has bad reduction. We will define $S(E/F_\infty)$ as a subgroup of $H^1(G_{F,\Sigma}, M)$. To do this we make the following additional simplifying hypothesis:

(sst) E has either good ordinary, multiplicative, or supersingular reduction at each $v \mid p$

(that is, E has semistable reduction at each $v \mid p$). Let S_p^{ord} be the set of $v \mid p$ at which E has good ordinary or multiplicative reduction. Then assuming (p-ram) and (sst) we have

$$S(E/F_\infty) = \ker \left\{ H^1(G_{F,\Sigma}, M) \overset{res}{\to} \prod_{v \in \Sigma, v \nmid p} H^1(F_v, M) \times \prod_{v \in S_p^{\mathrm{ord}}} H^1(I_v, T/T_v^+ \otimes_{\mathbb{Z}_p} \Lambda^\vee) \right\}.$$

Note that no condition is imposed at places $v \mid p$ at which E has supersingular reduction. If (fs) also holds, then we can replace the product $\prod_{v \in \Sigma, v \nmid p} H^1(F_v, M)$ with $\prod_{v \in \Sigma, v \nmid p} H^1(I_v, M)$. It can be shown that this definition of $S(E/F_\infty)$ is identified with the natural definition proposed above via the map $H^1(F, M) \to H^1(F_\infty, E[p^\infty])$ given by restriction to G_{F_∞} followed by evaluation at $1 \in \Gamma$.

Along the way toward the Main Conjectures and their applications we will need some variations on $S(E/F_\infty)$.

3.2.2. $S_{\mathrm{Gr}}(E/K_\infty)$. Let $K \subset \overline{\mathbb{Q}}$ be an imaginary quadratic field. We assume that

(split) $$p \text{ splits in } K\colon\ p = v\bar{v},$$

where v corresponds to the valuation determined by $K \subset \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$.

Letting $F_\infty = K_\infty$, we write $\mathcal{M}$ for the G_K-module M defined above. Let Σ be a finite set of places of K containing all those that dividing p or at which E has bad reduction. We put

$$S_{\mathrm{Gr}}(E/K_\infty) = \ker\left\{ H^1(G_{K,\Sigma}, \mathcal{M}) \overset{res}{\to} \prod_{w\in\Sigma, w\nmid p} H^1(I_w, \mathcal{M}) \times H^1(K_{\bar{v}}, \mathcal{M}) \right\}.$$

This Selmer group is supposed to capture the Selmer groups of the twists of T_pE by characters whose Hodge–Tate weight at v is > 1 and at $\bar{v}$ is < -1.

3.2.3. $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$. This is essentially a variation on $S_{\mathrm{Gr}}(E/K_\infty)$. Taking $F_\infty = K_\infty^{\mathrm{ac}}$, the anticyclomtomic $\mathbb{Z}_p$-extension of K, we let M_{ac} be the corresponding G_K-module M. We put

$$S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) = \ker\left\{ H^1(G_{K,\Sigma}, M_{\mathrm{ac}}) \overset{res}{\to} \prod_{w\in\Sigma, w\nmid p} H^1(K_w, M_{\mathrm{ac}}) \times H^1(K_{\bar{v}}, M_{\mathrm{ac}}) \right\}.$$

Note that for an inert prime $q \in \Sigma$, since (fs) does not hold, we cannot always replace $H^1(K_q, M_{\mathrm{ac}})$ with $H^1(I_q, M_{\mathrm{ac}})$.

3.2.4. $S_\pm(E/\mathbb{Q}_\infty)$. Suppose $E/\mathbb{Q}$ has supersingular reduction at p. Then the definition of $S(E/\mathbb{Q}_\infty)$ has no restriction on the classes at p. This results in a Λ-module that is too big to be useful. If $a_p(E) = 0$ (which will always be the case if $p \geq 5$), then Kobayashi [38] defined two subgroups $S_\pm(E/\mathbb{Q}_\infty) \subset S(E/\mathbb{Q}_\infty)$ which, building on work of Kato [34], can be shown to be co-torsion in the sense described in §3.3 below.

Let $\mathbb{Q}_n \subset \mathbb{Q}_\infty$ be the finite extension of $\mathbb{Q}$ with $\Gamma_n = \mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q}) \cong \mathbb{Z}_p/p^n\mathbb{Z}_p$ (the last isomorphism depends on the choice of γ; the identification with $1 + p\mathbb{Z}_p/1 + p^{n+1}\mathbb{Z}_p$ is canonical). The extension $\mathbb{Q}_n/\mathbb{Q}$ is totally ramified at p and we denote by $\mathbb{Q}_{n,p}$ the completion of $\mathbb{Q}_n$ at the unique prime above p. Then $\mathbb{Q}_{n,p}/\mathbb{Q}_p$ has Galois group Γ_n. Let

$$E^\pm(\mathbb{Q}_{n,p}) = \left\{ P \in E(\mathbb{Q}_{n,p}) \ : \ \mathrm{Tr}_{\mathbb{Q}_{n,p}/\mathbb{Q}_{m+1,p}} P \in E(\mathbb{Q}_{m,p}) \forall 0 \leq m < n, m \equiv \frac{1 \mp (-1)}{2} \bmod 2 \right\}.$$

Then we let

$$\mathrm{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_n) = \left\{ c \in \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}_n) \ : \ res_p(c) \in \kappa_p(E^\pm(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \right\},$$

where res_p denotes restriction at the unique prime above p and κ_p is the Kummer map at this prime. The Selmer groups Kobayashi defined are

$$S_\pm(E/\mathbb{Q}_\infty) = \varinjlim_n \mathrm{Sel}_{p^\infty}^\pm(E/\mathbb{Q}_n).$$

Shapiro's lemma gives an identification

$$H^1(\mathbb{Q}_{p,n}, E[p^\infty]) = H^1(\mathbb{Q}_p, \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[\Gamma_n], E[p^\infty])),$$

where the $G_{\mathbb{Q}_p}$ action on $\mathbb{Z}_p[\Gamma_n]$ is $g \cdot \sum n_\gamma \gamma = \sum n_\gamma \gamma g^{-1}$. Let

$$H^1_\pm(\mathbb{Q}_p, M) = \varinjlim_n \kappa_p(E^\pm(\mathbb{Q}_{n,p}) \otimes \mathbb{Q}_p/\mathbb{Z}_p) \subset \varinjlim_n H^1(\mathbb{Q}_p, \mathrm{Hom}_{\mathbb{Z}_p}(\mathbb{Z}_p[\Gamma_n], E[p^\infty])) = H^1(\mathbb{Q}_p, M).$$

Then $H^1_\pm(\mathbb{Q}_p, M)$ is a Λ-submodule of $H^1(\mathbb{Q}_p, M)$. We can rewrite the definition of $S_\pm(E/\mathbb{Q}_\infty)$ as

$$S_\pm(E/\mathbb{Q}_\infty) = \left\{ c \in S(E/\mathbb{Q}_\infty) \ : \ res_p(c) \in H^1_\pm(\mathbb{Q}_p, M) \right\}.$$

3.2.5. *Vista: Iwasawa cohomology and Coleman maps.* The cohomology group

$$H^1_{\mathrm{Iw}}(T) = \varprojlim_n H^1(\mathbb{Q}_{p,n}, T),$$

where the inverse limit is taken with respect to the corestriction maps, is often called the Iwasawa cohomology of T. The group $H^1_{\mathrm{Iw}}(T)$ can be identified with $H^1(\mathbb{Q}_p, T \otimes_{\mathbb{Z}_p} \Lambda)$, where the $G_{\mathbb{Q}_p}$-action on $T \otimes \Lambda$ is just $\rho \otimes \Psi$. One can define a local subgroup $\mathcal{L}_p \subset H^1(\mathbb{Q}_p, M)$ – to be part of a Selmer structure for M, say – by first defining a subgroup $L_p \subset H^1_{\mathrm{Iw}}(T)$ and taking $\mathcal{L}_p$ to be the annihilator of L_p under the pairing of local Tate duality. In many cases of interest, the group L_p is the kernel of a Λ-homomorphism $H^1_{\mathrm{Iw}}(T) \to \Lambda$ (or something similar) which is often called a Coleman map. This is true, for example, of the local conditions at p defining the Selmer groups $S(E/\mathbb{Q}_\infty)$, when E has ordinary reduction at p, and $S_\pm(E/\mathbb{Q}_\infty)$, when E has supersingular reduction at p. For the latter see [38], and for a more general discussion see [40].

3.3. $S_?(E/F_\infty)$ **as a Λ-module.** The group $H = H^1(G_{F,\Sigma}, M)$ has a natural structure as a discrete Λ-module. So its Pontryagin dual $X = \mathrm{Hom}_{cts}(H, \mathbb{Q}_p/\mathbb{Z}_p)$ is a compact Λ-module, with the Λ-action being $(\lambda \cdot f)(x) = f(\lambda x)$. Similarly, the submodule $S(E/\mathbb{Q}_\infty) \subset H$ is a discrete Λ-module and its Pontryagin dual

$$X_?(E/F_\infty) = \mathrm{Hom}_{cts}(S_?(E/F_\infty), \mathbb{Q}_p/\mathbb{Z}_p), \quad ? = \emptyset, \mathrm{Gr}, \mathrm{BDP}, \text{ or } \pm,$$

which is a quotient of X, is a compact Λ-module. (Of course, by $? = \emptyset$ we mean no subscript.)

Proposition 2. *X is a finitely-generated Λ-module.*

Proof. We will prove this by induction on the $\mathbb{Z}_p$-rank d of $\Gamma \cong \mathbb{Z}_p^d$.

Suppose first that $d = 0$. Then $H = H^1(G_{F,\Sigma}, E[p^\infty])$ and we want to show that $X = \mathrm{Hom}_{cts}(H, \mathbb{Q}_p/\mathbb{Z}_p)$ is a finitely-generated $\mathbb{Z}_p$-module. By the compactness of X and Nakayama's lemma, it suffices to show that X/pX is a finite. And by duality the latter is equivalent to the finiteness of $H[p]$. From the short exact sequence $0 \to E[p] \to E[p^\infty] \xrightarrow{p} E[p^\infty] \to 0$ we obtain a surjection $H^1(G_{F,\Sigma}, E[p]) \twoheadrightarrow H^1(G_{F,\Sigma}, E[p^\infty])[p] = H[p]$. We have already observed that $H^1(G_{F,\Sigma}, E[p])$ is finite, hence $H[p]$ is finite.

For the induction step, let γ belong to a topological generating set of Γ. Then $\Gamma' = \Gamma/\overline{\langle\gamma\rangle} \cong \mathbb{Z}_p^{d-1}$, and $\Lambda/(\gamma-1)\Lambda = \mathbb{Z}_p[\![\Gamma']\!] = \Lambda'$. Note that $M[\gamma-1] = T \otimes_{\mathbb{Z}_p} \mathrm{Hom}_{cts}(\Lambda/(\gamma-1)\Lambda, \mathbb{Q}_p/\mathbb{Z}_p) = T \otimes_{\mathbb{Z}_p} \mathrm{Hom}_{cts}(\Lambda', \mathbb{Q}_p/\mathbb{Z}_p) = M'$. From the short exact sequence $0 \to M' \to M \xrightarrow{\gamma-1} M \to 0$ we obtain a surjection $H^1(G_{F,\Sigma}, M') \to H^1(G_{F,\Sigma}, M)[\gamma-1]$, and so by duality an injection $X/(\gamma-1)X \hookrightarrow \mathrm{Hom}_{cts}(H^1(G_{F,\Sigma}, M'), \mathbb{Q}_p/\mathbb{Z}_p) = X'$. By the induction hypothesis, X' is a finitely-generated Λ'-module, hence $X/(\gamma-1)X$ is a finitely-generated Λ'-module (by the Noetherian-ness of Λ'). That X is a finitely-generated Λ-module follows from Nakayama's lemma as before. □

Corollary 3. *Let $\mathcal{S} \subset H^1(G_{F,\Sigma}, M)$ be a Λ-submodule. Its Pontryagin dual $\mathcal{X} = \mathrm{Hom}_{cts}(\mathcal{S}, \mathbb{Q}_p/\mathbb{Z}_p)$ is a finitely-generated Λ-module. In particular, $X_?(E/F_\infty)$ is a finitely-generated Λ-module.*

There is a structure theorem for finitely-generated Λ-modules that is reminiscent of finitely-generated modules over a PID. Such a Λ-module X admits a Λ-homomorphism

$$X \to \Lambda^r \oplus \prod_{i=1}^s \Lambda/(f_i), \quad f_i \neq 0,$$

with pseudonull kernel and cokernel. Pseudonull means that the localizations at all height one primes of Λ are zero; if $d = 1$, then finitely-generated and pseudonull is equivalent to finite order. The integer r is uniquely determined and is called the Λ-rank of X; we will denote it by $r(X)$. The ideal $\xi(X) = (f_1 \cdots f_s) \subset \Lambda$ is also uniquely determined. The characteristic ideal $\xi(X) \subseteq \Lambda$ of the Λ-module X is 0 if $r > 0$ and is the ideal $(f_1 \cdots f_s)$ if $r = 0$.

One useful result, which points to the utility of this structure theorem is:

Lemma 4. *Suppose $d = 1$ (so $\Lambda \cong \mathbb{Z}_p[\![T]\!]$). Let X be a finitely-generated, torsion Λ-module with no non-zero pseudonull submodule. Let $0 \neq \lambda \in \Lambda$. Then*

$$\#X/\lambda X = \#\Lambda/(\xi(X), \lambda).$$

In particular, if $f \in \xi(X)$ is a generator, then

$$\#X/(\gamma - 1)X = \#\mathbb{Z}_p/f(0).$$

These equalities should be understood to mean that if one side is infinite then so is the other.

The proof of this lemma essentially amounts to multiplying the exact sequence

$$0 \to X \to \prod_{i=1}^{s} \Lambda/(f_i) \to \text{coker} \to 0$$

by λ and appealing to the snake lemma and noting that coker has finite order and so $\#\text{coker}[\lambda] = \#\text{coker}/\lambda\text{coker}$.

Some natural questions to ask about $X = X(E/F_\infty)$:

- What is $r(X)$? Is it ever 0? positive?
- What is $\xi(X)$?
- Does X have a non-zero pseudonull Λ-submodule?

The Iwasawa theory of elliptic curves is partly focused on answering these questions. The arithmetic significance of the answers will become more clear as we go on.

3.3.1. *Vista: Selmer groups of p-adic deformations.* The Iwasawa modules $S_?(E/F_\infty)$ that we have defined are some of the simplest examples of Selmer groups for p-adic deformations. In this case the deformation is $T_pE \otimes_{\mathbb{Z}_p} \Lambda$ (with G_F acting as $\rho \otimes \Psi^{-1}$), which deforms the twist of T_pE by the trivial character by the universal G_F-character that factors through Γ. Other possible deformations could include deforming T_pE. Here we use 'deformation' in the sense of Greenberg [22]; the reader should consult *op. cit.* for more on Selmer groups in this context.

3.3.2. *Horizon: Selmer complexes.* Nekovář [51] developed a formalism for Iwasawa theory based on 'big Galois representations' (such as $T \otimes \mathbb{Z}_p\Lambda$) and their cohomological invariants, working within the framework of derived categories. This both recovers and extends many of the results about Selmer groups, leading to generalized Cassels–Tate pairings and generalized p-adic height pairings, among many others. The epigraph following the introduction: '*Selmer groups are dead. Long live Selmer complexes.*'

3.4. **Control theorems.** It is natural to ask whether the group $\mathrm{Sel}_{p^\infty}(E/F)$ can be recovered from $S(E/F_\infty)$. Certainly, there is a canonical map $\mathrm{Sel}_{p^\infty}(E/F) \to S(E/F_\infty)$ with image in the Γ-invariants $S(E/F_\infty)^\Gamma = S(E/F_\infty)[\gamma_1 - 1, \cdots, \gamma_d - 1]$. How are these two groups related? The answer to this is a case of what is often called a 'control theorem.'

Instead of proving the most general theorems, we concentrate on some important cases. To make our task easier, we will always assume

$$(\mathrm{irred}_F) \qquad\qquad E[p] \text{ is an irreducible } G_F\text{-representation.}$$

Under this assumption it is not hard to deduce that if $x_1, ..., x_j \in \Lambda$, then the natural map

$$H^1(G_\Sigma, M[x_1, ..., x_j]) \xrightarrow{\sim} H^1(G_\Sigma, M)[x_1, ..., x_j]$$

is an isomorphism. And using that F_∞/F is unramified at each $v \nmid p$ one can also deduce that if $x_1, ..., x_j$ is a regular sequence, then

$$H^1(I_v, M[x_1, ..., x_j]) \xrightarrow{\sim} H^1(I_v, M)[x_1, ..., x_j], \quad v \nmid p.$$

3.4.1. $S(E/\mathbb{Q}_\infty)$*: ordinary case.* Suppose that $E/\mathbb{Q}$ has good ordinary or multiplicative reduction at p. Let $M^- = T/T^+ \otimes_{\mathbb{Z}_p} \Lambda^\vee$, and let

$$\mathcal{P}_\Sigma = \prod_{\ell \in \Sigma} \mathcal{P}_\ell, \quad \mathcal{P}_\ell = \begin{cases} H^1(I_\ell, M)^{G_{\mathbb{Q}_\ell}} & \ell \neq p \\ H^1(I_p, M^-)^{G_{\mathbb{Q}_p}} & \ell = p. \end{cases}$$

Then $S(E/\mathbb{Q}_\infty) = \ker\left\{H^1(G_\Sigma, M) \xrightarrow{res} \mathcal{P}_\Sigma\right\}$. Let

$$P_\Sigma = \prod_{\ell \in \Sigma} P_\ell, \quad P_\ell = \begin{cases} H^1(\mathbb{Q}_\ell, E[p^\infty]) & \ell \neq p \\ \frac{H^1(\mathbb{Q}_p, E[p^\infty])}{\mathrm{im}\left\{H^1(\mathbb{Q}_p, T^+ \otimes_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p) \to H^1(\mathbb{Q}_p, E[p^\infty])\right\}_{\mathrm{div}}} & \ell = p. \end{cases}$$

Then there is an exact sequence

$$0 \to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \to S(E/\mathbb{Q}_\infty)[\gamma - 1] \to \mathrm{im}\left\{H^1(G_\Sigma, E[p^\infty]) \xrightarrow{res} P_\Sigma\right\} \cap \ker\left\{P_\Sigma \to \mathcal{P}_\Sigma[\gamma - 1]\right\}.$$

If $X(E/\mathbb{Q}_\infty)$ is a torsion Λ-module, then using global Tate duality one can show that $H^1(G_\Sigma, M) \xrightarrow{res} \mathcal{P}_\Sigma$ is surjective, hence $S(E/\mathbb{Q}_\infty)[\gamma - 1] = \ker\left\{H^1(G_\Sigma, E[p^\infty]) \xrightarrow{res} \mathcal{P}_\Sigma[\gamma - 1]\right\}$. It follows that the displayed sequence is exact on the right. And if $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is finite, then one can similarly show that $H^1(G_\Sigma, E[p^\infty]) \xrightarrow{res} P_\Sigma$ is surjective. This yields:

Proposition 5 (Control Theorem for the ordinary case)**.** *Suppose $E/\mathbb{Q}$ has good ordinary or multiplicative reduction at p and that* $(\mathrm{irred}_\mathbb{Q})$ *holds. Suppose also that $X(E/\mathbb{Q}_\infty)$ is a torsion Λ-module and that $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is finite. Then there is an exact sequence*

$$0 \to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \to S(E/\mathbb{Q}_\infty)[\gamma - 1] \to \ker\left\{P_\Sigma \to \mathcal{P}_\Sigma[\gamma - 1]\right\} \to 0.$$

To be precise, the arguments above actually show that if $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is finite, then $X(E/\mathbb{Q}_\infty)$ is a torsion Λ-module.

Let $K_\ell = \ker\left\{P_\ell \to \mathcal{P}_\ell\right\}$. Then as a consequence of Proposition 5:

Corollary 6. *Under the assumptions of the preceding proposition,*

$$\#S(E/\mathbb{Q}_\infty)[\gamma - 1] = \#\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \cdot \prod_{\ell \in \Sigma} \#K_\ell.$$

The orders of the groups K_ℓ are readily computed. Suppose first that $\ell \nmid p$. Then from the earlier observation that $H^1(I_\ell, E[p^\infty]) \xrightarrow{\sim} H^1(I_\ell, M)[\gamma - 1]$, it follows that

$$\#K_\ell = \#H^1(\mathbb{F}_\ell, E[p^\infty]^{I_\ell}) = \begin{cases} |c_\ell(E/\mathbb{Q})|_p^{-1} & \ell \mid N_E, \ell \neq p \\ 1 & \ell \nmid N_E, \end{cases}$$

where N_E is the conductor of E, and $c_\ell(E/\mathbb{Q})$ is the Tamagawa factor at ℓ for $E/\mathbb{Q}$. Now suppose that E has good ordinary reduction at p. Then a straightforward but more involved calculation shows that

$$\#K_p = (\#\mathbb{Z}_p/(1 - \alpha_p))^2,$$

where again α_p is the p-adic unit root of $x^2 - a_p(E)x + p$. As $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) = Ш(E/\mathbb{Q})[p^\infty]$ when Sel_{p^∞} is finite, we can now restate the preceding corollary as:

Corollary 7. *Under the assumptions of the preceding proposition and assuming that E has good ordinary reduction at p,*

$$\#S(E/\mathbb{Q}_\infty)[\gamma - 1] = \left| (1 - \alpha_p)^2 \cdot \#Ш(E/\mathbb{Q})[p^\infty] \cdot \prod_{\ell \mid N_E} c_\ell(E/\mathbb{Q}) \right|_p^{-1}.$$

More generally, let $\psi_\zeta : G_\mathbb{Q} \to \Gamma \xrightarrow{\gamma \mapsto \zeta} \overline{\mathbb{Q}}_p^\times$ be the finite order character sending γ (or any lift of it) to the pth-power root of unity ζ. One can also compare $(S(E/\mathbb{Q}_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Z}[\zeta])[\gamma - \zeta]$ to $\mathrm{Sel}(E, \psi_\zeta^{-1})$ in a similar way. Doing so yields:

Proposition 8 (Control Theorem for twists in the ordinary case)**.** *Suppose $E/\mathbb{Q}$ has good ordinary or multiplicative reduction at p and that* $(\mathrm{irred}_\mathbb{Q})$ *holds. Let ζ be a pth-power root of unity. Suppose also that $X(E/\mathbb{Q}_\infty)$ is a torsion Λ-module and that $\mathrm{Sel}(E, \psi_\zeta^{-1})$ is finite. Then there is an exact sequence*

$$0 \to \mathrm{Sel}(E, \psi_\zeta^{-1}) \to (S(E/\mathbb{Q}_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Z}[\zeta])[\gamma - \zeta] \to \ker\left\{ P_{\Sigma,\zeta} \to (\mathcal{P}_\Sigma \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\zeta])[\gamma - \zeta] \right\} \to 0.$$

Here $P_{\Sigma,\zeta} = \prod_{\ell \in \Sigma} P_{\ell,\zeta}$ with $P_{\ell,\zeta}$ defined just as P_ℓ but with $E[p^\infty]$ replaced with the group $W = E[p^\infty] \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\zeta]$ with $G_\mathbb{Q}$ acting as $\rho \otimes \psi_\zeta^{-1}$.

Both of these propositions are particularly useful if $X(E/\mathbb{Q}_\infty)$ has no non-zero pseudonull submodule. If this is so, then by Lemma 4 the order of $S(E/\mathbb{Q}_\infty)[\gamma - 1]$, which is the order of $X(E/\mathbb{Q}_\infty)/(\gamma - 1)X(E/\mathbb{Q}_\infty)$, equals the order of $\mathbb{Z}_p/(g_E(0))$ for any generator g_E of $\xi(E/\mathbb{Q}_\infty)$. This highlights the utility of the next proposition.

Proposition 9 (No pseudonull submodule)**.** *Suppose $E/\mathbb{Q}$ has good ordinary or multiplicative reduction at p and that* $(\mathrm{irred}_\mathbb{Q})$ *holds. Suppose also that $X(E/\mathbb{Q}_\infty)$ is a torsion Λ-module. Then $X(E/\mathbb{Q}_\infty)$ has no non-zero pseudonull submodules.*

Combining these results we conclude:

Proposition 10. *Suppose $E/\mathbb{Q}$ has good ordinary reduction at p and that* $(\mathrm{irred}_\mathbb{Q})$ *holds. Suppose also that $X(E/\mathbb{Q}_\infty)$ is a torsion Λ-module and that $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is finite. Let g_E be a generator of the characteristic ideal $\xi(E/\mathbb{Q}_\infty)$. Then*

$$|g_E(0)|_p^{-1} = \#S(E/\mathbb{Q}_\infty)[\gamma - 1] = \left| (1 - \alpha_p)^2 \cdot \#Ш(E/\mathbb{Q})[p^\infty] \cdot \prod_{\ell \mid N_E} c_\ell(E/\mathbb{Q}) \right|_p^{-1}.$$

This result can be extended to cover the case of multiplicative reduction and even to allow for $E[p^\infty]^{G_{\mathbb{Q}}} \neq 0$. This as well as many details can be found in the papers of Greenberg (see especially [23, Thm. 4.1] and also [63, § 3.2]).

3.4.2. $S_{\mathrm{Gr}}(E/K_\infty)$. Let $\gamma_\pm \in \Gamma_K^\pm \subset \Gamma_K = \mathrm{Gal}(K_\infty/K)$ be topological generators such that γ_+ maps to γ in $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. The next proposition relates $\mathrm{Sel}_{\mathrm{Gr}}(E/K_\infty)[\gamma_+ - 1]$ and $\mathrm{Sel}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$. Let $\Lambda_K = \mathbb{Z}_p[\![\Gamma_K]\!]$ and $\Lambda_{\mathrm{ac}} = \mathbb{Z}_p[\![\Gamma^-]\!] = \mathbb{Z}_p[\![\mathrm{Gal}(K_\infty^{\mathrm{ac}}/K)]\!]$.

Proposition 11. *Suppose E has either good or multiplicative reduction at p and that* (irred$_K$) *holds. Suppose that* (split) *holds. Suppose also that $X_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ is a torsion Λ_{ac}-module. Let Σ^- be the set of primes at which E has bad reduction and which are inert in K. Then there is an exact sequence*

$$0 \to \mathrm{Sel}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) \to S_{\mathrm{Gr}}(E/K_\infty)[\gamma_+ - 1] \to \prod_{\ell \in \Sigma^-} H^1_{\mathrm{ur}}(K_\ell, M_{\mathrm{ac}}) \times H_{\bar{v}} \to 0,$$

where

$$H_{\bar{v}} = \ker\left\{H^1(K_{\bar{v}}, M_{\mathrm{ac}}) \to H^1(K_{\bar{v}}, \mathcal{M})[\gamma_+ - 1]\right\} \cong M^{G_{\bar{v}}}.$$

Note that $H_{\bar{v}}$ has finite order and is even trivial if E has supersingular reduction at p. On the other hand, for $\ell \in \Sigma^-$, $H^1_{\mathrm{ur}}(K_\ell, M^{\mathrm{ac}}) \cong \mathrm{Hom}_{cts}(\Lambda_{\mathrm{ac}}, E[p^\infty]^{I_\ell})$. The characteristic ideal of the dual of this last group is $(c_\ell(E/K)) \subset \Lambda_{\mathrm{ac}}$, the ideal generated by the Tamagawa number of E/K at the prime ℓ.

The proof of Proposition 11 proceeds along the lines of the proof of Proposition 5.

3.4.3. $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$. We assume that (split) holds. The Selmer group $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ was defined so as to closely interpolate the Selmer groups for twists of V_pE by anticyclotomic characters $\chi : G_K \twoheadrightarrow \Gamma_K^{\mathrm{ac}} \to \mathcal{O}^\times$ with Hodge–Tate weight > 1 at v (and so < -1 at $\bar{v}$). So it would be natural to formulate a control theorem relating such a Selmer group to $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})[\gamma_- - \chi(\gamma)]$. We leave it to the interested reader to do so. Instead we consider the Selmer group $\mathrm{Sel}_{\mathrm{BDP}}(E/K)$ defined to be the group

$$\ker\left\{H^1(G_{K,\Sigma}, E[p^\infty]) \overset{res}{\to} \prod_{w \in \Sigma, w \nmid p} H^1(K_w, E[p^\infty]) \times \frac{H^1(K_v, E[p^\infty])}{H^1(K_v, E[p^\infty])_{\mathrm{div}}} \times H^1(K_{\bar{v}}, E[p^\infty])\right\}.$$

Note that $\mathrm{Sel}_{\mathrm{BDP}}(E/K)$ is not a Bloch–Kato Selmer group: the local condition at the places $w \mid p$ is not that imposed by the Bloch–Kato subgroup $H^1_f(K_w, E[p^\infty])$. However, $\mathrm{Sel}_{\mathrm{BDP}}(E/K)$ is defined by a Selmer structure.

The control theorem of interest to us is:

Proposition 12. *Suppose E has good reduction at p and that* (irred$_K$) *holds. Suppose that* (split) *holds. Suppose also that $\mathrm{Sel}_{\mathrm{BDP}}(E/K)$ has finite order. Let Σ^+ be the set of places of K of residue degree 1 at which E has bad reduction. Then there is an exact sequence*

$$0 \to \mathrm{Sel}_{\mathrm{BDP}}(E/K) \to S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})[\gamma_- - 1] \to \prod_{w \in \Sigma^+} H^1_{\mathrm{ur}}(I_w, E[p^\infty]) \times K_v \times K_{\bar{v}} \to 0,$$

where

$$H_v = H^1(K_v, E[p^\infty])/H^1(K_v, E[p^\infty])_{\mathrm{div}} \cong H^1(K_v, T_pE)^\vee_{\mathrm{tors}} \cong H^0(K_v, E[p^\infty])^\vee,$$

and

$$H_{\bar{v}} = \ker\left\{H^1(K_{\bar{v}}, E[^\infty]) \to H^1(K_{\bar{v}}, M_{\mathrm{ac}})[\gamma_- - 1]\right\} \cong M_{\mathrm{ac}}^{G_{K_{\bar{v}}}}/(\gamma_- - 1)M_{\mathrm{ac}}^{G_{K_{\bar{v}}}}.$$

Note that $\#H_{\bar{v}} = \#H^0(K_{\bar{v}}, E[p^\infty])$. In particular, both H_v and $H_{\bar{v}}$ are trivial if E has supersingular reduction at p and otherwise both have order equal to $\#\mathbb{Z}_p/(1 - a_p(E) + p)$.

Write $N_E = N^+N^-$ with N^+ divisible by primes split or ramified in K and N^- divisible by primes inert in K.

Corollary 13. *Under the hypotheses of the preceding proposition,*

$$|\#S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})[\gamma_- - 1]|_p^{-1} = \left|\#\mathrm{Sel}_{\mathrm{BDP}}(E/K) \cdot \prod_{\ell|N^+} c_\ell(E/\mathbb{Q})^2 \cdot \delta_p(E)^2\right|_p^{-1},$$

where $\delta_p(E) = 1$ if E has supersingular reduction at p, and $\delta_p(E) = 1 - a_p(E) + p$ if E has good ordinary reduction at p.

3.4.4. $S_\pm(E/\mathbb{Q}_\infty)$. Kobayashi established a control theorem for the $\pm$-Selmer groups $S_\pm(E/\mathbb{Q}_\infty)$ which is the obvious analog of Proposition 5.

Proposition 14 (Control Theorem for the supersingular case)**.** *Suppose $E/\mathbb{Q}$ has good supersingular reduction at p with $a_p(E) = 0$ and that* (irred$_\mathbb{Q}$) *holds. Suppose also that $X_\pm(E/\mathbb{Q}_\infty)$ is a torsion Λ-module and that* $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ *is finite. Then there is an exact sequence*

$$0 \to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \to S_\pm(E/\mathbb{Q}_\infty)[\gamma - 1] \to \prod_{\ell\in\Sigma, \ell\neq p} \ker\{P_\ell \to \mathcal{P}_\ell[\gamma - 1]\} \to 0.$$

Under the hypothesis that $X_\pm(E/\mathbb{Q}_\infty)$ is a torsion Λ-module, B.D. Kim [35] has shown that $X_\pm(E/\mathbb{Q}_\infty)$ has no non-zero pseudonull submodule. As a consequence, just as in the ordinary case, we have

Proposition 15. *Suppose $E/\mathbb{Q}$ has good ordinary reduction at p and that* (irred$_\mathbb{Q}$) *holds. Suppose also that $X_\pm(E/\mathbb{Q}_\infty)$ is a torsion Λ-module and that* $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ *is finite. Let $g_{E,\pm}$ be a generator of the characteristic ideal $\xi_\pm(E/\mathbb{Q}_\infty) = \xi(X_\pm(E/\mathbb{Q}_\infty))$. Then*

$$|g_{E,\pm}(0)|_p^{-1} = \#S_\pm(E/\mathbb{Q}_\infty)[\gamma - 1] = \left|\#Ш(E/\mathbb{Q})[p^\infty] \cdot \prod_{\ell|N_E} c_\ell\right|_p^{-1}.$$

4. Main Conjectures

The Main Conjectures for elliptic curves generally have two ingredients: the characteristic ideal of the dual of the Selmer group and a related p-adic L-function, ideally both in some Λ. Then the conjecture generally has two parts: the torsion-ness over Λ of the dual of the Selmer group (and hence the non-vanishing of the characteristic ideal) and the assertion that the p-adic L-function generates the characteristic ideal. In some cases it is also possible to formulate a Main Conjecture 'without L-functions.' This generally means that the p-adic L-function has been replaced with some appropriate element in an Iwasawa cohomology group (a universal norm). These elements often come from an Euler system. The Main Conjectures without L-functions have proven useful in relating different Main Conjectures.

Let E be an elliptic curve over $\mathbb{Q}$. In the preceding section we defined Selmer groups for E and certain $\mathbb{Z}_p^d$-extensions F_∞/F. In the following we recall the Main Conjectures for these groups. In order to do so it is helpful to recall some facts about E and its L-series.

Recall that E is modular. This means there is a weight 2 newform $f_E \in S_2(\Gamma_0(N_E))$, where N_E is the conductor of E, such that the Fourier expansion $f_E = \sum_{n=1}^\infty a_n q^n$ has coefficients in $\mathbb{Z}$ and $L(E,s) = L(f_E,s) = \sum_{n=1}^\infty a_n n^{-s}$. It also means that there exists a surjective morphism $\phi_E : X_0(N_E) \to E$ over $\mathbb{Q}$ under which the ∞ cusp is mapped to the identity element (that is, the point at infinity) of E. The pullback under ϕ_E of a Néron differential ω_E of E satisfies $\phi_E^*\omega_E = c2\pi i f_E(\tau)d\tau = c\omega_{f_E}$, for some non-zero constant c.

4.1. **p-adic L-functions.** We first recall the p-adic L-functions that appear in the statements of the Main Conjectures.

4.1.1. *$\mathcal{L}(E/\mathbb{Q}_\infty)$ and $\mathcal{L}(E/K_\infty)$.* We begin with the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. We assume that E has good ordinary or multiplicative reduction at p.

Given a primitive p^tth-power root of unity ζ, recall that ψ_ζ is the finite order character of $G_\mathbb{Q}$ obtained by projecting to $\Gamma_\mathbb{Q}$ and composing with the character of $\Gamma_\mathbb{Q}$ that sends γ to ζ. Similarly, $\phi_\zeta : \Lambda \to \mathbb{Z}_p[\zeta] \subset \overline{\mathbb{Q}}_p$ is the homomorphism sending $\gamma \in \Gamma$ to ζ (so the homomorphism of $\Lambda_\mathbb{Q} = \mathbb{Z}_p[\![T]\!]$ sending T to $\zeta - 1$). We also denote by ψ_ζ the Dirichlet character of $(\mathbb{Z}/p^{t+1}\mathbb{Z})^\times$ such that image of $\gamma \in 1+p\mathbb{Z}_p$ is sent to ζ (unless $t = 0$, in which case ψ_1 is the trivial character).

There exists an element $\mathcal{L}(E/\mathbb{Q}_\infty) \in \Lambda_\mathbb{Q} = \mathbb{Z}_p[\![\Gamma_\mathbb{Q}]\!]$ such that for any primitive p^tth root of unity ζ,

$$\phi_\zeta(\mathcal{L}(E/\mathbb{Q}_\infty)) = e_p(\zeta)\frac{L(f_E,\psi_\zeta^{-1},1)}{\Omega_{f_E}},$$

where Ω_{f_E} is a certain (essentially canonical) period of f_E and

$$e_p(\zeta) = \begin{cases} \alpha_p^{-(t+1)}\frac{p^{t+1}}{G(\psi_\zeta^{-1})} & \zeta \neq 1 \\ \alpha_p^{-1}\left(1-\frac{1}{\alpha_p}\right)^{m_p} & \zeta = 1. \end{cases}$$

Here $L(f_E,\psi_\zeta^{-1},s)$ is the twist of the L-function of f_E by the Dirichlet character ψ_ζ^{-1}. Also, α_p is the p-adic unit root of $x^2 - a_p(E)X + p$ if E has good ordinary reduction at p and $\alpha = a_p(E) \in \{\pm 1\}$ if E has multiplicative reduction at p, $G(\psi_\zeta^{-1})$ is the Gauss sum, and $m_p = 2$ if E has good reduction at p and $m_p = 1$ if E has multiplicative reduction. This is the p-adic L-function of f_E first constructed by Amice-Vélu and Vishik (see also [46]).

Let K be an imaginary quadratic field and suppose that (split) holds (for simplicity). There exists an element $\mathcal{L}(E/K_\infty) \in \Lambda_K$ defined by an interpolation property for finite characters of Γ_K that is analogous to that of $\mathcal{L}(E/\mathbb{Q}_\infty)$. A construction of this p-adic L-function can be made through p-adic interpolation of Rankin–Selberg integrals, as done by Perrin-Riou [54] (see also [64]), or via modular symbols along the lines of the construction of $\mathcal{L}(E/\mathbb{Q}_\infty)$ by Amice-Vélu and Vishik (cf. [43]). The p-adic L-functions $\mathcal{L}(E/\mathbb{Q}_\infty)$ and $\mathcal{L}(E/K_\infty)$ are related by

$$\mathcal{L}(E/\mathbb{Q}_\infty)\mathcal{L}(E^K/\mathbb{Q}_\infty) = \mathcal{L}(E/K_\infty) \bmod (\gamma_- - 1). \tag{L-fact}$$

Here E^K is the K-twist of E (so $L(E^K,s) = L(E,\chi_K,s)$, where χ_K is the quadratic Dirichlet character associated with $K/\mathbb{Q}$).

4.1.2. $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$. We assume that (split) holds. For simplicity we will assume that the conductor N_E of E and the discriminant $-D_K$ of K are relatively prime and neither is divisible by p (this just simplifies some formulas).

Let $\Xi_{\mathrm{Gr}} \subset \mathrm{Hom}_{cts}(\Gamma_K, \overline{\mathbb{Q}}_p^\times)$ be the subset of characters such that the composition $G_K \twoheadrightarrow \Gamma_K \xrightarrow{\chi} \overline{\mathbb{Q}}_p$ is crystalline at both v and $\bar{v}$ and such that the Hodge–Tate weight at v is < -1 and at $\bar{v}$ is > 1. These are the Galois characters associated with unramified algebraic Hecke characters ψ of K such that the restriction of ψ to $(K \otimes \mathbb{R})^\times = \mathbb{C}^\times$ is just $z^n \bar{z}^{-m}$ for integers $n, m > 1$ and such that $n, m \equiv 0 \bmod p-1$. Given $\chi \in \Xi_{\mathrm{Gr}}$ we will write χ_{alg} for the corresponding algebraic Hecke character (so $\sigma_{\chi_{\mathrm{alg}}} = \chi$).

Let $\Lambda_K^{\mathrm{ur}} = \Lambda_K \hat{\otimes}_{\mathbb{Z}_p} \mathbb{Z}_p^{\mathrm{ur}}$, where $\mathbb{Z}_p^{\mathrm{ur}}$ is the p-adic completion of the ring of integers of the maximal unramified extension of $\mathbb{Q}_p$. Let $\chi : \Gamma_K \to \overline{\mathbb{Q}}_p^\times$ be a continuous character. Then χ determines a $\mathbb{Z}_p^{\mathrm{ur}}$-homomorphism $\phi_\chi : \Lambda_K^{\mathrm{ur}} = \mathbb{Z}_p^{\mathrm{ur}}[\![\Gamma_K]\!] \to \widehat{\overline{\mathbb{Q}}}_p$ by linear extension (it is the unique $\mathbb{Z}_p^{\mathrm{ur}}$-homomorphism such that $\phi_\chi(\gamma) = \chi(\gamma)$ for all $\gamma \in \Gamma_K \subset \Lambda_K^\times$).

There exists an element $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty) \in \Lambda_K^{\mathrm{ur}}$ such that for any $\chi \in \Xi_{\mathrm{Gr}}$,

$$\phi_\chi(\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)) = c(\chi) \cdot E(f,\chi) \cdot \pi^{2n-1} \left(\frac{\Omega_{K,p}}{\Omega_{K,\infty}}\right)^{2(n+m)} L(f_E, \chi_{\mathrm{alg}}^{-1}, 1),$$

where

$$E(f,\chi) = (1 - a_p(E)\chi_{\mathrm{alg}}(\varpi_v)^{-1}p^{-1} + \chi_{\mathrm{alg}}(\varpi_v)^{-2}p^{-1})(1 - a_p(E)\chi_{\mathrm{alg}}(\varpi_{\bar{v}})p^{-1} + \chi_{\mathrm{alg}}(\varpi_{\bar{v}})^2 p^{-1}),$$

with ϖ_v and $\varpi_{\bar{v}}$ respective uniformizers at v and $\bar{v}$, $c(\chi)$ is a product of powers of 2, i, N, and D_K that depend on on n and m but do not matter for our applications (as these factors are all prime to p), and $\Omega_{K,\infty}$ and $\Omega_{K,p}$ are, respectively, archimedean and p-adic CM periods associated to K. While the latter depend on choices, these choices only change the factors by a multiple of $(\mathbb{Z}_p^{\mathrm{ur}})^\times$.

As in the case of the p-adic L-function $\mathcal{L}(E/\mathbb{Q}_\infty)$, there exists an interpolation formula for characters $\chi : \Gamma_K \to \overline{\mathbb{Q}}_p^\times$ that are ramified at v or $\bar{v}$ but the same restrictions on Hodge–Tate weights. However, we will not go into this here.

There are essentially two constructions of $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ (and the two are closely related). The first realizes $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ as a special case of Hida's construction of p-adic Rankin–Selberg L-functions [29] involving a Hida family of CM eigenforms. The other realizes $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ as a p-adic L-function for a cuspform on a definite unitary group $U(2)$, constructed via the doubling method (see [70] and [16]).

Remark 4.1.2.a. It is possible to define a slight modification of $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ that is actually an element of Λ_K and not just Λ_K^{ur}. This requires normalizing the L-values by a 'congruence period' for the anticyclotomic character $\chi_{\mathrm{alg}}^{\mathrm{c}}/\chi_{\mathrm{alg}}$, but the result is less canonical.

Remark 4.1.2.b. It is also possible to construct $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ when $p \mid N_E$ or when $(N_E, D_K) \neq 1$, but the result is more cumbersome to write down.

4.1.3. $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$. We again assume that (split) holds and that the conductor N_E of E and the discriminant $-D_K$ of K are relatively prime, and neither is divisible by p. We also assume that $(\mathrm{irred})_{\mathbb{Q}}$ holds (as with the other hypotheses, this is mostly to simplify formulas). We make

the additional assumption that

(Heeg)
- $N_E = N^+N^-$ with N^+ divisible only by primes that split in K and N^- divisible only by primes that are inert in E;
- N^- is the squarefree product of an even number of distinct primes.

This is essentially the Heegner hypothesis. It ensures that the root number $w(E/K)$ equals -1, among other things. It also ensures that the sign of the functional equation of $L(f_E, \chi_{\mathrm{alg}}^{-1}, s)$ is $+1$ for any (anticyclotomic) character $\chi \in \Xi_{\mathrm{Gr}}$ that factors through Γ_K^{ac}.

Let $\Xi_{\mathrm{BDP}} \subset \mathrm{Hom}_{cts}(\Gamma_K^{\mathrm{ac}}, \overline{\mathbb{Q}}_p^\times)$ be the subset of characters such that the composition $G_K \twoheadrightarrow \Gamma_K^{\mathrm{ac}} \xrightarrow{\chi} \overline{\mathbb{Q}}_p$ is crystalline at both v and $\bar{v}$ and such that the Hodge–Tate weight at v is < -1 and at $\bar{v}$ is > 1. These are the Galois characters associated with unramified algebraic Hecke characters ψ of K such that the restriction of ψ to $(K \otimes \mathbb{R})^\times = \mathbb{C}^\times$ is just $(z/\bar{z})^n$ for and integer $n > 1$ and such that $n \equiv 0 \bmod p-1$. Note that these are also just the $\chi \in \Xi_{\mathrm{Gr}}$ that factor through the projection $\Gamma_K \twoheadrightarrow \Gamma_K^{\mathrm{ac}}$.

Let $\Lambda_{\mathrm{ac}}^{\mathrm{ur}} = \Lambda_{\mathrm{ac}} \hat{\otimes}_{\mathbb{Z}_p} \mathbb{Z}_p^{\mathrm{ur}}$. There exists an element $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) \in \Lambda_{\mathrm{ac}}^{\mathrm{ur}}$ such that for any $\chi \in \Xi_{\mathrm{BDP}}$,

$$\phi_\chi(\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})) = c(\chi) \cdot E(f,\chi) \cdot \pi^{2n-1} \left(\frac{\Omega_{K,p}}{\Omega_{K,\infty}}\right)^{4n} L(f_E, \chi_{\mathrm{alg}}^{-1}, 1) \prod_{\ell | N^-} c_\ell(E/K)^{-1},$$

where $E(f,\chi)$ and $c(\chi)$ are is in the interpolation formula for $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$, and $c_\ell(E/K)$ is the Tamagawa number for E/K at the prime ℓ of K.

This p-adic L-function was essentially constructed in [4] and [6] as the *square* of another p-adic funtion. This second p-adic L-function interpolates weighted sums of the values on CM points on a Shimura curve of powers of the Maass–Shimura operator applied to the modular form f_E (or of a Jacquet–Langlands transfer of f_E to the Shimura curve); the weights and the power of the operator vary with χ. This is just a p-adic interpolation of integral formulas of Waldspurger and Gross. The p-adic L-function resulting from the constructions in *op. cit.* may differ from the $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty)$ as we have described by multiplication by a unit in $\Lambda_{\mathrm{ac}}^{\mathrm{ur},\times}$. The factor $\prod_{\ell|N^-} c_\ell(E/K)^{-1}$ arises from the normalization of the Jacquet–Langlands transfer of f_E to the Shimura curve – it is at this point that we use the hypothesis that ($\mathrm{irred}_{\mathbb{Q}}$) holds.

Comparing interpolation formulas it is clear that:

Lemma 16. *Suppose* (split) *holds and that N_E is coprime to D_K and both are prime to p. Suppose also that* (Heeg) *and* ($\mathrm{irred}_{\mathbb{Q}}$) *hold. Then*

$$\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) \cdot \prod_{\ell|N^-} c_\ell(E/K) = \mathcal{L}_{\mathrm{Gr}}(E/K_\infty) \bmod (\gamma_+ - 1).$$

We record two other important facts about $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$. The first fact is of an Iwasawa-theoretic nature:

Theorem 17 ($\mu = 0$)**.** *Suppose all the hypotheses of Lemma 16 hold. Suppose also that N is squarefree. Then the μ-invariant of $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ is 0, that is, $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ is non-zero modulo p.*

This theorem was proved by Burungale [7, Thm. B]. Note that this includes the assertion that $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) \neq 0$, which is far from obvious!

The second fact is of clear arithmetic import:

Theorem 18 (The BDP formula)**.** *Suppose all the hypotheses of Lemma 16 hold. Suppose also that N is squarefree if $N^- \neq 1$. Then*

$$\phi_1(\mathcal{L}_{\mathrm{BDP}}) = u \left(\frac{1 - a_p(E) + p}{p} \cdot \log_{E(K_v)} y_K \right)^2$$

for some $u \in (\mathbb{Z}_p^{\mathrm{ur}})^\times$.

Here $y_K \in E(K)$ is a Heegner point associated with K and the parametrization of E by the Shimura curve (the same curve that occurs in the construction of $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$), and $\log_{E(K_v)}$ is the log map on the p-adic Lie group $E(K_v)$ defined by the formal group logarithm. Note that the trivial character 1 of Γ_K^{ac} does not belong to Ξ_{BDP}. Theorem 18 follows from the main results of [4] and [6].

4.1.4. $\mathcal{L}_\pm(E/\mathbb{Q}_\infty)$. This begins with a closer look at the constructions of Amice-Vélu and Vishik. Let E be an elliptic curve with good reduction at p. Let α_p and β_p be the roots of $x^2 - a_p(E)x + p$. Then Amice-Vélu and Vishik constructed two power series (this construction is also explained in [46])

$$\mathcal{L}(E, \bullet; T) \in \mathcal{H}_{1,\mathbb{Q}_p} = \left\{ \sum_{n=0}^{\infty} a_n T^n \in \mathbb{Q}_p[\![T]\!] \ : \ \lim_{n\to\infty} \frac{|a_n|_p}{n} = 0 \right\}, \bullet \in \{\alpha_p, \beta_p\},$$

with the property that for a primitive p^tth root of unity ζ,

$$\mathcal{L}(E, \bullet; \zeta - 1) = e_p(\zeta, \bullet) \frac{L(f_E, \psi_\zeta^{-1}, 1)}{\Omega_{f_E}},$$

where

$$e_p(\zeta, \bullet) = \begin{cases} (\bullet)^{-(t+1)} \frac{p^{t+1}}{G(\psi_\zeta^{-1})} & \zeta \neq 1 \\ \left(1 - \frac{1}{\bullet}\right)^2 & \zeta = 1. \end{cases}$$

However, the $\mathcal{L}(E, \bullet; T)$ do not belong to $\Lambda_{\mathbb{Q}} = \mathbb{Z}_p[\![T]\!]$ unless $\bullet$ is a p-adic unit (which is the case when E has ordinary reduction and $\bullet = \alpha_p$ is the unit root).

Now suppose that $a_p(E) = 0$, so $\beta_p = -\alpha_p$. Let

$$\log_p^+(1+T) = \frac{1}{p} \prod_{n=1}^{\infty} \frac{\Phi_{p^{2n}}(1+T)}{p} \quad \text{and} \quad \log_p^-(1+T) = \frac{1}{p} \prod_{n=1}^{\infty} \frac{\Phi_{p^{2n-1}}(1+T)}{p},$$

where $\Phi_{p^m}(X)$ is the p^mth cyclotomic polynomial. Pollack [52] has shown that there exist $\mathcal{L}_\pm(E/\mathbb{Q}_\infty) \in \Lambda_{\mathbb{Q}}$ such that

$$\mathcal{L}(E, \pm\alpha_p; T) = \log_p^+(1+T) \cdot \mathcal{L}_-(E/\mathbb{Q}_\infty) \pm \alpha_p \log_p^-(1+T) \cdot \mathcal{L}_+(E/\mathbb{Q}_\infty).$$

The functions $\mathcal{L}_\pm(E/\mathbb{Q}_\infty)$ have the following interpolation property. Suppose ζ is a primitive p^tth root of unity. If $t > 0$ is even, then

$$\phi_\zeta(\mathcal{L}_+(E/\mathbb{Q}_\infty)) = (-1)^{\frac{t+2}{2}} \frac{p^{t+1}}{G(\psi_\zeta^{-1})} \left(\prod_{\text{odd } m=1}^{t-1} \Phi_{p^m}(\zeta)^{-1} \right) \frac{L(f_E, \psi_\zeta^{-1}, 1)}{\Omega_{f_E}}.$$

If $t > 0$ is odd, then

$$\phi_\zeta(\mathcal{L}_-(E/\mathbb{Q}_\infty)) = (-1)^{\frac{t+1}{2}} \frac{p^{t+1}}{G(\psi_\zeta^{-1})} \left(\prod_{\text{even } m=2}^{t-1} \Phi_{p^m}(\zeta)^{-1} \right) \frac{L(f_E, \psi_\zeta^{-1}, 1)}{\Omega_{f_E}}.$$

Also,

$$\phi_1(\mathcal{L}_+(E/\mathbb{Q}_\infty)) = 2\frac{L(f_E,1)}{\Omega_{f_E}} \quad \text{and} \quad \phi_1(\mathcal{L}_-(E/\mathbb{Q}_\infty)) = (p-1)\frac{L(f_E,1)}{\Omega_{f_E}}.$$

Remark 4.1.4.c. Sprung [66] has extended Pollack's construction to cover the remaining supersingular cases, where $a_p(E) \neq 0$. It is also possible to extend the construction of $\mathcal{L}_\pm(E/\mathbb{Q}_\infty)$ to two-variable L-functions in Λ_K, at least when (split) holds. This yields 'doubly-signed' p-adic L-functions as it involves the choice of a root of $x^2 - a_p(E)x + p$ for each of the primes above p. Such a construction can be found in [43] (see also [44]).

4.2. **The Main Conjectures.** We are now in a position to state the Main Conjectures we are interested in.

4.2.1. *$S(E/\mathbb{Q}_\infty)$ and $S(E/K_\infty)$.* Let E be an elliptic curve over $\mathbb{Q}$. The Main Conjecture for $S(E/\mathbb{Q}_\infty)$ is just:

Conjecture 19 (The cyclotomic Iwasawa–Greenberg Main Conjecture for E)**.** *Suppose E has good ordinary or multiplicative reduction at p. The Pontryagin dual $X(E/\mathbb{Q}_\infty)$ of $S(E/\mathbb{Q}_\infty)$ is a torsion $\Lambda_\mathbb{Q}$-module and its characteristic ideal $\xi(E/\mathbb{Q}_\infty) = \xi(X(E/\mathbb{Q}_\infty))$ is generated by $\mathcal{L}(E/\mathbb{Q}_\infty)$ in $\Lambda_\mathbb{Q} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and even in $\Lambda_\mathbb{Q}$ if* ($\text{irred}_\mathbb{Q}$) *holds.*

This conjecture can be partially motivated by the combination of control theorems such as Propositions 5 and 8 and the Bloch–Kato conjectures on special values. The latter predicts that $\#(S(E/\mathbb{Q}_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Z}_p[\zeta])[\gamma - \zeta]$ should equal $\#\mathbb{Z}_p[\zeta]/\phi_\zeta(\mathcal{L}(E/\mathbb{Q}_\infty))$ – upon using the control theorem to relate the first group order with the size of a Bloch-Kato Selmer group and using the interpolation properties of the p-adic L-function to relate the second group order to a special value of an L-function. And since the first group order should be (upon assuming torsion-ness and no non-zero pseudonull submodule) $\#\mathbb{Z}_p[\zeta]/\phi_\zeta(g_E)$, for $g_E \in \xi(E/\mathbb{Q}_\infty)$ a generator, the most optimistic (and reasonable) conjecture to make is that g_E can be taken to be $\mathcal{L}(E/\mathbb{Q}_\infty)$.

The main conjecture for $S(E/K_\infty)$ is:

Conjecture 20 (The 2-variable Iwasawa–Greenberg Main Conjecture for E/K)**.** *Suppose E has good ordinary or multiplicative reduction at p. The Pontryagin dual $X(E/K_\infty)$ of $S(E/K_\infty)$ is a torsion Λ_K-module and its characteristic ideal $\xi(E/K_\infty) = \xi(X(E/K_\infty))$ is generated by $\mathcal{L}(E/K_\infty)$ in $\Lambda_K \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and even in Λ_K if* (irred_K) *holds.*

4.2.2. *$S_{\text{Gr}}(E/K_\infty)$.* At this point it should be easy to guess what the main conjecture for $S_{\text{Gr}}(E/K_\infty)$ is:

Conjecture 21 (The two-variable Iwasawa–Greenberg Main Conjecture for $S_{\text{Gr}}(E/K_\infty)$)**.** *Suppose E has good reduction at p. Let K be an imaginary quadratic field such that* (split) *holds. The Pontryagin dual $X_{\text{Gr}}(E/K_\infty)$ of $S_{\text{Gr}}(E/K_\infty)$ is a torsion Λ_K-module and its characteristic ideal $\xi_{\text{Gr}}(E/K_\infty) = \xi(X_{\text{Gr}}(E/K_\infty))$ is generated by $\mathcal{L}_{\text{Gr}}(E/K_\infty)$ in $\Lambda_K^{\text{ur}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and even in Λ_K^{ur} if* (irred_K) *holds.*

Note that unlike Conjecture 19, this conjecture allows E to have supersingular reduction at p.

4.2.3. $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$. An obvious variant on Conjecture 21 is:

Conjecture 22 (The anticyclotomic Main Conjecture for $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$)**.** *Suppose E has good or multiplicative reduction at p. Let K be an imaginary quadratic field such that* (split) *holds. The Pontryagin dual $X_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ of $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ is a torsion Λ_{ac}-module and its characteristic ideal $\xi_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) = \xi(X_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}))$ is generated by $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ in $\Lambda_{\mathrm{ac}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and even in Λ_{ac} if* (irred_K) *holds.*

Remark 4.2.3.a. Proposition 11 and Lemma 16 show that Conjectures 21 and 22 are closely connected. In particular, under the hypotheses of Lemma 16, it follows that Conjecture 21 implies Conjecture 22.

4.2.4. $S_\pm(E/\mathbb{Q}_\infty)$. Finally, we state the Main Conjecture for the $\pm$-Selmer groups:

Conjecture 23 (The cyclotomic $\pm$-Iwasawa Main Conjecture for E)**.** *Suppose E has supersingular reduction at p and $a_p(E) = 0$. The Pontryagin dual $X_\pm(E/\mathbb{Q}_\infty)$ of $S_\pm(E/\mathbb{Q}_\infty)$ is a torsion $\Lambda_{\mathbb{Q}}$-module and its characteristic ideal $\xi_\pm(E/\mathbb{Q}_\infty) = \xi(X_\pm(E/\mathbb{Q}_\infty))$ is generated by $\mathcal{L}_\pm(E/\mathbb{Q}_\infty)$ in $\Lambda_{\mathbb{Q}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and even in $\Lambda_{\mathbb{Q}}$ if* $(\mathrm{irred}_{\mathbb{Q}})$ *holds.*

4.3. **Main Conjectures without L-functions.** The classical Main Conjecture of Iwasawa theory has an equivalent formulation that does not involve p-adic L-functions. Following especially [34, §12], analogous formulations exist for the Main Conjectures of elliptic curves. In the rest of this section we give a rough description of this in some of the cases already considered in these lectures.

Let $E/\mathbb{Q}$ be an elliptic curve. We will assume that E has good ordinary reduction at p.

4.3.1. *The cyclotomic Main Conjecture.* For simplicity, we also assume $(\mathrm{irred}_{\mathbb{Q}})$ holds. Let

$$H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}}) = \ker \left\{ H^1(G_\Sigma, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}}) \overset{res}{\to} \prod_{\ell \in \Sigma, \ell \neq p} H^1(I_\ell, T \otimes \Lambda_{\mathbb{Q}}) \right\}.$$

Here we let $G_{\mathbb{Q}}$ act on $T \otimes \Lambda_{\mathbb{Q}}$ via $\rho \otimes \Psi$. Let

$$S_{\mathrm{str}}(E/\mathbb{Q}_\infty) = \ker \left\{ S(E/\mathbb{Q}_\infty) \to H^1(\mathbb{Q}_p, M) \right\} \quad \text{and} \quad X_{\mathrm{str}}(E/\mathbb{Q}_\infty) = S_{\mathrm{str}}(E/\mathbb{Q}_\infty)^\vee.$$

Kato has constructed, more-or-less naturally, a free $\Lambda_{\mathbb{Q}}$-module $Z_{\mathrm{Kato}} \subset H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})$. The Main Conjecture without L-function in this case asserts that $H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})$ is a torsion-free rank one $\Lambda_{\mathbb{Q}}$-module, that $Z_{\mathrm{Kato}} \neq 0$, and that

$$\xi(H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})/Z_{\mathrm{Kato}}) \overset{?}{=} \xi(X_{\mathrm{str}}(E/\mathbb{Q}_\infty)). \tag{IMC-noL}$$

The connection with Main Conjecture with L-function comes about as follows. Let

$$H^1_{/f}(\mathbb{Q}_p, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}}) = \frac{H^1(\mathbb{Q}_p, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})}{\mathrm{im}(H^1(\mathbb{Q}_p, T^+ \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}}))} = \left(\mathrm{im}(H^1(\mathbb{Q}_p, M^+))\right)^\vee,$$

where the second $=$ is the identification coming from local duality. Then there is a Coleman isomorphism

$$\mathrm{Col} : H^1_{/f}(\mathbb{Q}_p, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}}) \overset{\sim}{\to} \Lambda_{\mathbb{Q}}$$

of $\Lambda_{\mathbb{Q}}$-modules, which essentially interpolates the dual Bloch–Kato exponential maps for all the specializations $T(\psi_\zeta)$ of $T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}}$.

It is a consequence of global duality that there is an exact sequence

$$0 \to \frac{H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})}{Z_{\mathrm{Kato}}} \overset{res_p}{\to} \frac{H^1_{/f}(\mathbb{Q}_p, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})}{res_p(Z_{\mathrm{Kato}})} \overset{res_p^\vee}{\to} X(E/\mathbb{Q}_\infty) \to X_{\mathrm{str}}(E/\mathbb{Q}_\infty) \to 0.$$

Aside from the exactness on the left, this is just a special case of (SES). The left-exactness holds since $H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})$ is assumed to be a torsion-free $\Lambda_{\mathbb{Q}}$-module of rank one (part of the Main Conjecture without L-function) and since $\mathrm{Col}(res_p(Z_{\mathrm{Kato}})) = (\mathcal{L}(E/\mathbb{Q}_\infty))$, which has been proved by Kato, and since $\mathcal{L}(E/\mathbb{Q}_\infty) \neq 0$ by a result of Rohrlich [56]. Admitting the equality in the Main Conjecture without L-function and appealing to the previously mentioned results of Kato and Rohrlich, $H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})/Z_{\mathrm{Kato}}$, $H^1_{/f}(\mathbb{Q}_p, T \otimes \Lambda_{\mathbb{Q}})/res_p(Z_{\mathrm{Kato}})$, and $X_{\mathrm{str}}(E/\mathbb{Q}_\infty)$ are all torsion $\Lambda_{\mathbb{Q}}$-modules, hence so too is $X(E/\mathbb{Q}_\infty)$. Moreover, since characteristic ideals behave well in exact sequences, we also have

$$\xi(E/\mathbb{Q}_\infty) = \xi(H^1_{/f}(\mathbb{Q}_p, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})/Z_{\mathrm{Kato}}) = \xi(\Lambda_{\mathbb{Q}}/\mathrm{Col}(Z_{\mathrm{Kato}})) = (\mathcal{L}(E/\mathbb{Q}_\infty),$$

so the Main Conjecture with L-function follows.

Remark 4.3.1.a. The formulation of the cyclotomic Main Conjecture without L-function in (IMC-noL) makes sense even in the case of supersingular reduction at p. It is only in the connection to the Main Conjecture with L-function (Conjecture 19) that made use of ordinary reduction.

4.3.2. *The two-variable Main Conjectures for E/K_∞.* Let K be an imaginary quadratic field such that (split) holds. Let $H^1(\mathcal{O}_K[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_K)$ be defined in analogy with $H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})$. Let

$$H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K) = \ker\left\{ H^1(\mathcal{O}_K[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_K) \overset{res}{\to} \frac{H^1(K_v, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{\mathrm{im}(H^1(K_v, T^+ \otimes_{\mathbb{Z}_p} \Lambda_K)} \right\},$$

and let $S_{\mathrm{ord,str}}(E/K_\infty) \subset S(E/K_\infty)$ be the subgroup of classes whose restriction at the place $\bar{v}$ is trivial.

Lei, Loeffler, and Zerbes [42] have constructed a free Λ_K-submodule $Z_{\mathrm{LLZ}} \subset H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)$ (essentially norm-compatible systems of their Beilinson–Flach elements – this also requires varying them in Hida families (cf. [37])). The Main Conjecture without L-function in this case is that $H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)$ is a torsion-free Λ_K-module of rank one, that $Z_{\mathrm{LLZ}} \neq 0$, and

$$\xi(H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)/Z_{\mathrm{LLZ}}) \overset{?}{=} \xi(X_{\mathrm{ord,str}}(E/K_\infty)), \quad X_{\mathrm{ord,str}}(E/K_\infty) = S_{\mathrm{ord,str}}(E/K_\infty)^\vee.$$

One of the remarkable features of this Main Conjecture without L-function is that it is also related to the Main Conjecture with L-function for both $S_{\mathrm{Gr}}(E/K_\infty)$ and $S(E/K_\infty)$. It implies two distinct Main Conjectures!

The connection with the two-variable Main Conjecture for $S_{\mathrm{Gr}}(E/K_\infty)$ comes via the exact sequence:

$$0 \to \frac{H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{Z_{\mathrm{LLZ}}} \overset{res_v}{\to} \frac{\mathrm{im}(H^1(K_v, T^+ \otimes_{\mathbb{Z}_p} \Lambda_K)}{res_v(Z_{\mathrm{LLZ}})} \overset{res_v^\vee}{\to} X_{\mathrm{Gr}}(E/K_\infty) \to X_{\mathrm{ord,str}}(E/K_\infty) \to 0.$$

Other than the exactness on the left, this sequence is just a special case of (SES). The exactness on the left follows from the assumption that $H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)$ is a torsion-free Λ_K-module of rank one together with $res_v(Z_{\mathrm{LLZ}})$ being non-torsion. The latter follows from a suitably normalized version of Perrin-Riou's 'big logarithm' map $\mathrm{Log}_v : \mathrm{im}(H^1(K_v, T^+ \otimes_{\mathbb{Z}_p} \Lambda_K) \otimes_{\Lambda_K} \Lambda_K^{\mathrm{ur}} \overset{\sim}{\to} \Lambda_K^{\mathrm{ur}}$ and the expectation (essentially proved by Lei, Loeffler, and Zerbes) that $\mathrm{Log}_v(Z_{\mathrm{LLZ}}) =$

($\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ together with the non-vanishing of $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ (which is easier to prove than for $\mathcal{L}(E/\mathbb{Q}_\infty)$). The argument concluding the Main Conjecture with L-functions now proceeds as before.

The connection with the two-variable Main Conjecture for $S(E/K_\infty)$ comes about via a second exact sequence:

$$0 \to \frac{H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{Z_{\mathrm{LLZ}}} \overset{res_{\bar{v}}}{\to} \frac{H^1_{/f}(K_{\bar{v}}, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{res_{\bar{v}}(Z_{\mathrm{LLZ}}))} \overset{res^\vee_{\bar{v}}}{\to} X(E/K_\infty) \to X_{\mathrm{ord,str}}(E/K_\infty) \to 0,$$

where as before $H^1_{/f}(K_w, T \otimes_{\mathbb{Z}_p} \Lambda_K) = H^1(K_w, T \otimes_{\mathbb{Z}_p} \Lambda_K)/\mathrm{im}(H^1(K_w, T^+ \otimes_{\mathbb{Z}_p} \Lambda_K)$. The key to this second sequence is the Coleman isomorphism $\mathrm{Col}_{\bar{v}} : H^1_{/f}(K_{\bar{v}}, T \otimes_{\mathbb{Z}_p} \Lambda_K) \overset{\sim}{\to} \Lambda_K$ and the expectation that $\mathrm{Col}_{\bar{v}}(Z_{\mathrm{LLZ}}) = (\mathcal{L}(E/K_\infty))$ (essentially proved by Kings, Loeffler, and Zerbes) and the non-vanishing of $\mathcal{L}(E/K_\infty)$ (which follows from (L-fact) and the aforementioned result of Rohrlich). The argument again proceeds as before.

4.3.3. *The Heegner point Main Conjecture.* Before the work of Kato and Lei–Loeffler–Zerbes, Perrin-Riou [53] formulated an anticyclotomic Main Conjecture for $S(E/K^{\mathrm{ac}}_\infty)$ in cases where the Heegner hypotheses (such as (Heeg)) hold. Let

$$H^1_{\mathrm{ord}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathrm{ac}}) = \ker \left\{ H^1(\mathcal{O}_K[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathrm{ac}}) \overset{res}{\to} \prod_{w|p} \frac{H^1(K_w, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathrm{ac}})}{\mathrm{im}(H^1(K_w, T^+ \otimes_{\mathbb{Z}_p} \Lambda_{\mathrm{ac}})} \right\}.$$

The Heegner points over the ring class fields of $K[p^n]$ form norm-compatible sequences in $H^1_{\mathrm{ord}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathrm{ac}})$ that generate a free Λ_{ac}-submodule $Z_{\mathrm{Heeg}} \subset H^1_{\mathrm{ord}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathrm{ac}})$. In this case Perrin-Riou's anticyclotomic Main Conjecture is that $X(E/K^{\mathrm{ac}}_\infty) \sim \Lambda_{\mathrm{ac}} \oplus N \oplus N$ for N a torsion Λ_{ac}-module and that

$$\xi(N) \overset{?}{=} c_E^{-1} \xi(H^1_{\mathrm{ord}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathrm{ac}})/Z_{\mathrm{Heeg}}),$$

where c_E is the Manin constant for the modular parameterization of E (by the Shimura curve dictated by the hypothesis (Heeg)). This conjecture is closely connected with the Main Conjecture for $S_{\mathrm{BDP}}(E/K^{\mathrm{ac}}_\infty)$.

5. Theorems and ideas of their proofs

We recall a few of the results, some recent, towards proofs of the Main Conjectures stated earlier. We also try to give some idea of their proofs.

5.1. **Cyclotomic Main Conjectures: the ordinary case.** We begin, as always, with the case of the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. One result that encompasses many instances of the Main Conjecture for this case is:

Theorem 24. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Let $p \geq 3$ be a prime at which E has good ordinary or multiplicative reduction. Suppose that* ($\mathrm{irred}_{\mathbb{Q}}$) *holds. Suppose also that there exists a prime $\ell \,||\, N_E$, $\ell \neq p$, such that $E[p]$ is ramified at ℓ. Then the Iwasawa–Greenberg Main Conjecture for $S(E/\mathbb{Q}_\infty)$ is true. In particular, $X(E/\mathbb{Q}_\infty)$ is a torsion $\Lambda_{\mathbb{Q}}$-module and*

$$\xi(E/\mathbb{Q}_\infty) = (\mathcal{L}(E/\mathbb{Q}_\infty)) \subseteq \Lambda_{\mathbb{Q}}.$$

The proof of this theorem is contained in [34] [64] [63].

5.1.1. *Remarks on related results.* Of course, there are many other interesting results toward this case of the Main Conjectures for elliptic curves. We comment on a few:

- The Main Conjecture for a CM elliptic curve with ordinary reduction at p (which is excluded by this theorem because of the hypothesis on some $\ell \,||\, N_E$) was proved much earlier by Rubin [58].
- Kato's divisibility ((Div-1) below) also holds, at least in $\Lambda_{\mathbb{Q}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$, when (irred$_{\mathbb{Q}}$) fails to. Greenberg and Vatsal [26] exploited this and the classical Main Conjecture for Dirichlet characters to deduce the cyclotomic Main Conjecture for some elliptic curves E for which $E[p]$ is a reducible $G_{\mathbb{Q}}$-representation. In the same paper Greenberg and Vatsal pioneered a method of showing that when the analytic and algebraic Iwasawa μ-invariants vanish, the Main Conjecture for one elliptic curve E (or eigenform f) implies the Main Conjecture for any congruent elliptic curve (or eigenform). These ideas were then further developed by Emerton, Pollack, and Weston [17].
- Results of Grigorov [27] and more recently of Kim, Kim, and Sun [36] make it possible to 'numerically verify' instances of the cyclotomic Main Conjecture (showing that is implied by some value being prime-to-p). This yields examples of the cyclotomic Main Conjecture for elliptic curves with, say, squarefull conductors.

5.1.2. *Idea of the proof of Theorem 24.* Theorem 24 was proved in two big steps and one smaller one.

In the first step, Kato proved that $X(E/\mathbb{Q}_\infty)$ is a torsion $\Lambda_{\mathbb{Q}}$-module and that

$$(\mathcal{L}(E/\mathbb{Q}_\infty)) \subseteq \xi(E/\mathbb{Q}_\infty) \quad \text{if } E \text{ has good ordinary reduction at } p. \tag{Div-1}$$

This was done by an Euler system argument. To be precise, the argument requires that E have good reduction at p as well as the existence of an element $\sigma \in G_{\mathbb{Q}}$ that fixes $\mathbb{Q}_\infty$ and is such that $T/(\sigma - 1)T$ is a free $\mathbb{Z}_p$-module of rank 1. The hypothesis that $E[p]$ is ramified at some $\ell \,||\, N_E$, $\ell \neq p$, ensures the existence of such an element σ.

In the second step, Urban and the lecturer showed that if K is an imaginary quadratic field of discriminant $-D_K$ such that (a) $(D_K, 4Np) = 1$, (b) p splits in K, and (c) $N_E = N^- N^+$ with N^- (resp. N^+) divisible only by primes that are inert in K (resp. split in K) and N^- is the square-free product of an odd number of primes ℓ such that $E[p]$ is ramified at ℓ, then

$$\xi(E/\mathbb{Q}_\infty)\xi(E^K/\mathbb{Q}_\infty) \subseteq (\mathcal{L}(E/\mathbb{Q}_\infty)\mathcal{L}(E^K/\mathbb{Q}_\infty)) \subseteq \Lambda_{\mathbb{Q}}. \tag{Div-2}$$

Here E^K is the K-twist of E.

Suppose now that E is as in the statement of the theorem. It is easy to see that it is always possible to choose K so that all the hypotheses required for (Div-2) are satisfied. If in addition E has good ordinary reduction, then combining (Div-1) (for both the curve E and its K-twist E^K, which will also have good ordinary reduction at p) with (Div-2) yields the Main Conjecture for E.

The final step is to extend this result to include those E with multiplicative reduction. This was done in [63]. The argument there uses the fact that the results in [34] and [64] actually prove the Main Conjecture for p-ordinary newforms $f \in S_k(\Gamma_0(N))$, $p \nmid N$, with $k \equiv 2 \bmod p - 1$. A simple congruence argument then shows that the Main Conjecture for an E with multiplicative reduction at p can be deduced from the Main Conjectures for such f. The key point is that f_E, the newform associated with E, is a p-adic limit of such newforms f.

As noted, Kato's proof of (Div-1) goes via Euler systems. In particular, it involves progress toward the Main Conjecture without L-function for E as in Section 4.3. More precisely, Kato constructs an Euler system for T. The base of this Euler system, when it is non-zero, is a rank one $\Lambda_{\mathbb{Q}}$-module $Z_{\mathrm{Kato}} \subset H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})$. The machinery of Euler systems then proves that in this case $H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})$ is a free $\Lambda_{\mathbb{Q}}$-module of rank one and that

$$\xi(H^1(\mathbb{Z}[\frac{1}{p}], T \otimes_{\mathbb{Z}_p} \Lambda_{\mathbb{Q}})/Z_{\mathrm{Kato}}) \subseteq \xi(X_{\mathrm{str}}(E/\mathbb{Q}_\infty)).$$

Furthermore, via a deep 'explicit reciprocity law' Kato also shows that $\mathrm{Col}(Z_{\mathrm{Kato}}) = (\mathcal{L}(E/\mathbb{Q}_\infty))$. Then arguing much as in Section 4.3.1 yields both that $X(E/\mathbb{Q}_\infty)$ is torsion and (Div-1).

To try to say much about the proof of (Div-2) would take us far afield of the focus of these lectures. So suffice it to say that the proof is an extensive generalization of the Eisenstein congruence arguments used in Wiles's proof [73] of the Iwasawa Main Conjecture for totally real fields. Moreover, (Div-2) is actually just a consequence of the main theorem in [64], which is in fact an inclusion towards a three-variable Main Conjecture: the extra variables come from including f_E, the newform associated with E, in a Hida family and working with the extension K_∞/K. The very rough idea is to first construct a three-variable p-adic family of Eisenstein series on $GU(2,2)$ whose constant term is divisible by this three-variable L-function. Then to show that this Eisenstein family is coprime to the p-adic L-function by showing that for any height one prime divisor of the p-adic L-function there is some Fourier coefficient that is not divisible by this height one prime. Finally, use the Galois representations associated to cuspidal families on $GU(2,2)$ that are congruent to this Eisenstein family (by the preceding steps, these congruences are 'measured' by the p-adic L-function) to construct classes in the appropriate Selmer group.

5.2. **The Main Conjectures for $S_{\mathrm{Gr}}(E/K_\infty)$ and $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$.** Recently, progress has been made towards the Main Conjectures for $S_{\mathrm{Gr}}(E/K_\infty^{\mathrm{ac}})$ and $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$. One result that encompasses some of this progress is:

Theorem 25. *Let E be either a semistable elliptic curve or a quadratic twist of such a curve. Suppose E has good reduction at p and that* (irred$_{\mathbb{Q}}$) *holds. Suppose also that there exists a prime $\ell \,||\, N_E$, $\ell \neq p$, such that $E[p]$ is ramified at ℓ. Let K be an imaginary quadratic field with discriminant $-D_K$. Suppose* (split) *holds, $(D_K, N_E) = 1$, and ℓ is inert in K. Suppose also that* (Heeg) *holds.*

(i) *$X_{\mathrm{Gr}}(E/K_\infty)$ is a torsion Λ_K^{ur}-module and $X_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ is a torsion $\Lambda_{\mathrm{ac}}^{\mathrm{ur}}$-module.*
(ii) *There exists an element $0 \neq a \in \Lambda_{\mathrm{cyc}}^{\mathrm{ur}} = \mathbb{Z}_p^{\mathrm{ur}}[\![\Gamma_K^{\mathrm{cyc}}]\!]$ such that $a \cdot \xi_{\mathrm{Gr}}(E/K_\infty)^{\mathrm{ur}} \subseteq (\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)) \subset \Lambda_K^{\mathrm{ur}}$.*
(iii) *$\xi_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})^{\mathrm{ur}} \subseteq (\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})) \subset \Lambda_{\mathrm{ac}}^{\mathrm{ur}}$.*
(iv) *If $p \nmid c_\ell(E/K)$ for all $\ell \mid N^-$, then* (i) *holds with $a = 1$.*

Here we have written $\xi_?(\cdot)^{\mathrm{ur}}$ to mean $\xi_?(\cdot)\Lambda_{??}^{\mathrm{ur}}$. Part (ii) of this theorem is essentially the main results of [70] and [71]. The element a in (i) can be taken to be divisible only by height one primes of $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ that are of the form $P\Lambda_K^{\mathrm{ur}}$ for some height one prime $P \subset \Lambda_{\mathrm{cyc}}^{\mathrm{ur}}$.

Combining Theorem 25 with results toward the cyclotomic Main Conjecture, via arguments like those in Section 4.3.2, yields case of the Main Conjectures for $S_{\mathrm{Gr}}(E/K_\infty)$ and $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$. For example:

Theorem 26. *Let E be either a semistable elliptic curve or a quadratic twist of such a curve. Suppose E has good ordinary reduction at p and that* (irred$_{\mathbb{Q}}$) *holds. Suppose also that there exists a prime $\ell \,||\, N_E$, $\ell \neq p$, such that $E[p]$ is ramified at ℓ. Let K be an imaginary quadratic field with discriminant $-D_K$. Suppose* (split) *holds, $(D_K, N_E) = 1$, and ℓ is inert in K. Suppose also that* (Heeg) *holds and that $p \nmid c_\ell(E/K)$ for all $\ell \mid N^-$. Then $X_{\mathrm{Gr}}(E/K_\infty)$ is a torsion Λ_K^{ur}-module and $X_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ is a torsion $\Lambda_{\mathrm{ac}}^{\mathrm{ur}}$-module, and*

$$\xi_{\mathrm{Gr}}(E/K_\infty)^{\mathrm{ur}} = (\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)) \subset \Lambda_K^{\mathrm{ur}} \quad \textit{and} \quad \xi_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})^{\mathrm{ur}} = (\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})) \subset \Lambda_{\mathrm{ac}}^{\mathrm{ur}}.$$

That is, the Main Conjectures for $S_{\mathrm{Gr}}(E/K_\infty)$ and $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ hold.

5.2.1. *Idea of the proofs of Theorems 25 and 26.* Part (i) of Theorem 25 is a relatively easy consequence of work of Cornut and Vatsal [10] together with the theorems of Gross–Zagier and Kolyvagin (as extended by others to Heegner points coming from Shimura curve parameterizations). In particular, by [10, Thm. 1.5] there is some finite order character χ of Γ_K^{ac} such that $L'(f_E, \chi_{\mathrm{alg}}^{-1}, 1) \neq 0$. Let $\mathcal{O}$ be the ring of integers of the finite extension L of $\mathbb{Q}_p$ containing the values of χ. Let $W = E[p^\infty] \otimes_{\mathbb{Z}_p} \mathcal{O}(\chi^{-1})$. It then follows from the Gross–Zagier theorem and Kolyvagin's Euler system argument that $H_f^1(K, W)$ has $\mathcal{O}$-corank 1, with the $\mathcal{O}$-divisible part generated by the image of Heegner points. A simple Galois cohomology argument, such as appears in Section 6.2 below, then shows that $H^1_{\mathrm{BDP}}(K, W)$ is finite, where by $H^1_{\mathrm{BDP}}(K, W)$ we mean the group of classes that are trivial at all places except v. A control theorem argument like that of Proposition 12 shows that the dual $H^1_{\mathrm{BDP}}(K, W)^\vee$ is a quotient of $X_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) \otimes_{\mathbb{Z}_p} \mathcal{O}$ mod $(\gamma_- - \chi(\gamma_-))$ with a finite order kernel. It follows that $X_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ is a torsion Λ_{ac}-module. It then follows similarly from Proposition 11 that $X_{\mathrm{Gr}}(E/K_\infty)$ is a torsion Λ_K-module.

Part (ii) is a consequence of the main results in [70] and [71], in much the same way that (Div-2) is a consequence of the main result in [64]. These main results are also inclusions toward three-variable main conjectures, the additional variable arising from including f_E in a Hida or Coleman family. Again, the very rough idea is to first construct a three-variable p-adic family of Eisenstein series, in this case on $GU(3,1)$, whose constant term is divisible by the three-variable L-function. Then to show that this Eisenstein family is coprime to the p-adic L-function. This step is complicated by the fact that forms on $GU(3,1)$ do not have Fourier expansions, only Fourier–Jacobi expansions. And then, once this is done, use the Galois representations associated to cuspidal families on $GU(3,1)$ that are congruent to this Eisenstein family (by the preceding steps, these congruences are 'measured' by the p-adic L-function) to construct classes in the appropriate Selmer group.

The passage from (ii) to (iii) follows from combining Proposition 11, Lemma 16, and Theorem 17. To make this work one must also note that Lemma 16 together with $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) \neq 0$ (see Theorem 17) imply that $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ (and hence a) is not divisible by $\gamma_+ - 1$.

The stronger conclusion of (iv) follows since if $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ had a divisor of the form $P\Lambda_K$ for some height one prime $P \subset \Lambda_{\mathrm{cyc}}^{\mathrm{ur}}$, then $\mathcal{L}_{\mathrm{Gr}}(E/K_\infty)$ mod $(\gamma_+ - 1)$ would be divisible by P mod $(\gamma_+ - 1)$, which is a power of p (we already observed that P mod $(\gamma_+ - 1)$ is non-zero when passing from (ii) to (iii)). But this would contradict Theorem 17.

To deduce Theorem 26 from Theorem 25, one can argue much as in Section 4.3.2. As $X_{\mathrm{Gr}}(E/K_\infty)$ is a torsion Λ_K-module by part (i) of Theorem 25, so too is its quotient $X_{\mathrm{ord,str}}(E/K_\infty)$. The latter being torsion implies that $H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K) = 0$ (here we use (irred$_K$)). This in turn

implies that there is an exact sequence

$$0 \to \frac{H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{Z_{\mathrm{LLZ}}} \overset{res_v}{\to} \frac{\mathrm{im}(H^1(K_v, T^+ \otimes_{\mathbb{Z}_p} \Lambda_K)}{res_v(Z_{\mathrm{LLZ}})} \overset{res_v^\vee}{\to} X_{\mathrm{Gr}}(E/K_\infty) \to X_{\mathrm{ord,str}}(E/K_\infty) \to 0.$$

Part (iv) of Theorem 25 implies that

$$\xi(X_{\mathrm{Gr}}(E/K_\infty)) \subseteq \xi(\frac{\mathrm{im}(H^1(K_v, T^+ \otimes_{\mathbb{Z}_p} \Lambda_K)}{res_v(Z_{\mathrm{LLZ}})}),$$

hence

$$\xi(X_{\mathrm{ord,str}}(E/K_\infty)) \subseteq \xi(\frac{H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{Z_{\mathrm{LLZ}}}).$$

Furthermore, each of these inclusions is an equality if the other is. We will explain that the second inclusion is an equality, hence so is the first.

By noting that $S(E/K_\infty)[\gamma_- - 1] \cong S(E/\mathbb{Q}_\infty) \oplus S(E^K/\mathbb{Q}_\infty)$, one readily sees that $X(E/K_\infty)$ is a torsion Λ_K-module (since $X(E/\mathbb{Q}_\infty)$ and $X(E^K/\mathbb{Q}_\infty)$ are both torsion $\Lambda_{\mathbb{Q}}$-modules). It follows that $H^1_{\mathrm{ord}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K) = 0$ (here we again use that (Heeg_K) holds. It then follows that there is an exact sequence

$$0 \to \frac{H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{Z_{\mathrm{LLZ}}} \overset{res_{\bar{v}}}{\to} \frac{H^1_{/f}(K_{\bar{v}}, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{res_{\bar{v}}(Z_{\mathrm{LLZ}}))} \overset{res_{\bar{v}}^\vee}{\to} X(E/K_\infty) \to X_{\mathrm{ord,str}}(E/K_\infty) \to 0,$$

As $\xi(X_{\mathrm{ord,str}}(E/K_\infty)) \subseteq \xi(H^1_{\mathrm{ord,rel}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_K)/Z_{\mathrm{LLZ}}$, it follows that

$$\xi(X(E/K_\infty)) \subseteq \xi(\frac{H^1_{/f}(K_{\bar{v}}, T \otimes_{\mathbb{Z}_p} \Lambda_K)}{res_{\bar{v}}(Z_{\mathrm{LLZ}}))}) = (\mathcal{L}(E/K_\infty)).$$

And again, each inclusion is an equality if the other is. But by reducing the last equation modulo $(\gamma_- - 1)$ and appealing to the cyclotomic Main Conjecture for both E and E^K (or even just Kato's divisibilities Div-1), we conclude that this last inclusion is an equality. Hence so are the others. This proves the Main Conjecture for $S_{\mathrm{Gr}}(E/K_\infty)$. The Main Conjecture for $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ essentially follows by reducing modulo $(\gamma_+ - 1)$.

5.2.2. *Remarks on related results.*

- Wan's results actually allow D_K and N to have prime factors in common. This is important for some applications.
- Wan also proved a version of Theorem 25(ii) when (Heeg) is replaced by a condition that allows the root number $w(E/K)$ to equal $+1$. In this case $\mathcal{L}_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}}) = 0$ and $X_{\mathrm{BDP}}(E/K_\infty)$ is not torsion.
- A careful read of the deduction of Theorem 26 from Theorem 25 shows that it actually gives a second proof of the cyclotomic Main Conjecture for E and E^K! (This is so, as one can get away with appealing to Kato's divisibility at the crucial step.)
- Wan has a modification of these results that allows many of the arguments to be applied to E with supersingular reduction at p [71]. A summary of some of this is in [9].

5.3. **Cyclotomic Main Conjectures: the supersingular case.** The work of Wan, in combination with the Beilinson–Flach elements of Lei–Loeffler–Zerbes, has provided a means to approach the cyclotomic Main Conjectures for $S_\pm(E/\mathbb{Q}_\infty)$ when E has supersingular reduction at p and $a_p(E) = 0$.

Theorem 27. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Suppose that E is either a semistable curve or a quadratic twist of such. Let $p \geq 3$ be a prime at which E has supersingular reduction and $a_p(E) = 0$. Suppose that* (irred$_{\mathbb{Q}}$) *holds. Suppose also that there exists a prime $\ell \,||\, N_E$, $\ell \neq p$, such that $E[p]$ is ramified at ℓ. Then the Main Conjecture for $S_{\pm}(E/\mathbb{Q}_\infty)$ is true. In particular, $X_{\pm}(E/\mathbb{Q}_\infty)$ is a torsion $\Lambda_{\mathbb{Q}}$-module and*

$$\xi_{\pm}(E/\mathbb{Q}_\infty) = (\mathcal{L}_{\pm}(E/\mathbb{Q}_\infty)) \subseteq \Lambda_{\mathbb{Q}}.$$

The proof of this theorem combines work of Kobayashi [38] and Wan [71]. The argument essentially follows as indicated in the third remark of Section 5.2.2, only everything is decorated with a subscript $\pm$ and Kato's divisibility is replaced with Kobayashi's.

5.3.1. *Remarks on related results.*

- The Main Conjecture for a *CM* elliptic curve with supersingular reduction at p was proved earlier by Pollack and Rubin [55].
- The Main Conjecture for $S_{\pm}(E/\mathbb{Q}_\infty)$ is equivalent to the Kato's Main Conjecture without L-functions for E; the equivalence runs along the same lines as described for the ordinary case in Section 4.3.1.
- Sprung [66] [67] has extended Theorem 27 to include those E with supersingular reduction at p but with $a_p(E) \neq 0$.

5.4. **Perrin-Riou's Heegner point Main Conjecture.** The proofs of the Main Conjectures with L-functions described so far have both invoked progress toward Main Conjectures *without* L-functions and resulted in the proof of such in many cases. This is one more.

Theorem 28. *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E and good ordinary reduction at p. Suppose that N is either a semistable curve or a quadratic twist of a semistable curve. Suppose* (irred$_{\mathbb{Q}}$) *holds. Let K be an imaginary quadratic field of discriminant $-D_K$ such that* (split) *holds. Suppose that N_E and D_K are relatively prime and that* (Heeg) *holds. Suppose further that $N^- \neq 1$ and $p \nmid c_\ell(E/K)$ for all $\ell \mid N^-$. Then Perrin-Riou's Heegner point Main Conjecture is true. That is,*

(a) *$X(E/K_\infty^{\mathrm{ac}}) \sim \Lambda_{\mathrm{ac}} \oplus N \oplus N$ with N a torsion Λ_{ac}-module, and*
(b) *$\xi(N) = \xi(H^1_{\mathrm{ord}}(K, T \otimes_{\mathbb{Z}_p} \Lambda_{\mathrm{ac}})/Z_{\mathrm{Heeg}})$.*

Here, the $\sim$ in (a) means that there is a Λ_{ac} homomorphism with pseudonull kernel and cokernel (this is reflexive). See Section 4.3.3 for definition of the terms in the statement of (b).

Part (a) of this theorem was known from earlier work of Bertolini, Cornut, and Nekovář, while Howard [30] [31] proved the inclusion $\supseteq$ in (b). Wan [72] showed that equality could be deduced from Howard's inclusion in combination with his work on the Main Conjecture for $S_{\mathrm{Gr}}(E/K_\infty)$.

Remark 5.4.0.a. Castella and Wan [9] have formulated and proved a version of the Heegner point Main Conjecture when E has supersingular reduction at p and $a_p(E) = 0$.

6. Arithmetic consequences

By this point the reader will have recognized that many of the theorems towards the Main Conjectures for elliptic curves have interesting consequences, especially for the (conjectured) Birch–Swinnerton-Dyer formula. We explain a few in the following.

6.1. **Results when $L(E,1) \neq 0$.** As an almost immediate consequence of Theorem 24 and the control theorems and especially Proposition 10, we have:

Theorem 29. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Let $p \geq 3$ be a prime at which E has good ordinary or multiplicative reduction. Suppose that* $(\mathrm{irred}_{\mathbb{Q}})$ *holds. Suppose also that there exists a prime $\ell \,||\, N_E$, $\ell \neq p$, such that $E[p]$ is ramified at ℓ. If $L(E,1) \neq 0$, then*

$$\left|\frac{L(E,1)}{\Omega_E}\right|_p^{-1} = \left|\#Ш(E/\mathbb{Q}) \cdot \prod_{\ell | N_E} c_\ell\right|_p^{-1}.$$

Additional argument is required when E has split multiplicative reduction at p due to the trivial zero of $\mathcal{L}(E/\mathbb{Q}_\infty)$ at $T = 0$. The details of this case are included in [63]. We have written $\#Ш(E/\mathbb{Q})$ and not just $\#Ш(E/\mathbb{Q})[p^\infty]$ as it is known by the work of Kolyvagin that when $L(E,1) \neq 0$ the Tate–Shafaravich group $Ш(E/\mathbb{Q})$ has finite order.

The corresponding result for the case of supersingular reduction, a consequence of Theorem 27 and Proposition 15 is just:

Theorem 30. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Suppose that E is either semistable or a quadratic twist of a semistable curve. Let $p \geq 3$ be a prime at which E has good supersingular reduction with $a_p(E) = 0$. Suppose that* $(\mathrm{irred}_{\mathbb{Q}})$ *holds. Suppose also that there exists a prime $\ell \,||\, N_E$, $\ell \neq p$, such that $E[p]$ is ramified at ℓ. If $L(E,1) \neq 0$, then*

$$\left|\frac{L(E,1)}{\Omega_E}\right|_p^{-1} = \left|\#Ш(E/\mathbb{Q}) \cdot \prod_{\ell | N_E} c_\ell\right|_p^{-1}.$$

6.2. **Results when $L(E,1) = 0$.** The Main Conjecture also has consequences when $L(E,1) = 0$. Again combining Theorem 24 and the control theorems, one can deduce:

Theorem 31. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Let $p \geq 3$ be a prime at which E has good ordinary or multiplicative reduction. Suppose that* $(\mathrm{irred}_{\mathbb{Q}})$ *holds. Suppose also that there exists a prime $\ell \,||\, N_E$, $\ell \neq p$, such that $E[p]$ is ramified at ℓ. If $L(E,1) = 0$, then $\#\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) = \infty$ and so its $\mathbb{Z}_p$-corank is at least one. Moreover, if E does not have split multiplicative reduction at p and $\mathrm{ord}_{s=1}L(E,s)$ is even and positive, then the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is at least two.*

The key point here is that if $L(E,1) = 0$ then $g_E(0) = 0$, so by Lemma 4 we have $\#S(E/\mathbb{Q}_\infty)[\gamma - 1] = \infty$. By the arguments used to establish the control theorems we have an exact sequence

$$0 \to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \to S(E/\mathbb{Q}_\infty)[\gamma - 1] \to \prod_{\ell \in \Sigma} K_\ell.$$

As the groups on the right are finite (at least if E does not have split multiplicative reduction), then $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ has infinite order if and only if $S(E/\mathbb{Q}_\infty)[\gamma - 1]$ does. The modifications of

this argument needed to handle the case of split multiplicative reduction at p are included in [63]. The claim about the $\mathbb{Z}_p$-corank being at least two follows from combining the result that the $\mathbb{Z}_p$-corank being positive with the proof of the parity conjecture by Nekovář [50].

The analog of this theorem in the supersingular case is:

Theorem 32. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N_E. Suppose that E is either semistable or a quadratic twist of a semistable curve. Let $p \geq 3$ be a prime at which E has supersingular reduction and $a_p(E) = 0$. Suppose that* $(\mathrm{irred}_{\mathbb{Q}})$ *holds. Suppose also that there exists a prime $\ell \,||\, N_E$, $\ell \neq p$, such that $E[p]$ is ramified at ℓ. If $L(E,1) = 0$, then $\#\mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) = \infty$ and so its $\mathbb{Z}_p$-corank is at least one. Moreover, if E does not have split multiplicative reduction at p and $\mathrm{ord}_{s=1}L(E,s)$ is even and positive, then the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is at least two.*

Remark 6.2.0.a. Theorems 31 and 32 provide some evidence toward the Birch–Swinnerton-Dyer Conjecture. This conjecture asserts that if $L(E,1) = 0$ then $E(\mathbb{Q})$ has positive rank, and the fundamental exact sequence $0 \to E(\mathbb{Q})\otimes\mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_{p^\infty}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p^\infty] \to 0$ then shows that $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ must have $\mathbb{Z}_p$-corank at least one. Moreover, if the order of vanishing is at least two, then the rank of $E(\mathbb{Q})$ should be at least two and hence the $\mathbb{Z}_p$-corank of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ should be at least two. So the conclusions of the theorems agree with implications of the Birch–Swinnerton-Dyer Conjecture. Furthermore, assuming that $Ш(E/\mathbb{Q})$ is finite, we can conclude the expected facts about the rank of $E(\mathbb{Q})$!

6.3. **Results when** $\mathrm{ord}_{s=1}L(E,s) = 1$**.** Suppose the analytic rank of E is 1, that is, the order of vanishing at $s = 1$ of the L-function $L(E,s)$ is 1. Then we know from the work of Gross, Zagier, and Kolyvagin that $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q}) = 1$ and $Ш(E/\mathbb{Q})$ is finite. It is even known that $L'(E,1)/\Omega_E \cdot R(E/\mathbb{Q}) \in \mathbb{Q}^\times$. What can be said regarding its conjectured value (the Birch–Swinnerton-Dyer formula (BSD-f))? The following theorem is progress toward this:

Theorem 33. *Let E be a semistable elliptic curve and p a prime of good reduction such that $a_p(E) = 0$ if E has supersingular reduction at p. Suppose* $(\mathrm{irred})_{\mathbb{Q}}$ *holds. If E has analytic rank one, then*

$$\left|\frac{L'(E,1)}{\Omega_E R(E/\mathbb{Q})}\right|_p^{-1} = \left|\#Ш(E/\mathbb{Q}) \prod_{\ell|N_E} c_\ell(E/\mathbb{Q})\right|_p^{-1}.$$

A proof of this theorem is given in [32]. This proof combines the Gross–Zagier theorem [28] [74] with Kolyvagin's Euler system argument [41] and with the results toward the Main Conjecture for $S_{\mathrm{BDP}}(E/K_\infty^{\mathrm{ac}})$ and Theorems 29 and 30. These arguments have been extended to the case of multiplicative reduction by Castella [8].

6.3.1. *Remarks on related results.*

- Cases of Theorem 33 have also been proved by Zhang [75] and by Berti, Bertolini, and Venerucci [3]. Each of these imposes some restrictions on the primes $\ell \mid N_E$ at which p is allowed to divide $c_\ell(E/\mathbb{Q})$. Furthermore, each also appeals to Theorem 29.
- The supersingular case of Theorem 33 has also been proved by Kobayashi [39] as a consequence of a remarkable result on the non-vanishing of the p-adic height of the Heegner point when E has supersingular reduction at p. This proof, too, appeals to the Theorems 27 and 30.

6.3.2. *Idea of the proof of Theorem 33.* We give a quick sketch of the proof of Theorem 33.

One first chooses an auxiliary imaginary quadratic field such that the hypotheses of Theorem 25 hold and $L(E^K,1)\neq 0$ (so $\mathrm{ord}_{s=1}L(E/K,s)=1$). The theorems of Gross–Zagier and Kolyvagin then give a non-torsion Heegner point $y_K\in E(K)$ that generates a subgroup of finite index. From parts (i) and (iii) of Theorem 25 together with Corollary 13 one deduces that

$$\left|\frac{1-a_p(E)+p}{p}\cdot \log_{E(K_v)} y_K\right|_p^{-2} \leq \left|\#\mathrm{Sel}_{\mathrm{BDP}}(E/K)\cdot \prod_{\ell|N^+} c_\ell(E/\mathbb{Q})^2\cdot \delta_p(E)^2\right|_p^{-1}$$

Using that $\mathrm{Sel}_{p^\infty}(E/K)\twoheadrightarrow E(K_v)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p/\mathbb{Z}_p$ (since the image of y_K has infinite order in $E(K_v)$) together with $\mathrm{rank}_{\mathbb{Z}}E(K)=1$, a simple Galois cohomological argument shows that

$$\#\mathrm{Sel}_{\mathrm{BDP}}(E/K)=\#Ш(E/K)[p^\infty]\cdot[E(K_v)/E(K_v)_{\mathrm{tors}}:\mathbb{Z}_p\cdot y_K]^2.$$

Substituting this into the preceding inequality yields

$$[E(K)\otimes_{\mathbb{Z}}\mathbb{Z}_p:\mathbb{Z}_p\cdot y_K]^2\leq \left|\#Ш(E/K)[p^\infty]\cdot\prod_{\ell|N^+}c_\ell(E/\mathbb{Q})^2\right|_p^{-1}.$$

The Gross–Zagier formula expresses $\frac{L'(E,1)}{\Omega_{E/K}R(E/\mathbb{Q})}$ in terms of the square of the index $[E(K):\mathbb{Z}\cdot y_K]$ and ratio of the degree of the modular parametrization of E and the degree of the Shimura curve parametrization of E (the latter gives rise to y_K). Using a result of Ribet and Takahashi on the p-part of the latter, we can conclude that

$$\left|\frac{L'(E/K,1)}{\Omega_{E/K}R(E/K)}\right|_p^{-1}\leq \left|\#Ш(E/K)[p^\infty]\prod_{\ell|N_E}c_\ell(E/K)\right|_p^{-1}.$$

Since $L(E/K,s)$ factors as $L(E/K,s)=L(E,s)L(E^K,s)$, $L'(E/K,1)=L'(E,1)L(E^K,1)$. A comparison of periods shows that since (irred_K) holds, $\Omega_{E/K}$ is a p-adic unit multiple of $\Omega_E\Omega_{E^K}$. Furthermore, $R(E/\mathbb{Q})$ is just $R(E/K)$ since $E^K(\mathbb{Q})$ is finite. So we have

$$\left|\frac{L'(E/K,1)}{\Omega_{E/K}R(E/K)}\right|_p^{-1}=\left|\frac{L'(E,1)}{\Omega_E R(E/\mathbb{Q})}\right|_p^{-1}\cdot\left|\frac{L(E^K,1)}{\Omega_{E^K}}\right|_p^{-1}.$$

On the other hand, $Ш(E/K)[p^\infty]=Ш(E/\mathbb{Q})[p^\infty]\oplus Ш(E^K/\mathbb{Q})[p^\infty]$ and $\prod_{\ell|N_E}c_\ell(E/K)$ equals $\prod_{\ell|N_E}c_\ell(E/\mathbb{Q})\cdot\prod_{\ell|N_{E^K}}c_\ell(E^K/\mathbb{Q})$ up to a power of 2. It follows that

$$\left|\#Ш(E/K)[p^\infty]\prod_{\ell|N^+}c_\ell(E/K)\right|_p^{-1}=\left|\#Ш(E/\mathbb{Q})[p^\infty]\prod_{\ell|N_E}c_\ell(E/\mathbb{Q})\right|_p^{-1}$$
$$\times\left|\#Ш(E^K/\mathbb{Q})[p^\infty]\prod_{\ell|N_{E^K}}c_\ell(E^K/\mathbb{Q})\right|_p^{-1}.$$

Combining the last three displayed equations with Theorems 29 and 30 for $L(E^K,1)$ we conclude that

$$\left|\frac{L'(E,1)}{\Omega_E R(E/\mathbb{Q})}\right|_p^{-1} \leq \left|\#Ш(E/\mathbb{Q})[p^\infty]\prod_{\ell|N_E} c_\ell(E/\mathbb{Q})\right|_p^{-1}.$$

This is the upper bound predicted by the Birch–Swinnerton-Dyer formula.

To achieve the predicted lower bound, we choose a possibly *different* quadratic field K such that (split) and (Heeg) hold, $L(E^K,1)\neq 0$, and $p\nmid c_\ell(E/\mathbb{Q})$ for all $\ell \mid N^+$. Then Kolyvagin's Heegner point Euler system argument yields

$$[E(K)\otimes_{\mathbb{Z}}\mathbb{Z}_p : \mathbb{Z}_p\cdot y_K]^2 \geq \left|\#Ш(E/K)[p^\infty]\cdot\prod_{\ell|N^+} c_\ell(E/\mathbb{Q})^2\right|_p^{-1}.$$

Arguing as above we now conclude that

$$\left|\frac{L'(E,1)}{\Omega_E R(E/\mathbb{Q})}\right|_p^{-1} \geq \left|\#Ш(E/\mathbb{Q})[p^\infty]\prod_{\ell|N_E} c_\ell(E/\mathbb{Q})\right|_p^{-1}.$$

Equality follows.

Remark 6.3.2.a. For the argument sketched above to always apply, one actually needs to be able to choose K so that D_K and N_E are possibly not coprime (see the first remark in Section 5.2.2). This is primarily to be able to deal with the case where N_E is a prime (or E is a quadratic twist of a such a curve).

6.4. **Converses to Gross–Zagier/Kolyvagin.** If E has analytic rank one, then the theorems of Gross, Zagier, and Kolyvagin imply that $\mathrm{rank}_{\mathbb{Z}}E(\mathbb{Q})$ is one and $Ш(E/\mathbb{Q})$ is finite. In particular, the corank of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is one. Conversely, as noted (see (BSD-crk)), admitting the conjectures of Birch–Swinnerton-Dyer and the finiteness of the Tate-Shafarevich group, if the corank of $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is one, then E has analytic rank one. Can this converse can be made unconditional?

The following theorem is an example of what one can prove about this:

Theorem 34. *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N_E and good ordinary reduction at p. Suppose E is semistable. Suppose* $(\mathrm{irred}_{\mathbb{Q}})$ *holds. If* $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ *has corank one, then* $\mathrm{ord}_{s=1}L(E,s)=1$. *In particular, $E(\mathbb{Q})$ has rank one and $Ш(E/\mathbb{Q})$ is finite.*

This is essentially in [72]. An analog for the case of supersingular reduction is proved in [9].

The idea of the proof of Theorem 34 is as follows. One begins by choosing an imaginary quadratic field K so that E and K satisfy the hypotheses of Theorem 28 and $L(E^K,1)\neq 0$. It follows from the theorems of Gross, Zagier, and Kolyvagin that $\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})$ is finite, so the corank of $\mathrm{Sel}_{p^\infty}(E/K)=\mathrm{Sel}_{p^\infty}(E/\mathbb{Q})\oplus\mathrm{Sel}_{p^\infty}(E^K/\mathbb{Q})$ is also one. A control theorem argument shows that $\mathrm{Sel}_{p^\infty}(E/K)\subset S(E/K_\infty)[\gamma_- -1]$ with finite index, so $X(E/K_\infty^{\mathrm{ac}})/(\gamma_- -1)X(E/K_\infty^{\mathrm{ac}})$ has rank one. Then it follows from part (a) of Theorem 28 that $N/(\gamma_- -1)N$ is finite. It then follows from part (b) of the same theorem that the image of Z_{Heeg} in

$$H^1_{\mathrm{ord}}(K,T\otimes\mathbb{Z}_p\Lambda_{\mathrm{ac}})/(\gamma_- -1)H^1_{\mathrm{ord}}(K,T\otimes\mathbb{Z}_p\Lambda_{\mathrm{ac}})\hookrightarrow H^1_{\mathrm{ord}}(K,T)\cong\mathbb{Z}_p.$$

has finite index. But this image of Z_{Heeg} is spanned by the Heegner point y_K. So y_K is non-torsion. It then follows from the Gross–Zagier theorem that $\mathrm{ord}_{s=1}L(E/K,s) = 1$, and this, together with $L(E^K,1) \neq 0$, implies that $\mathrm{ord}_{s=1}L(E,s) = 1$.

Remark 6.4.0.a. Variants on this theorem have also been proved by the lecturer [62] and Zhang [75] [65] and Venerucci [69]. Such converses to Gross–Zagier were a key piece of the arguments in [1] and [2] that show that a positive proportion of elliptic curves have both algebraic and analytic rank one.

References

[1] Manjul Bhargava and Christopher Skinner, *A positive proportion of elliptic curves over $\mathbb{Q}$ have rank one*, J. Ramanujan Math. Soc. **29** (2014), no. 2, 221–242.

[2] Manjul Bhargava, Christopher Skinner, and Wei Zhang, *A positive proportion of elliptic curves over $\mathbb{Q}$ have rank one*, arXiv:1401.0233.

[3] Andrea Berti, Massimo Bertolini, and Rodolfo Venerucci, *Congruences between modular forms and the Birch and Swinnerton-Dyer conjecture*, Elliptic curves, modular forms and Iwasawa theory, Springer Proc. Math. Stat., vol. 188, Springer, Cham, 2016, pp. 1–31.

[4] Massimo Bertolini, Henri Darmon, and Kartik Prasanna, *Generalized Heegner cycles and p-adic Rankin L-series*, Duke Math. J. **162** (2013), no. 6, 1033–1148. With an appendix by Brian Conrad.

[5] Spencer Bloch and Kazuya Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

[6] Ernest Hunter Brooks, *Shimura curves and special values of p-adic L-functions*, Int. Math. Res. Not. IMRN **12** (2015), 4177–4241.

[7] Ashay A. Burungale, *On the non-triviality of the p-adic Abel-Jacobi image of generalised Heegner cycles modulo p, II: Shimura curves*, J. Inst. Math. Jussieu **16** (2017), no. 1, 189–222.

[8] Francesc Castalla, *On the p-part of the Birch-Swinnerton-Dyer formula for multiplicative primes*, Camb. J. Math. (to appear).

[9] Francesc Castella and Xin Wan, *Perrin-Riou's main conjecture for elliptic curves at supersingular primes*, arXiv:1607.02019.

[10] Christophe Cornut and Vinayak Vatsal, *Nontriviality of Rankin-Selberg L-functions and CM points*, L-functions and Galois representations, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, pp. 121–186.

[11] Kęstutis Česnavičius, *Selmer groups as flat cohomology groups*, J. Ramanujan Math. Soc. **31** (2016), no. 1, 31–61.

[12] John Coates, *p-adic L-functions and Iwasawa's theory*, Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 269–353.

[13] J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), no. 3, 223–251.

[14] Pierre Colmez, *La conjecture de Birch et Swinnerton-Dyer p-adique*, Astérisque **294** (2004), ix, 251–319.

[15] Henri Darmon, Fred Diamond, and Richard Taylor, *Fermat's last theorem*, Current developments in mathematics, 1995 (Cambridge, MA), Int. Press, Cambridge, MA, 1994, pp. 1–154.

[16] Ellen Eischen, Michael Harris, Jian-Shu Li, and Christopher Skinner, *p-adic L-functions for unitary groups*, arXiv:1602.01776.

[17] Matthew Emerton, Robert Pollack, and Tom Weston, *Variation of Iwasawa invariants in Hida families*, Invent. Math. **163** (2006), no. 3, 523–580.

[18] Jean-Marc Fontaine and Bernadette Perrin-Riou, *Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 599–706.

[19] Ralph Greenberg, *On p-adic L-functions and cyclotomic fields*, Nagoya Math. J. **56** (1975), 61–77.

[20] ———, *Iwasawa theory for p-adic representations*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 97–137.

[21] ———, *Iwasawa theory for motives*, L-functions and arithmetic (Durham, 1989), London Math. Soc. Lecture Note Ser., vol. 153, Cambridge Univ. Press, Cambridge, 1991, pp. 211–233.

[22] ———, *Iwasawa theory and p-adic deformations of motives*, Motives (Seattle, WA, 1991), Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 193–223.

[23] ———, *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, pp. 51–144.
[24] ———, *Introduction to Iwasawa theory for elliptic curves*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 407–464.
[25] ———, *On the structure of certain Galois cohomology groups*, Doc. Math. **Extra Vol.** (2006), 335–391.
[26] Ralph Greenberg and Vinayak Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), no. 1, 17–63.
[27] Grigor Tsankov Grigorov, *Kato's Euler system and the Main Conjecture*, ProQuest LLC, Ann Arbor, MI, 2005. Thesis (Ph.D.)–Harvard University.
[28] Benedict H. Gross and Don B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.
[29] Haruzo Hida, *A p-adic measure attached to the zeta functions associated with two elliptic modular forms. II*, Ann. Inst. Fourier (Grenoble) **38** (1988), no. 3, 1–83.
[30] Benjamin Howard, *The Heegner point Kolyvagin system*, Compos. Math. **140** (2004), no. 6, 1439–1472.
[31] ———, *Iwasawa theory of Heegner points on abelian varieties of* GL_2 *type*, Duke Math. J. **124** (2004), no. 1, 1–45.
[32] Dimitar Jetchev, Christopher Skinner, and Xin Wan, *The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one*, Camb. J. Math. **5** (2017), no. 3, 369–434.
[33] Kazuya Kato, *Lectures on the approach to Iwasawa theory for Hasse-Weil L-functions via* B_{dR}. *I*, Arithmetic algebraic geometry (Trento, 1991), Lecture Notes in Math., vol. 1553, Springer, Berlin, 1993, pp. 50–163.
[34] ———, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), ix, 117–290. Cohomologies *p*-adiques et applications arithmétiques. III.
[35] Byoung Du Kim, *The plus/minus Selmer groups for supersingular primes*, J. Aust. Math. Soc. **95** (2013), no. 2, 189–200.
[36] C-H. Kim, M. Kim, and H-S. Sun, *On the indivisibility of derived Kato's Euler systems and the Main Conjecture for modular forms*, arXiv:1709.05780v2.
[37] Guido Kings, David Loeffler, and Sarah Livia Zerbes, *Rankin-Eisenstein classes and explicit reciprocity laws*, Camb. J. Math. **5** (2017), no. 1, 1–122.
[38] Shin-ichi Kobayashi, *Iwasawa theory for elliptic curves at supersingular primes*, Invent. Math. **152** (2003), no. 1, 1–36.
[39] ———, *The p-adic Gross-Zagier formula for elliptic curves at supersingular primes*, Invent. Math. **191** (2013), no. 3, 527–629.
[40] Antonio Lei, David Loeffler, and Sarah Livia Zerbes, *Wach modules and Iwasawa theory for modular forms*, Asian J. Math. **14** (2010), no. 4, 475–528.
[41] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.
[42] Antonio Lei, David Loeffler, and Sarah Livia Zerbes, *Euler systems for Rankin-Selberg convolutions of modular forms*, Ann. of Math. (2) **180** (2014), no. 2, 653–771.
[43] David Loeffler, *p-adic integration on ray class groups and non-ordinary p-adic L-functions*, Iwasawa theory 2012, Contrib. Math. Comput. Sci., vol. 7, Springer, Heidelberg, 2014, pp. 357–378.
[44] David Loeffler and Sarah Livia Zerbes, *Iwasawa theory and p-adic L-functions over* $\mathbb{Z}_p^2$*-extensions*, Int. J. Number Theory **10** (2014), no. 8, 2045–2095.
[45] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61.
[46] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1–48.
[47] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), no. 2, 179–330.
[48] Barry Mazur and Karl Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96.
[49] J. S. Milne, *Arithmetic duality theorems*, 2nd ed., BookSurge, LLC, Charleston, SC, 2006.
[50] Jan Nekovář, *On the parity of ranks of Selmer groups. II*, C. R. Acad. Sci. Paris Sér. I Math. **332** (2001), no. 2, 99–104.
[51] ———, *Selmer complexes*, Astérisque **310** (2006), viii+559 (English, with English and French summaries).
[52] Robert Pollack, *On the p-adic L-function of a modular form at a supersingular prime*, Duke Math. J. **118** (2003), no. 3, 523–558.
[53] Bernadette Perrin-Riou, *Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), no. 4, 399–456 (French, with English summary).
[54] ———, *Fonctions L p-adiques associées à une forme modulaire et à un corps quadratique imaginaire*, J. London Math. Soc. (2) **38** (1988), no. 1, 1–32 (French).

[55] Robert Pollack and Karl Rubin, *The main conjecture for CM elliptic curves at supersingular primes*, Ann. of Math. (2) **159** (2004), no. 1, 447–464.
[56] David E. Rohrlich, *On L-functions of elliptic curves and anticyclotomic towers*, Invent. Math. **75** (1984), no. 3, 383–408.
[57] Karl Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), no. 3, 527–559.
[58] ———, *The "Main Conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), no. 1, 25–68.
[59] ———, *Euler systems and modular elliptic curves*, Galois representations in arithmetic algebraic geometry (Durham, 1996), London Math. Soc. Lecture Note Ser., vol. 254, Cambridge Univ. Press, Cambridge, 1998, pp. 351–367.
[60] A. J. Scholl, *An introduction to Kato's Euler systems*, Galois representations in arithmetic algebraic geometry (Durham, 1996), London Math. Soc. Lecture Note Ser., vol. 254, Cambridge Univ. Press, Cambridge, 1998, pp. 379–460.
[61] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.
[62] Christopher Skinner, *A converse to a theorem of Gross, Zagier, and Kolyvagin*, arXiv:1405.7294.
[63] ———, *Multiplicative reduction and the cyclotomic Main Conjecture for* GL_2, Pacific J. Math. **283** (2016), no. 1, 171–200.
[64] Christopher Skinner and Eric Urban, *The Iwasawa Main Conjectures for* GL_2, Invent. Math. **195** (2014), no. 1, 1–277.
[65] Christopher Skinner and Wei Zhang, *Indivisibility of Heegner points in the multiplicative case*, arXiv:1407.1099.
[66] Florian E. Ito Sprung, *Iwasawa theory for elliptic curves at supersingular primes: a pair of main conjectures*, J. Number Theory **132** (2012), no. 7, 1483–1506.
[67] ———, *The Iwasawa Main Conjecture for elliptic curves at odd supersingular primes*, arXiv:1610.10017.
[68] John Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Dix exposés sur la cohomologie des schémas, Adv. Stud. Pure Math., vol. 3, North-Holland, Amsterdam, 1968, pp. 189–214.
[69] Rodolfo Venerucci, *On the p-converse of the Kolyvagin-Gross-Zagier theorem*, Comment. Math. Helv. **91** (2016), no. 3, 397–444.
[70] Xin Wan, *Iwasawa Main Conjecture for Rankin–Selberg p-adic L-functions*, arXiv:1408.4044.
[71] ———, *Iwasawa Main Conjecture for supersingular elliptic curves*, arXiv:1411.6352.
[72] ———, *Heegner point Kolyvagin system and Iwasawa Main Conjecture*, arXiv:1408.4043.
[73] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. (2) **131** (1990), no. 3, 493–540.
[74] Shouwu Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2) **153** (2001), no. 1, 27–147.
[75] Wei Zhang, *Selmer groups and the indivisibility of Heegner points*, Camb. J. Math. **2** (2014), no. 2, 191–253.

Department of Mathematics, Princeton University, Fine Hall, Washington Road, Princeton, NJ 08544-1000, USA

E-mail address: cmcls@princeton.edu