Tamagawa defect of Euler systems

Kâzım Büyükboduk [1]

IHÉS, Le Bois-Marie, 35, Route de Chartres F-91440 Bures-sur-Yvette FRANCE

Abstract

As remarked by Mazur an Rubin (2004, *Mem. Amer. Math. Soc.*, 168(799)) one does not expect the Kolyvagin system obtained from an Euler system for a p-adic Galois representation T to be *primitive* (in the sense of *loc. cit.*) if p divides a Tamagawa number at a prime $\ell \neq p$; thus fails to compute the correct size of the relevant Selmer module. In this paper we obtain a lower bound for the size of the cokernel of the Euler system to Kolyvagin system map in terms of the local Tamagawa numbers of T, refining a result of *loc. cit.*. We show how this partially accounts for the missing Tamagawa factors in Kato's calculations with his Euler system.

Key words: Euler systems, Kolyvagin systems, Tamagawa Numbers, the Birch and Swinnerton-Dyer Conjecture.

1 Introduction

Let $p > 2$ be a rational prime and let $\mathcal{O}$ be the ring of integers of a finite extension of $\mathbb{Q}_p$. Denote the maximal ideal of $\mathcal{O}$ by $\mathfrak{m}$ and fix a generator π of $\mathfrak{m}$. Let T be a free $\mathcal{O}$-module of finite rank, on which the absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts continuously, and the action of $G_{\mathbb{Q}}$ on T is unramified outside a finite number of places. For such a T, the notion of an Euler system (which is originally due to Kolyvagin (Kol90)) has been generalized in Rubin (Rub00), Kato (Kato99) and Perrin-Riou (PR98) to prove upper bounds for the Selmer group attached to the Cartier dual T^* of the Galois representation T.

Email address: kazim@math.stanford.edu (Kâzım Büyükboduk).
URL: http://www.ihes.fr/∼kazim (Kâzım Büyükboduk).

[1] Supported by the Williams Hodge fellowship of IHÉS.

Starting from an Euler system, Kolyvagin uses his descent argument to obtain what he calls *derivative classes*. These derivative classes are used to produce bounds for the dual Selmer group. (MR04) starts exactly with these classes, and they observe that the derivative classes enjoy stronger local conditions than has been previously utilized. Classes with these stronger local conditions (and with the same interrelations that the derivative classes ought to satisfy) are called *Kolyvagin systems*. We refer the reader to (MR04, §3) for a detailed description. Since Kolyvagin systems are modeled after the derivative classes, they have exactly the same applications, namely they give upper bounds for the dual Selmer group. In fact, Mazur and Rubin exploits the extra rigidity gained by their observation to prove, in many cases of interest, that the Kolyvagin system bound on the dual Selmer group is strict and in fact one could completely determine the structure of the dual Selmer group in terms of a Kolyvagin system (if the Kolyvagin system we use is *primitive* in the sense of Definition 17 below); see (MR04, Theorems 4.5.6, 4.5.9 and 5.2.14).

The discussion above already portrays Kolyvagin systems as more fundamental objects than Euler systems. In fact, it is also possible to prove that Kolyvagin systems exist in many cases, however, it is impossible to write these down explicitly in full generality. The only cases where the bound provided by a Kolyvagin system can be made explicit are the cases where the Kolyvagin system used comes from an Euler system, via Kolyvagin's descent. This map from the collection of Euler systems to the collection of Kolyvagin systems will be referred to as the *Euler system to Kolyvagin system map*; see Theorem 18 below for a slightly more detailed description of this map.

One important feature of the bounds provided by a Kolyvagin system obtained from one of the Euler systems known to date is that they are closely related to the special values of L-functions. Such bounds thus provide evidence for the Bloch-Kato conjectures (BK90), which predict the orders of these Selmer groups in terms of the special values of a relevant L-function.

A natural question to ask is when these bounds given by an Euler system (or, equivalently, by the Kolyvagin system obtained from it) are sharp. In view of the results of (MR04), this is equivalent to (under certain technical assumptions) asking when the Kolyvagin system obtained from the Euler system we started with is primitive. For example, consider Kato's Euler system (Kat04), which is an Euler system for $T = T_p(E)$, the p-adic Tate module of an elliptic curve $E_{/\mathbb{Q}}$. As explained in (MR04, Remark 6.2.5), Kato's Euler system does not give rise to a primitive Kolyvagin system if p divides one of the Tamagawa numbers of E. In fact they prove that the Euler system to Kolyvagin system map in this setting has non-trivial cokernel if p divides a Tamagawa number, and as a result it is impossible to obtain a primitive Kolyvagin system from an Euler system in this case. We call this phenomenon the *Tamagawa defect of Euler systems*.

However, the arguments of (MR04) (particularly Proposition 6.2.6 of *loc. cit.*) is not sufficient to obtain an improved lower bound on the size of this cokernel in terms the Tamagawa factors. This is what we do in this paper:

Theorem A *Suppose π^n divides a Tamagawa number of the Galois representation T. Under suitable hypotheses on T (cf. the statement of Theorem 23) the image of the Euler system to Kolyvagin system map (of Theorem 18) is contained in $\mathfrak{m}^n\mathbf{KS}(T)$, where $\mathbf{KS}(T)$ denotes the $\mathcal{O}$-module of Kolyvagin systems for T.*

See Theorem 23 below for details.

In particular, the hypotheses of Theorem A hold when $T = T_p(E)$, i.e. when T is the p-adic Tate module of an elliptic curve $E_{/\mathbb{Q}}$ with conductor N. Let κ^{Kato} denote the Kolyvagin system obtained from Kato's Euler system, as in (MR04, §6.2). Let c_ℓ be the Tamagawa number of E at ℓ, and suppose $p^n | c_\ell$.

Theorem B $\kappa^{\mathrm{Kato}} \in p^n\mathbf{KS}(T)$.
As a corollary, this shows that the bound obtained using κ^{Kato} (see (MR04, Theorem 6.2.4), for example) can be improved as follows:

Theorem C *Let III_E be the Tate-Shafarevich group of E, $L_N(E,s)$ the "non-primitive" Hasse-Weil L-function associated to E with Euler factors at the primes dividing N removed and Ω_E the fundamental real period of E. Then*

$$\mathrm{length}(\mathrm{III}_E[p^\infty]) \leq \mathrm{ord}_p\left(\frac{L_N(E,1)}{c_\ell \cdot \Omega_E}\right).$$

See also Corollary 27 below.

As one may notice, the "improvement" we give above includes only one Tamagawa factor. A further improvement which shall include all Tamagawa factors unfortunately escapes our method. We discuss this matter further in §4. We also elaborate on the hypotheses of Theorem 23 to produce other interesting occurrences of the Tamagawa defect of Euler systems for representations other than the Tate module of an elliptic curve.

Our results are somewhat related to that of (Jet), however they are more general in the sense that our Theorem 23 gives a conceptual explanation for the Tamagawa defect for many Galois representations; yet the setting for which Theorem 23 applies is disjoint from that of Jetchev's as far as the Kolyvagin system machinery is concerned.

Acknowledgements

We would like to express our gratitude to Karl Rubin, who encouraged us to compute the cokernel of the specialization map on the module of Λ-adic systems. This paper is essentially a response to his suggestions. We also thank Olivier Fouquet and Jan Nekovář for their feedback; Ofer Gabber and Tetsushi Ito for valuable conversations about the component groups of abelian varieties. Many thanks are also due to Laurent Lafforgue for putting us in touch with Michel Raynaud, and to Michel Raynaud for his kind e-mail regarding the current state of the art for component groups. We also wish to thank the anonymous referee for suggestions to improve the exposition. Finally, we would like to thank IHÉS, where this paper was written up, for their warm hospitality.

2 Technical Results

2.1 Basic Definitions

2.1.1 Notation

Fix once and for all an odd rational prime p. Let R be a local principal ideal ideal ring with finite residue field of characteristic p, $\mathfrak{m}$ be its maximal ideal and $\mathbf{k} = R/\mathfrak{m}$ be its residue field. We fix a generator π of $\mathfrak{m}$. For the main applications of our technical results R will the ring of integers of a finite extension $\mathbb{Q}_p$, in that case we write F for its field of fractions.

For any field K (local or global) $\overline{K}$ will be a fixed separable algebraic closure of K and G_K will denote Galois group $\mathrm{Gal}(\overline{K}/K)$. For every rational prime ℓ we fix an embedding $G_{\mathbb{Q}_\ell} \hookrightarrow G_{\mathbb{Q}}$. This fixes a decomposition group of ℓ, and we write $\mathcal{I}_\ell$ for the inertia subgroup inside of this fixed decomposition group.

Let T be an R-module endowed with a continuous $G_{\mathbb{Q}}$-action, which is free of finite rank over R. We will assume that T is unramified outside finitely many primes. If R is the ring of integers of a finite extension $\mathbb{Q}_p$, we write V for $T \otimes_R F$ and W for $T \otimes_R F/R = V/T$. By $H^*(K, X) := H^*(G_K, X)$ we mean the group cohomology of G_K computed with respect to continuous cochains with values in X for $X = T, V, W$ or their subquotients.

If a group H acts on a set X, then the subset of elements of X fixed (pointwise) by H is denoted by X^H.

If M is an R-module and I is an ideal of R, then $M[I]$ will denote the submodule of M killed by I. If M is a $G_{\mathbb{Q}}$-module, $\mathbb{Q}(M)$ will be defined as the

fixed field in $\overline{\mathbb{Q}}$ of the kernel of the map $G_{\mathbb{Q}} \to \mathrm{Aut}(M)$.

2.1.2 Local Cohomology Groups and Local Conditions

Much of the definitions and results we record in §2.1.2 can be found in (MR04, Chapter 1).

Throughout this section let K denote a non-archimedean local field and $\overline{K}$ a fixed separable algebraic closure of K. $\mathcal{O}$ will be the ring of integers in K, $\mathbb{F}$ its residue field, and $K^{\mathrm{unr}} \subset \overline{K}$ the maximal unramified subfield of $\overline{K}$. Let $\mathcal{I}$ be the inertia subgroup $\mathrm{Gal}(\overline{K}/K^{\mathrm{unr}})$, and $G_{\mathbb{F}} = \mathrm{Gal}(K^{\mathrm{unr}}/K)$.

2.1.2.1. *Galois Cohomology of Local Fields.* There is an exact sequence of profinite groups

$$\{1\} \longrightarrow \mathcal{I} \longrightarrow G_K \longrightarrow G_{\mathbb{F}} \longrightarrow \{1\}$$

Further, since the cohomological dimension of $G_{\mathbb{F}} \cong \hat{\mathbb{Z}}$ is one it follows that $H^2(G_{\mathbb{F}}, T^{\mathcal{I}})$ vanishes. Thus the Hochschild-Serre spectral sequence gives rise to the following exact sequence:

$$0 \longrightarrow H^1(G_{\mathbb{F}}, T^{\mathcal{I}}) \longrightarrow H^1(K, T) \longrightarrow H^1(\mathcal{I}, T)^{G_{\mathbb{F}}} \longrightarrow 0$$

2.1.2.2. *Local Conditions.*

Definition 1 *A* local condition $\mathcal{F}$ *on* T *(at* ℓ *if* $K = \mathbb{Q}_\ell$*) is a choice of an* R*-submodule* $H^1_{\mathcal{F}}(K, T)$ *of* $H^1(K, T)$*.*

Suppose T is an R-module with a continuous G_K-action, and $\mathcal{F}$ is a local condition on T. If T' is a submodule of T (*resp.* T'' is a quotient module), then $\mathcal{F}$ induces local conditions (which we still denote by $\mathcal{F}$) on T' (*resp.* on T''), by taking $H^1_{\mathcal{F}}(K, T')$ (*resp.* $H^1_{\mathcal{F}}(K, T'')$) to be the inverse image (*resp.* the image) of $H^1_{\mathcal{F}}(K, T)$ under the natural maps induced by

$$T' \hookrightarrow T, \qquad T \twoheadrightarrow T''.$$

Definition 2 Propagation *of a local condition* $\mathcal{F}$ *on* T *to a submodule* T' *(and a quotient* T'' *of* T *is the local condition* $\mathcal{F}$ *on* T' *(and on* T''*) obtained following the above procedure.*

For example, if I is an ideal of R, then a local condition on T induces local conditions on T/IT and $T[I]$, by *propagation.*

Let $\mathrm{Quot}_R(T)$ be the category $R[[G_K]]$-modules whose objects are quotients T/IT for all ideals I of R, and where the morphisms from T/IT to T/JT are all scalar multiplications r such that $rI \subset J$.

Definition 3 *A local condition $\mathcal{F}$ is* cartesian *on* $\mathrm{Quot}_R(T)$ *(or on a subcategory of* $\mathrm{Quot}_R(T)$*) if for any injective $R[[G_K]]$-module homomorphism $\phi : T_1 \to T_2$ the local condition $\mathcal{F}$ on T_1 is the same as the local condition obtained by propagating $\mathcal{F}$ from T_2 to T_1.*

2.1.2.3. *Examples of Local Conditions.* We review several choices for local conditions which will appear quite frequently.

Definition 4 *Suppose L is an extension of K in $\overline{K}$, and define*

$$H^1_L(K,T) := H^1(\mathrm{Gal}(L/K), T^{G_L}) = \ker\left\{H^1(K,T) \to H^1(L,T)\right\} \subset H^1(K,T)$$

Thus every choice of an algebraic extension L/K gives a choice of a local condition. We note that $H^1_L(K,T)$ is functorial in T. The *unramified* condition frequently appears in this paper and is obtained by taking $L = K^{\mathrm{unr}}$. Namely

$$H^1_{\mathrm{unr}}(K,T) := H^1_{K^{\mathrm{unr}}}(K,T) = H^1(G_{\mathbb{F}}, T).$$

When T is unramified (i.e. $\mathcal{I}$ acts trivially on T), we will also call this the *finite* condition and write $H^1_{\mathrm{f}}(K,T) = H^1_{\mathrm{unr}}(K,T)$.

In general, if $\mathrm{char}(\mathbb{F}) \neq p$ and R is the ring of integers of a finite extension $\mathbb{Q}_p$, the finite condition at K is given by

$$H^1_{\mathrm{f}}(K,T) = \ker\left\{H^1(K,T) \longrightarrow H^1(K^{\mathrm{unr}}, V)\right\}.$$

See (Rub00, §3.1) for a more detailed discussion on the finite and unramified local conditions.

2.1.2.4.*Dual Local Conditions.*

Definition 5 *Define the* Cartier dual *of T to be the $R[[G_K]]$-module*

$$T^* := \mathrm{Hom}(T, \mu_{p^\infty})$$

where μ_{p^∞} stands for the p-power roots of unity inside $\overline{\mathbb{Q}_p}$.

There is the perfect local Tate pairing

$$< , > : H^1(K,T) \times H^1(K,T^*) \longrightarrow H^2(K, \mu_{p^\infty}) \xrightarrow{\sim} \mathbb{Q}_p/\mathbb{Z}_p$$

Definition 6 *The* dual local condition $\mathcal{F}^*$ *on T^* of a local condition $\mathcal{F}$ on T is defined so that $H^1_{\mathcal{F}^*}(K,T^*)$ is the orthogonal complement of $H^1_{\mathcal{F}}(K,T)$ under the local Tate pairing $< , >$.*

Proposition 7 (MR04, Proposition 1.3.2) *Suppose that the residue characteristic of the local field K is different from p. Then $H^1_{\mathrm{f}}(K,T)$ and $H^1_{\mathrm{f}}(K,T^*)$ are orthogonal complements under the local Tate pairing $<,>$.*

2.1.3 Selmer structures and Selmer groups

Definitions and results we record in this section can be found in (MR04, Chapter 2).

For the rest of this paper, unless otherwise is stated, T will be a free R-module endowed with a continuous action of $G_{\mathbb{Q}}$, which is unramified outside a finite set of rational primes. Below notation will also be in effect till the end.

Let $\overline{\mathbb{Q}} \subset \mathbb{C}$ be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, and for each rational prime ℓ we fix an algebraic closure $\overline{\mathbb{Q}_\ell}$ of $\mathbb{Q}_\ell$ containing $\overline{\mathbb{Q}}$. We will ignore the infinite place of $\mathbb{Q}$ systematically since we assumed $p > 2$. Occasionally we will denote $G_{\mathbb{Q}_\ell} = \mathrm{Gal}(\overline{\mathbb{Q}_\ell}/\mathbb{Q}_\ell)$ by $\mathcal{D}_\ell$, whenever we would like to identify this group by a closed subgroup of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$; namely with a particular decomposition group at ℓ in $G_{\mathbb{Q}}$. We further define $\mathcal{I}_\ell \subset \mathcal{D}_\ell$ to be the inertia group and $\mathrm{Fr}_\ell \in \mathcal{D}_\ell/\mathcal{I}_\ell$ to be the arithmetic Frobenius element at ℓ.

Definition 8 *A* Selmer structure $\mathcal{F}$ *on T is a collection of the following data:*

- *a finite set $\Sigma(\mathcal{F})$ of places of $\mathbb{Q}$, including ∞, p, and all primes where T is ramified.*
- *for every $\ell \in \Sigma(\mathcal{F})$ a local condition (in the sense of Definition 1) on T (which we view now as a $R[[\mathcal{D}_\ell]]$-module), i.e., a choice of R-submodule*

$$H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) \subset H^1(\mathbb{Q}_\ell, T).$$

If $\ell \notin \Sigma(\mathcal{F})$ we will also write $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) = H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T)$.

Definition 9 *If $\mathcal{F}$ is a Selmer structure, we define the* Selmer module $H^1_{\mathcal{F}}(\mathbb{Q}, T)$ *to be the kernel of the sum of the restriction maps*

$$H^1(\mathrm{Gal}(\mathbb{Q}_{\Sigma(\mathcal{F})}/\mathbb{Q}), T) \longrightarrow \bigoplus_{\ell \in \Sigma(\mathcal{F})} H^1(\mathbb{Q}_\ell, T)/H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)$$

where $\mathbb{Q}_{\Sigma(\mathcal{F})}$ is the maximal extension of $\mathbb{Q}$ which is unramified outside $\Sigma(\mathcal{F})$.

Example 10 *Suppose R is the ring of integers of a finite extension $\mathbb{Q}_p$. The* canonical Selmer structure $\mathcal{F}_{\mathrm{can}}$ *on T is given by*

- $\Sigma(\mathcal{F}_{\mathrm{can}}) = \{\ell : T \text{ is ramified at } \ell\} \cup \{p, \infty\}$,
- *if $\ell \in \Sigma(\mathcal{F}_{\mathrm{can}})$ and $\ell \neq p, \infty$ then $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_\ell, T) = H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T)$,*
- $H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_p, T) = H^1(\mathbb{Q}_p, T)$.

Note that we may safely ignore the infinite place since $p > 2$, therefore one has $H^1(\mathbb{R}, T) = 0$.

If I is an ideal of R we define the canonical Selmer structure on T/IT (which we still denote by $\mathcal{F}_{\text{can}}$) to be the Selmer structure obtained from $\mathcal{F}_{\text{can}}$ on T by propagation *of local conditions.*

Definition 11 *A* Selmer triple *is a triple $(T, \mathcal{F}, \mathcal{P})$ where T is an $R[[G_{\mathbb{Q}}]]$-module which is free of finite rank over R, unramified outside finitely many primes; $\mathcal{F}$ is a Selmer structure on T and $\mathcal{P}$ is a set of rational primes, disjoint from $\Sigma(\mathcal{F})$.*

2.2 Hypotheses

In this section we record the hypotheses which were utilized by Mazur, Rubin and Howard to prove their main theorems on Kolyvagin systems in (MR04). For a discussion of these hypotheses see (MR04, §3.5).

H1 $T/\mathfrak{m}T$ is an absolutely irreducible $\mathbf{k}[G_{\mathbb{Q}}]$-representation.
H2 There is a $\tau \in G_{\mathbb{Q}}$ such that $\tau = 1$ on μ_{p^∞} and $T/(\tau - 1)T$ is free of rank one over R.
H3 $H^1(\mathbb{Q}(T, \mu_{p^\infty})/\mathbb{Q}, T/\mathfrak{m}T) = H^1(\mathbb{Q}(T, \mu_{p^\infty})/\mathbb{Q}, T^*[\mathfrak{m}]) = 0$.
H4 Either
  H4a $\text{Hom}_{\mathbf{k}[[\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]]}(T/\mathfrak{m}T, T^*[\mathfrak{m}]) = 0$, or
  H4b $p > 4$.
H5 $\mathcal{P}_t \subset \mathcal{P} \subset \mathcal{P}_1$ for some $t \in \mathbb{Z}^+$, where $\mathcal{P}_k$ is as in (MR04, Definition 3.1.6).
H6 For every $\ell \in \Sigma(\mathcal{F})$, the local condition $\mathcal{F}$ at ℓ is cartesian (in the sense of Definition 3) on the category $\text{Quot}_R(T)$ of quotients of T.

Remark 12 **i.** *Suppose R is the ring of integers of a finite extension $\mathbb{Q}_p$. Then $\mathcal{F}_{\text{can}}$ satisfies **H6** by (MR04, Lemma 3.7.1).*
ii. *Suppose that $E_{/\mathbb{Q}}$ is an elliptic curve defined over $\mathbb{Q}$ which does not have complex multiplication, and let $T = T_p(E)$ be its p-adic Tate module (which is a representation of $G_{\mathbb{Q}}$ which is free of rank 2 over $R = \mathbb{Z}_p$). It is verified in (Rub98) that $T_p(E)$ satisfies the hypotheses **H1-H4**, and the choice the set of primes $\mathcal{P}$ which satisfies **H5** has been explained (see also (Sch98)). Thus the hypotheses above hold for the Selmer triple $(T, \mathcal{F}_{\text{can}}, \mathcal{P})$.*

2.3 Theorems of Howard, Mazur and Rubin

Suppose $(T, \mathcal{F}, \mathcal{P})$ is a Selmer triple (in the sense of Definition 11). Let $\mathbf{KS}(T) = \mathbf{KS}(T, \mathcal{F}, \mathcal{P})$ denote the R-module of Kolyvagin systems for the Selmer triple

$(T, \mathcal{F}, \mathcal{P})$ defined as in (MR04, Definition 3.1.3). We also let $\overline{\mathbf{KS}}(T, \mathcal{F}, \mathcal{P})$ be the *generalized* module of Kolyvagin systems, see (MR04, Definition 3.1.6) for a definition. Under the hypotheses set in §2.2 above Howard, Mazur and Rubin show that the structure of the modules $\mathbf{KS}(T, \mathcal{F}, \mathcal{P})$ and $\overline{\mathbf{KS}}(T, \mathcal{F}.\mathcal{P})$ is determined by an invariant $\chi(T) = \chi(T, \mathcal{F})$ which they call the *core Selmer rank*, see (MR04, Definitions 4.1.11 and 5.2.4). In §2.3 we give a survey of their relevant results.

2.3.1 Core Selmer rank and the module of Kolyvagin systems

Recall the definition of the canonical Selmer structure $\mathcal{F}_{\text{can}}$. Theorem below (which is (MR04, Theorem 5.2.15)) enables us to calculate the core Selmer rank $\chi(T, \mathcal{F}_{\text{can}})$ of the canonical Selmer structure T:

Theorem 13 *Suppose R is a discrete valuation ring. Let $d^- = \text{rank}_R(T^-)$, where T^- is the -1-eigenspace for the action of some complex conjugation. Then*

$$\chi(T, \mathcal{F}_{\text{can}}) = d^- + \text{corank}_R(H^0(\mathbb{Q}_p, T^*)).$$

Example 14 *Suppose $E_{/\mathbb{Q}}$ is an elliptic curve defined over $\mathbb{Q}$ and let $T = T_p(E)$ be its p-adic Tate module. In this case $\chi(T, \mathcal{F}_{\text{can}}) = \text{rank}_{\mathbb{Z}_p} T^- = 1$.*

Fix a Selmer triple $(T, \mathcal{F}, \mathcal{P})$ until the end of §2.3, for which **H1-H6** hold.

Theorem 15 (MR04, Corollaries 4.5.1 and 4.5.2) *Suppose R is a principal artinian ring of length k.*

(i) *If $\chi(T) = 0$ then $\mathbf{KS}(T) = 0$.*
(ii) *If $\chi(T) \geq 2$ then for every positive integer d, $\mathbf{KS}(T)$ contains a free R-module of rank d.*
(iii) *Suppose $\chi(T) = 1$. Then,*
  (1) $\mathbf{KS}(T)$ is a free R-module of rank one.
  (2) If $j \leq k$ then the projection $T \to T/\mathfrak{m}^j T$ induces a surjective map $\mathbf{KS}(T) \to \mathbf{KS}(T/\mathfrak{m}^j T)$.

Building on Theorem 15, the following result is proved in (MR04, Proposition 5.2.9 and Theorem 5.2.10):

Theorem 16 *Suppose R is a discrete valuation ring.*

(i) *If $\chi(T) = 0$ then $\mathbf{KS}(T) = 0$.*
(ii) *Suppose $\chi(T) = 1$. Then,*
  (1) $\mathbf{KS}(T) \xrightarrow{\sim} \varprojlim \mathbf{KS}(T/\mathfrak{m}^k T, \mathcal{P}_k) \xrightarrow{\sim} \overline{\mathbf{KS}}(T)$,
  (2) $\mathbf{KS}(T)$ is a free R-module of rank one, generated by a $\kappa \in \mathbf{KS}(T)$ whose image in $\mathbf{KS}(T/\mathfrak{m}T)$ is nonzero.

Definition 17 *$\kappa \in \mathbf{KS}(T)$ is called* primitive *if the image of κ in $\mathbf{KS}(T/\mathfrak{m}T)$ is nonzero.*

2.3.2 Euler systems and the descent map

Suppose for this section that R is the ring of integers of a finite extension of $\mathbb{Q}_p$. Let $(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ be a Selmer triple, and let $\mathcal{K}$ be an abelian extension of $\mathbb{Q}$ which contains the maximal abelian p-extension of $\mathbb{Q}$ which is unramified outside p and $\mathcal{P}$. Following (MR04, Definition 3.2.2) we let $\mathbf{ES}(T) = \mathbf{ES}(T, \mathcal{P}, \mathcal{K})$ denote the collection of Euler systems for $(T, \mathcal{P}, \mathcal{K})$.

Theorem 18 (MR04, Theorem 3.2.4) *Suppose that $T/(\mathrm{Fr}_\ell - 1)T$ is a cyclic R-module for every $\ell \in \mathcal{P}$, and that $\mathrm{Fr}_\ell^{p^k} - 1$ is injective on T for every $\ell \in \mathcal{P}$ and every $k \geq 0$. Then there is a canonical homomorphism $\mathbf{ES}(T) \to \overline{\mathbf{KS}}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ such that if $\mathbf{c} \in \mathbf{ES}(T)$ maps to $\kappa \in \overline{\mathbf{KS}}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$, then $\kappa_1 = \mathbf{c}_{\mathbb{Q}}$.*

2.4 Comparison of Selmer structures and the Cartesian Condition

Lemma 19 *Suppose for the local condition $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) \subset H^1(\mathbb{Q}_\ell, T)$ the R-module $H^1(\mathbb{Q}_\ell, T)/H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)$ is torsion-free. Then for every $n \in \mathbb{Z}^+$ the induced local condition on the quotients $\mathrm{Quot}_{R/\mathfrak{m}^n}(T/\mathfrak{m}^n T) = \{T/\mathfrak{m}^j T\}_{j=1}^n$ of $R/\mathfrak{m}^n$-module $T/\mathfrak{m}^n T$ is cartesian (in the sense of Definition 3).*

PROOF. This is (MR04, Lemma 3.7.1 (i)). □

Proposition 20 *Suppose $H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T) \subset H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)$ are two local conditions on T at the prime ℓ such that*

(i) *$H^1(\mathbb{Q}_\ell, T)/H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)$ is R-torsion-free,*
(ii) *$H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T/\mathfrak{m}^n T)/H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T/\mathfrak{m}^n T)$ is a free $R/\mathfrak{m}^n$-module (where $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T/\mathfrak{m}^n T)$ (respectively $H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T/\mathfrak{m}^n T)$) is the local condition on $T/\mathfrak{m}^n T$ propagated from the local condition $\mathcal{F}$ (respectively $\mathcal{G}$) on T) in the sense of Definition 2.*

Then the local condition $\mathcal{G}$ is cartesian on the quotients $\mathrm{Quot}_{R/\mathfrak{m}^n}(T/\mathfrak{m}^n T) = \{T/\mathfrak{m}^j T\}_{j=1}^n$ (in the sense of Definition 3) of the $R/\mathfrak{m}^n$-module $T/\mathfrak{m}^n T$.

PROOF. Let the R-module Q be defined by the exactness of the following sequence:

$$0 \longrightarrow H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T) \longrightarrow H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) \longrightarrow Q \longrightarrow 0. \tag{2.1}$$

The propagated local condition $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T)$ is defined as the image of $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)$ under the canonical homomorphism

$$H^1(\mathbb{Q}_\ell, T)/\mathfrak{m}^j H^1(\mathbb{Q}_\ell, T) \hookrightarrow H^1(\mathbb{Q}_\ell, T/\mathfrak{m}^j)$$

(which is induced from the long exact sequence for the $G_{\mathbb{Q}_\ell}$-cohomology of the exact sequence

$$0 \longrightarrow T \xrightarrow{\pi^j} T \longrightarrow T/\mathfrak{m}^j \longrightarrow 0$$

where we recall that π is a uniformizer of R). In other words

$$H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T) = \mathrm{im}\left\{ H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) \to \frac{H^1(\mathbb{Q}_\ell, T)}{\mathfrak{m}^j H^1(\mathbb{Q}_\ell, T)} \hookrightarrow H^1(\mathbb{Q}_\ell, T/\mathfrak{m}^j T) \right\} \tag{2.2}$$

The kernel of the first map in (2.2) is $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) \cap \pi^j H^1(\mathbb{Q}_\ell, T)$ which is equal to $\pi^j H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)$ since we assumed that $H^1(\mathbb{Q}_\ell, T)/H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)$ is R-torsion-free. Thus

$$\begin{aligned} &H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T) \\ &\qquad = \mathrm{im}\left\{ \frac{H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)}{\mathfrak{m}^j H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)} \hookrightarrow \frac{H^1(\mathbb{Q}_\ell, T)}{\mathfrak{m}^j H^1(\mathbb{Q}_\ell, T)} \hookrightarrow H^1(\mathbb{Q}_\ell, T/\mathfrak{m}^j T) \right\} \end{aligned}$$

Similarly,

$$H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T) = \mathrm{im}\left\{ H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T) \to \frac{H^1(\mathbb{Q}_\ell, T)}{\mathfrak{m}^j H^1(\mathbb{Q}_\ell, T)} \hookrightarrow H^1(\mathbb{Q}_\ell, T/\mathfrak{m}^j T) \right\} \tag{2.3}$$

and the kernel of the first map in (2.3) is $H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T) \cap \pi^j H^1(\mathbb{Q}_\ell, T)$ which equals $H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T) \cap \pi^j H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)$ because $H^1(\mathbb{Q}_\ell, T)/H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)$ is R-torsion-free. We thus have

$$\begin{aligned} &H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T) = \\ &\mathrm{im}\left\{ \frac{H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T)}{\mathfrak{m}^j H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) \cap H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T)} \hookrightarrow \frac{H^1(\mathbb{Q}_\ell, T)}{\mathfrak{m}^j H^1(\mathbb{Q}_\ell, T)} \hookrightarrow H^1(\mathbb{Q}_\ell, T/\mathfrak{m}^j T) \right\} \end{aligned}$$

Consider the following exact sequence, which is simply obtained by tensoring the exact sequence (2.1) by $R/\mathfrak{m}^j$ and using the fact that taking tensor products is a right exact functor:

$$\frac{H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T)}{\mathfrak{m}^j H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T)} \longrightarrow \frac{H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)}{\mathfrak{m}^j H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)} \longrightarrow Q/\mathfrak{m}^j Q \longrightarrow 0.$$

This sequence may be completed to an exact sequence on the left by modifying the left most term:

$$0 \longrightarrow \frac{H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T)}{\mathfrak{m}^j H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T) \cap H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T)} \longrightarrow \frac{H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)}{\mathfrak{m}^j H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)} \longrightarrow Q/\mathfrak{m}^j Q \longrightarrow 0. \quad (2.4)$$

Now the exact sequence (2.4) and the description of the *propagated* local conditions $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T)$ and $H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T)$ above shows that the following sequence is exact.

$$0 \longrightarrow H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T) \longrightarrow H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T) \longrightarrow Q/\mathfrak{m}^j Q \longrightarrow 0. \quad (2.5)$$

To prove the statement of the Proposition we need to prove that

$$H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T/\mathfrak{m}^i T) = \ker \left\{ H^1(\mathbb{Q}_\ell, T/\mathfrak{m}^i T) \xrightarrow{[\pi^{j-i}]} \frac{H^1(\mathbb{Q}_\ell, T/\mathfrak{m}^j T)}{H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T)} \right\} \quad (2.6)$$

for $0 < i \leq j \leq n$, where $[\pi^{j-i}]$ is the map induced on the cohomology groups from the map $T/\mathfrak{m}^i T \xrightarrow{\pi^{j-i}} T/\mathfrak{m}^j T$. Now if $c \in H^1(\mathbb{Q}_\ell, T/\mathfrak{m}^i T)$ and $[\pi^{j-i}]c \in H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T) \subset H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T)$ it follows from Lemma 19 that $c \in H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T)$. Thus (2.6) is equivalent to the statement

$$H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T/\mathfrak{m}^i T) = \ker \left\{ H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T/\mathfrak{m}^i T) \xrightarrow{[\pi^{j-i}]} \frac{H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T)}{H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T)} \right\} \quad (2.7)$$

for $0 < i \leq j \leq n$.

To see (2.7) holds consider the following commutative diagram (where the rows come from the exact sequence (2.5)):

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T/\mathfrak{m}^i T) & \longrightarrow & H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T/\mathfrak{m}^i T) & \longrightarrow & Q/\mathfrak{m}^i Q & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle [\pi^{j-i}]} & & \downarrow{\scriptstyle [\pi^{j-i}]} & & \downarrow{\scriptstyle \pi^{j-i}} & & \\
0 & \longrightarrow & H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T) & \longrightarrow & H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T) & \longrightarrow & Q/\mathfrak{m}^j Q & \longrightarrow & 0
\end{array}$$

By our assumption that $H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T/\mathfrak{m}^n T)/H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T/\mathfrak{m}^n T) \xrightarrow{\sim} Q/\mathfrak{m}^n Q$ is a free $R/\mathfrak{m}^n$-module it follows that the right vertical map in the diagram above is injective for $0 < i \leq j \leq n$. This shows that the map

$$H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T/\mathfrak{m}^i T) \Big/ H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T/\mathfrak{m}^i T) \xrightarrow{[\pi^{j-i}]} H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T) \Big/ H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T/\mathfrak{m}^j T)$$

is injective for $0 < i \leq j \leq n$, which proves (2.7) and the Proposition. □

Corollary 21 *Suppose $\mathcal{F}$ is a Selmer structure on T and hypotheses* **H1**-**H6** *are satisfied for $(T, \mathcal{F}, \mathcal{P})$. Suppose further that the core Selmer rank $\chi(T, \mathcal{F})$*

is one. Let $\mathcal{G}$ be another Selmer structure on T, and suppose the local condition at ℓ determined $\mathcal{G}$ satisfies the assumptions of Proposition 20 and that $H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T) \subsetneq H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)$. Then

$$\mathbf{KS}(T/\mathfrak{m}^n T, \mathcal{G}, \mathcal{P}_n) = 0.$$

PROOF. It follows from Proposition 20 that the hypotheses **H1**-**H6** are satisfied by $(T/\mathfrak{m}^n T, \mathcal{G}, \mathcal{P}_n)$. Further, since $H^1_{\mathcal{G}}(\mathbb{Q}_\ell, T) \subsetneq H^1_{\mathcal{F}}(\mathbb{Q}_\ell, T)$, it follows from (Wil95, Proposition 1.6) (see also (MR04, Proposition 2.3.5)) that

$$\begin{aligned}\text{length}\left(H^1_{\mathcal{G}}\left(\mathbb{Q}, T/\mathfrak{m}^n T\right)\right) - \text{length}\left(H^1_{\mathcal{G}}\left(\mathbb{Q}, T^*[\mathfrak{m}^n]\right)\right) < \\ \text{length}\left(H^1_{\mathcal{F}}(\mathbb{Q}, T/\mathfrak{m}^n T)\right) - \text{length}\left(H^1_{\mathcal{F}}(\mathbb{Q}, T^*[\mathfrak{m}^n])\right).\end{aligned}$$

Using the definition (MR04, Definition 4.1.11) of the core Selmer rank and (MR04, Proposition 4.1.4), this translates into

$$0 \leq \chi(T/\mathfrak{m}^n T, \mathcal{G}) < \chi(T/\mathfrak{m}^n T, \mathcal{F}) = 1,$$

hence $\chi(T/\mathfrak{m}^n T, \mathcal{G}) = 0$. Now Theorem 15 shows that

$$\mathbf{KS}(T/\mathfrak{m}^n T, \mathcal{G}, \mathcal{P}_n) = 0,$$

as desired. □

3 Applications

Until the end of this paper we assume that R is the ring of integers of a finite extension of $\mathbb{Q}_p$ and let F be its field of fractions. Let $\mathcal{F}_{\text{can}}$ be the canonical Selmer structure as in Definition 10. Suppose $\mathcal{F}_{\text{u-}\ell}$ is the Selmer structure defined as follows:

- $\Sigma(\mathcal{F}_{\text{u-}\ell}) = \Sigma(\mathcal{F}_{\text{can}})$,
- if $q \in \Sigma(\mathcal{F}_{\text{u-}\ell})$ and $q \neq \ell$ then $H^1_{\mathcal{F}_{\text{u-}\ell}}(\mathbb{Q}_q, T) = H^1_{\mathcal{F}_{\text{can}}}(\mathbb{Q}_q, T)$,
- $H^1_{\mathcal{F}_{\text{u-}\ell}}(\mathbb{Q}_\ell, T) = H^1_{\text{unr}}(\mathbb{Q}_\ell, T)$,

where $H^1_{\text{unr}}(\mathbb{Q}_\ell, T) = \ker\{H^1(\mathbb{Q}_\ell, T) \to H^1(\mathbb{Q}_\ell^{\text{unr}}, T)\}$ is the unramified cohomology.

Remark 22 *By (Rub00, Lemma I.3.5) $H^1_{\mathcal{F}_{\text{u-}\ell}}(\mathbb{Q}_\ell, T) \subset H^1_{\mathcal{F}_{\text{can}}}(\mathbb{Q}_\ell, T)$ and*

$$H^1_{\mathcal{F}_{\text{can}}}(\mathbb{Q}_\ell, T)/H^1_{\mathcal{F}_{\text{u-}\ell}}(\mathbb{Q}_\ell, T) \xrightarrow{\sim} H^0(\mathbb{Q}_\ell, W^{I_\ell} \Big/ V^{I_\ell}/T^{I_\ell}),$$

where $I_\ell \subset G_{\mathbb{Q}_\ell}$ is the inertia subgroup, $V = T \otimes_R F$ and $W = V/T$. Note that the R-module $H^0(\mathbb{Q}_\ell, W^{I_\ell} \Big/ V^{I_\ell}/T^{I_\ell})$ is finite and its order is the p-part of the Tamagawa number at ℓ, cf. (FP94, §I.4.2.2).

Recall that there is a canonical map (which we call the Euler system to Kolyvagin system map)

$$\mathbf{ES}(T) \longrightarrow \overline{\mathbf{KS}}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$$

from the module of Euler systems to the *generalized* module of Kolyvagin systems (see (MR04, Definition 3.1.6)).

Theorem 23 *Let $\mathcal{F}_{\mathrm{can}}$ and $\mathcal{F}_{\text{u-}\ell}$ be as above. Suppose $(T, \mathcal{P})$ satisfies the hypotheses* **H1-H5**, *$\chi(T, \mathcal{F}_{\mathrm{can}}) = 1$ and $n \in \mathbb{Z}_{\geq 0}$ is such that the $R/\mathfrak{m}^n$-module $\left(H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_\ell, T)/H^1_{\mathcal{F}_{\text{u-}\ell}}(\mathbb{Q}_\ell, T)\right) \otimes R/\mathfrak{m}^n$ is free of positive rank. Then*

$$\mathrm{im}\,(\mathbf{ES}(T) \to \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})) \subset \mathfrak{m}^n \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P}).$$

PROOF. We begin with the remark that $\mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ is canonically isomorphic to $\overline{\mathbf{KS}}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ when the core Selmer rank $\chi(T, \mathcal{F}_{\mathrm{can}})$ is one. (This follows from (MR04, Proposition 5.2.9).) We thus allow ourselves to view the map from the module of Euler systems to the generalized module of Kolyvagin systems as a map $\mathbf{ES}(T) \longrightarrow \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ (and this is how the statement of the Theorem makes sense). Under the assumptions above, $\mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ is an R-module of rank one. Consider the map

$$\mathbf{ES}(T) \to \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P}) \to \mathbf{KS}(T/\mathfrak{m}^n T, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_n). \tag{3.1}$$

Since $\mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ is free of rank one, the statement of the Theorem is equivalent to the statement that the map (3.1) is zero. As pointed out in (MR04, Remark A.5), the proof of (MR04, Theorem 3.2.4) shows that the map (3.1) factors as follows:

$$\begin{array}{ccccc} \mathbf{ES}(T) & \longrightarrow & \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P}) & \longrightarrow & \mathbf{KS}(T/\mathfrak{m}^n T, \mathcal{F}_{\mathrm{can}}, \mathcal{P}_n) \\ & \searrow & & \nearrow & \\ & & \mathbf{KS}(T/\mathfrak{m}^n T, \mathcal{F}_{\text{u-}\ell}, \mathcal{P}_n) & & \end{array}$$

Thus it suffices to prove that $\mathbf{KS}(T/\mathfrak{m}^n T, \mathcal{F}_{\text{u-}\ell}, \mathcal{P}_n) = 0$. This follows immediately from Corollary 21 applied with $\mathcal{F} = \mathcal{F}_{\mathrm{can}}$ and $\mathcal{G} = \mathcal{F}_{\text{u-}\ell}$. Note that our assumptions guarantee that Corollary 21 applies with the choices above. □

Let $\mathbb{Q}_\infty$ be the (cyclotomic) $\mathbb{Z}_p$-extension of $\mathbb{Q}$, $\Gamma = \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$ be its Galois group and $\Lambda = \mathbb{Z}_p[[\Gamma]]$ be the cyclotomic Iwasawa algebra. Let $\mathbf{KS}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}})$ be the module of Λ-adic Kolyvagin systems for T (defined as in (Büy07, §3.2)).

Under certain hypotheses (see (Büy07, §2.2)) it is proved that the Λ-module $\mathbf{KS}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}})$ is free of rank one and that the specialization map

$$\mathbf{KS}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}}) \longrightarrow \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$$

is surjective. We remark that the hypotheses **H.T** of (Büy07, §2.2) holds if p does not divide any of the Tamagawa numbers at any prime $\ell \neq p$.

If, however, p does divide at least one Tamagawa number then the specialization map above is not surjective and it is predicted in (Büy07, Remark 3.25) that the cokernel of this map should be related to Tamagawa numbers. As a justification of this remark one may prove:

Theorem 24 *Suppose all the assumptions of the Theorem 23 hold for the triple $(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ and $\mathcal{F}_{\text{u-}\ell}$. Let $n \in \mathbb{Z}^+$ be as in Theorem 23. Then*

$$\mathrm{im}\,(\mathbf{KS}(T \otimes \Lambda, \mathcal{F}_{\mathrm{can}}) \longrightarrow \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})) \subset p^n \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P}).$$

PROOF. The proof of Theorem 23 applies in an identical way, by (Col98, Proposition II.1.1) (used instead of the proof of (MR04, Theorem 3.2.4)). □

We now exhibit a particular application of Theorem 23: We apply it with Kato's Euler system for the Tate module of an elliptic curve. Let $E_{/\mathbb{Q}}$ be an elliptic curve defined over $\mathbb{Q}$ and let $T = T_p(E)$ be its p-adic Tate module. We will also assume that

$$p > 3, \tag{3.2}$$

$$\text{the } p\text{-adic representation } G_{\mathbb{Q}} \to \mathrm{Aut}(E[p^\infty]) \text{ is surjective.} \tag{3.3}$$

Suppose the Tamagawa number $c_\ell = |E(\mathbb{Q}_\ell)/E_0(\mathbb{Q}_\ell)|$ at $\ell \neq p$ is divisible by p, and set $n = \mathrm{ord}_p(c_\ell)$. Since we assumed $p > 3$, this shows (cf. (Sil92, Corollary C.15.2.1)) that E has split multiplicative reduction at ℓ (thus $E_{/\mathbb{Q}_\ell}$ is a Tate curve Tate_q with Tate parameter $q \in \ell\mathbb{Z}_\ell$) and that the component group of the special fiber of the Néron model $\mathcal{E}_{/\mathrm{Spec}(\mathbb{Z}_\ell)}$ of $E_{/\mathbb{Q}_\ell}$ is a cyclic group isomorphic to $\mathbb{Z}/c_\ell\mathbb{Z}$. Thus we have an exact sequence

$$0 \longrightarrow E_0(\mathbb{Q}_\ell) \longrightarrow E(\mathbb{Q}_\ell) \longrightarrow \mathbb{Z}/c_\ell\mathbb{Z} \longrightarrow 0. \tag{3.4}$$

Further, one also has $\mathbb{Z}_\ell^\times \xrightarrow{\sim} E_0(\mathbb{Q}_\ell)$ under Tate uniformization (see for example (Sil92, Theorem C.14.1)). This shows that $X[p^\infty]$ is finite and $X[p^k] \cong X/p^kX$ for $X = E_0(\mathbb{Q}_\ell)$ or $X = E(\mathbb{Q}_\ell)$; and for all $k \in \mathbb{Z}^+$. Here $X[p^\infty]$ stands for the p-power torsion inside the group X.

One may check without difficulty that

$$H^1_{\mathrm{f}}(\mathbb{Q}_\ell, V) := \ker\{H^1(\mathbb{Q}_\ell, V) \longrightarrow H^1(\mathbb{Q}_\ell^{\mathrm{unr}}, V)\} = 0.$$

(One way to see this is via the fact that

$$H^1_{\mathrm{f}}(\mathbb{Q}_\ell, V) = \mathrm{im}\{E(\mathbb{Q}_\ell)^\wedge \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \hookrightarrow H^1(\mathbb{Q}_\ell, V)\}$$

and that $E(\mathbb{Q}_\ell)$ contains a pro-ℓ subgroup of finite index. Here $E(\mathbb{Q}_\ell)^\wedge$ stands for the p-adic completion of the abelian group $E(\mathbb{Q}_\ell)$. Alternatively, it follows from Kodaira-Néron theorem (and our assumption that $p > 3$) that E has split multiplication at ℓ. Using this fact, one may see at once that $V^{\mathcal{I}_\ell}$ is of $\mathbb{Q}_p$-dimension one, and the Frobenius $\mathrm{Fr}_\ell \in \mathcal{D}_\ell/\mathcal{I}_\ell$ at ℓ acts non-trivially on $V^{\mathcal{I}_\ell}$. Therefore

$$0 = V^{\mathcal{I}_\ell}/(\mathrm{Fr}_\ell - 1) \cong H^1_{\mathrm{f}}(\mathbb{Q}_\ell, V),$$

where the final isomorphism $V^{\mathcal{I}_\ell}/(\mathrm{Fr}_\ell - 1) \cong H^1_{\mathrm{f}}(\mathbb{Q}_\ell, V)$ is (Rub00, Lemma I.3.2(i)).)

Hence we conclude that the restriction map

$$H^1(\mathbb{Q}_\ell, V) \longrightarrow H^1(\mathbb{Q}_\ell^{\mathrm{unr}}, V)$$

is injective, thus

$$\begin{aligned} H^1_{\mathcal{F}_{\mathrm{can}}}(\mathbb{Q}_\ell, T) = H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T) &:= \ker\{H^1(\mathbb{Q}_\ell, T) \to H^1(\mathbb{Q}_\ell^{\mathrm{unr}}, V)\} \\ &= \ker\{H^1(\mathbb{Q}_\ell, T) \to H^1(\mathbb{Q}_\ell, V)\}, \end{aligned}$$

which equals the image of $E(\mathbb{Q}_\ell)[p^\infty]$ inside $H^1(\mathbb{Q}_\ell, T)$. See also (Rub00, §I.6.4). Similarly, one may show that $H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, T)$ is the image of $E_0(\mathbb{Q}_\ell)[p^\infty]$ inside $H^1(\mathbb{Q}_\ell, T)$. The diagram below summarizes our discussion in this paragraph:

$$\begin{array}{ccc} H^1_{\mathrm{f}}(\mathbb{Q}_\ell, T) & = & \mathrm{im}\{E(\mathbb{Q}_\ell)[p^\infty] \hookrightarrow H^1(\mathbb{Q}_\ell, T)\} \\ \cup\uparrow & & \\ H^1_{\mathrm{unr}}(\mathbb{Q}_\ell, T) & = & \mathrm{im}\{E_0(\mathbb{Q}_\ell)[p^\infty] \hookrightarrow H^1(\mathbb{Q}_\ell, T)\} \end{array}$$

This, together with (3.4), Example 14 and Theorem 23 (with $n = \mathrm{ord}_p(c_\ell)$) shows

Corollary 25 *Let $T = T_p(E), E, c_\ell, n$ be as above. Then*

$$\mathrm{im}\,(\mathbf{ES}(T) \to \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})) \subset p^n \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P}).$$

We remark that the hypotheses **H1**-**H5** hold in this setting (which is necessary in order to apply Theorem 23) thanks to our assumptions (3.2) and (3.3). See also (MR04, Lemma 6.2.3).

Let N be the conductor of E. Kato (Kat04) has constructed an Euler system which gives rise to a Kolyvagin system $\kappa^{\mathrm{Kato}} \in \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ for a suitably chosen set of primes $\mathcal{P}$, see (Rub98, §3.5) and (MR04, §6.2) for more

details. Corollary 25 shows that $\kappa^{\mathrm{Kato}} \in p^n \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$. Further we know (Theorem 16) that $\mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$ is a free $\mathbb{Z}_p$-module of rank one, and is generated by a primitive Kolyvagin system. We fix such a generator κ^E so that $\kappa^{\mathrm{Kato}} = p^\alpha \cdot \kappa^E$ for some $\alpha \geq n$.

The following Theorem is the main application of κ^{Kato}. Let $L(E, s)$ denote the Hasse-Weil L-function attached to E, and $L_N(E, s)$ the *non-primitive* L-function which is obtained by removing the Euler factors at primes dividing the conductor N of E. Let Ω_E be the fundamental period of E, and III_E be the Tate-Shafarevich group of E.

Theorem 26 (Kat04) *Assume (3.2) and (3.3) holds. Suppose further that*

- *E has good reduction at p,*
- *$p \nmid E(\mathbb{F}_p)$,*
- *p does not divide the integer r_E of (Rub98) Theorem 7.1,*
- *$L(E, 1) \neq 0$.*

Then

$$\mathrm{length}(\mathrm{III}_E[p^\infty]) \leq \mathrm{ord}_p(L_N(E, 1)/\Omega_E).$$

To prove this Theorem one utilizes

(i) Kolyvagin system machinery with κ^{Kato} to bound the classical Selmer group (see for example (Rub98, Theorem 3.2)),
(ii) and then Kato's calculations (see the proof of (Rub98, Theorem 8.6)) with the element κ_1^{Kato} (which appears as $c_{\mathbb{Q}}$ in (Rub98)).

More precisely, Kolyvagin system machinery with κ^{Kato} gives the inequality

$$\mathrm{length}\left(\mathcal{S}_E(\mathbb{Q})\right) \leq \mathrm{length}\left(H^1_{\mathrm{s}}(\mathbb{Q}_p, T)/\mathbb{Z}_p \cdot \mathrm{loc}_p^{\mathrm{s}}\left(\kappa_1^{\mathrm{Kato}}\right)\right), \tag{3.5}$$

cf. (Rub00, Theorem 2.2.10(ii)). Here $\mathcal{S}_E(\mathbb{Q})$ is the classical p-Selmer group attached to $E/\mathbb{Q}$, and $H^1_{\mathrm{s}}(\mathbb{Q}_p, T) = H^1(\mathbb{Q}_p, T)/H^1_{\mathrm{f}}(\mathbb{Q}_p, T)$ is the *singular quotient* with $H^1_{\mathrm{f}}(\mathbb{Q}_p, T) = \mathrm{im}\{E(\mathbb{Q}_p)^\wedge \hookrightarrow H^1(\mathbb{Q}_p, T)\}$ and $\mathrm{loc}_p^{\mathrm{s}}$ is the composition

$$H^1(\mathbb{Q}, T) \longrightarrow H^1(\mathbb{Q}_p, T) \longrightarrow H^1_{\mathrm{s}}(\mathbb{Q}_p.T).$$

The conclusion of Theorem 26 then follows from Kato's calculation of the right hand side of the inequality (3.5).

One could use κ^E instead of $\kappa^{\mathrm{Kato}} = p^\alpha \cdot \kappa^E$ to bound the classical Selmer group (which, in a sense, is a "better" Kolyvagin system). Using the fact that the singular quotient $H^1_{\mathrm{s}}(\mathbb{Q}_p, T)$ is a free (rank one) $\mathbb{Z}_p$-module (as it injects into $H^1_{\mathrm{s}}(\mathbb{Q}_p, V) = H^1(\mathbb{Q}_p, V)/H^1_{\mathrm{f}}(\mathbb{Q}_p, V)$), and replacing κ^{Kato} by κ^E, the inequality (3.5) is evidently improved by a factor of p^α and yields the following stronger version of Theorem 26:

Corollary 27 *Assume the hypotheses of Theorem 26 holds. Then*

$$\mathrm{length}(Ш_E[p^\infty]) \leq \mathrm{ord}_p\left(\frac{L_N(E,1)}{p^\alpha \cdot \Omega_E}\right) \leq \mathrm{ord}_p\left(\frac{L_N(E,1)}{c_\ell \cdot \Omega_E}\right).$$

4 Concluding Remarks

4.1 More on Kato's Euler system

Explicit calculations carried out by Kato (Kat04) to determine a bound on the size of the Selmer group are limited to the case $L(E,1) \neq 0$. In this case the classical Selmer group $\mathcal{S}_E$ attached to E is finite and one only has to deal with the very first term κ_1^{Kato} of the Kolyvagin system $\kappa^{\mathrm{Kato}} \in \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$. In fact, in Corollary 27 above we only use Corollary 25 to conclude that $\kappa_1^{\mathrm{Kato}} = p^\alpha \cdot \kappa_1^E$, where α and κ^E are as above. This is sufficient in the setting of Theorem 26.

However one should note that Corollary 25 says much more than the comparison above for the initial terms of these Kolyvagin systems, it in fact says that

$$\kappa_r^{\mathrm{Kato}} = p^\alpha \cdot \kappa_r^E \tag{4.1}$$

for every $r \in \mathcal{N}(\mathcal{P})$, where $\mathcal{N}(\mathcal{P})$ is the set of integers which are square free products of primes in $\mathcal{P}$. If κ_1^{Kato} (hence also κ_1^E) is non-zero (which essentially put us in the setting of Theorem 26) then (4.1) easily follows from the equality $\kappa_1^{\mathrm{Kato}} = p^\alpha \cdot \kappa_1^E$ and Theorem 15. Of course this is not always the case and (4.1) is a much stronger statement in general. Unfortunately, when the Hasse-Weil L-function vanishes at $s = 1$ (this *should* amount to saying $\kappa_1^{\mathrm{Kato}} = 0$, cf. (MR04, Corollary 5.2.13)) there is no computation yet available with Kato's Kolyvagin system to exemplify the content of Corollary 25 further, in terms of bounding the Selmer group (such as Corollary 27, which applies when $L(E,1) \neq 0$).

4.2 Tamagawa numbers and level lowering

We keep assuming $T = T_p(E)$, the p-adic Tate module of an elliptic curve $E_{/\mathbb{Q}}$, and hypotheses (3.2) and (3.3). Corollary 25 says that

$$\kappa^{\mathrm{Kato}} \in c_\ell \cdot \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P}).$$

This statement is reflected in Corollary 27 as an improvement to Kato's Theorem 26. However, this method captures only one Tamagawa factor. What

if there are more then one Tamagawa numbers which are divisible by p? A natural question to ask is:

Question 1. Is it true that $\kappa^{\mathrm{Kato}} \in \prod_{\ell|N} c_\ell \cdot \mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$?

This question turns out to be more delicate when there is more than one Tamagawa number which is divisible by p. We first consider a preliminary version of Question 1. Let d be the number of primes ℓ for which $p|c_\ell$.

Question 2. Is it true that $\kappa^{\mathrm{Kato}} \in p^d\mathbf{KS}(T, \mathcal{F}_{\mathrm{can}}, \mathcal{P})$?

To address this question we consider the newform f_E of level N associated with E. Since we assumed $p > 3$, $p|c_\ell$ implies that E has split multiplicative reduction at ℓ. Thus if $p|c_\ell$, then $\ell||N$. The assumption that $p|c_\ell$ in fact translates into the statement that the Galois representation $E[p] \cong T/pT$ is *finite* at ℓ (in the sense of (Ser87, §2.8); note that since $\ell \neq p$, this simply means that the Galois representation T/pT is unramified at ℓ). Thus, we may apply level lowering theorem of Ribet (Rib90) to arrive at a modular form g of level N/ℓ and a Galois representation T_g attached to g such that $T_g/pT_g \cong T/pT$. Note that ℓ is no longer a bad prime for g. The author is quite curious to see whether the Euler system for the modular form g could play a role in this context to answer Question 2.

More generally, Dummigan (Dum) has studied the Tamagawa factors of modular forms and level lowering for their mod p^n representations for $n > 1$. Similarly, one might try to approach more general Question 1 via Dummigan's more general level lowering results.

4.3 Tamagawa numbers for higher dimensional Abelian varieties

The discussion above with Kato's Euler system (for elliptic curves) suggests that if one would like to apply Theorem 23 with an abelian variety A of higher dimension, one should understand the structure of the p-part Φ_p of the component group of $A_{/\mathbb{Q}_\ell}$ for each $\ell \neq p$. For example, when $A = E$ is one dimensional Kodaira-Néron Theorem (Sil92, Corollary C.15.2.1) shows that Φ_p is always cyclic if $p > 2$, and this is exactly what we use to deduce Corollary 25 from Theorem 23.

Let $A_{/\mathbb{Q}_\ell}$ be an abelian variety (with $\ell \neq p$). Let $\mathcal{A}$ be its Néron model over $\mathbb{Z}_\ell$. Suppose t (resp. u) denote the dimension of the toric (resp. unipotent) part of the special fiber $\mathcal{A}_s$. Let $\Phi[p]$ denote the p-torsion of Φ. Since Φ is a finite group, we have $\Phi[p] \cong \Phi_p/p\Phi_p$. Theorem below can be found in (Abb00):

Theorem 28 (Abb00, Proposition 5.13 (i)) *If $p \geq 3$,*

$$\dim_{\mathbb{F}_p} \Phi[p] \leq t + u \leq \dim A.$$

Suppose now that $A_{/\mathbb{Q}} = A_f$ is an abelian variety of attached to a newform f of level N. Then A_f is an abelian variety of GL_2-type: Let $\mathcal{R}$ denote the ring generated by the Fourier coefficients of f and set $K = \mathbb{Q} \otimes \mathcal{R}$, then $\mathcal{R} \subset \mathrm{End}_{\mathbb{Q}}(A)$ and $[K : \mathbb{Q}] = \dim A$. We assume the following additional hypotheses on p:

$$\mathcal{R} \otimes \mathbb{F}_p \text{ is a field, i.e. } p \text{ is inert in } \mathcal{R}. \tag{4.2}$$

$\mathcal{R} \otimes \mathbb{F}_p$ acts on $\Phi[p]$, thus Theorem 28 and assumption (4.2) shows that

Corollary 29 *$\Phi[p]$ is a cyclic $\mathcal{R}/p\mathcal{R}$-module.*

Let $\mathcal{R}_p$ denote the completion of the ring R at p. The action of $\mathcal{R}$ on Φ_p naturally extends to an action of $\mathcal{R}_p$ on Φ_p. Corollary 29 and Nakayama's lemma implies the following

Corollary 30 *Under the hypotheses above Φ_p is a cyclic $\mathcal{R}_p$-module.*

Let $\mathcal{O}$ denote the maximal order of the number field K. One easily deduces from the assumption (4.2) that the ring homomorphism $\mathcal{R}/p\mathcal{R} \to \mathcal{O}/p\mathcal{O}$ is an isomorphism, hence p is inert in the extension $\mathcal{O}/\mathbb{Z}$ as well. Further, the inclusion $\mathcal{R} \hookrightarrow \mathcal{O}$ induces a natural isomorphism $\mathcal{R}_p \xrightarrow{\sim} \mathcal{O}_p$. Thus we proved

Proposition 31 *If we assume (4.2) then Φ_p is a cyclic $\mathcal{O}_p$-module.*

Note that this is the analogous statement for abelian varieties A_f to that for elliptic curves (i.e. to the case $K = \mathbb{Q}$), which, in that case, is implied by the Kodaira-Néron Theorem.

Consider the p-adic Tate module $T_p(A_f)$, and set

$$V_p(A_f) = \mathbb{Q}_p \otimes_{\mathbb{Z}_p} T_p(A_f).$$

We keep assuming (4.2). It is known that $V_p(A_f)$ is a K_p-vector space of dimension 2; choose a $G_{\mathbb{Q}}$-invariant lattice T inside $V_p(A_f)$ so that T is a free $\mathcal{O}_p$-module of rank 2. Kato (Kat04) has constructed an Euler system for this $\mathcal{O}_p[[G_{\mathbb{Q}}]]$ representation. One could use Theorem 23 (which applies thanks to Proposition 31 with $R = \mathcal{O}_p$) to obtain similar results to Corollary 25 in this setting.

References

[Abb00] A. Abbes, Réduction semi-stable des courbes d'après Artin, Deligne, Grothendieck, Mumford, Saito, Winters, ..., in: *Courbes semi-stables et groupe fondamental en géométrie algébrique (Luminy, 1998) Progr. Math.* **187** (2000) 59–110.

[BK90] S. Bloch and K.Kato, L-functions and Tamagawa numbers of motives, in: *The Grothendieck Festschrift, Vol. I* , *Progr. Math.* **86** (1990) 333–400.

[Büy07] K. Büyükboduk, Λ-adic Kolyvagin systems, preprint, available at: arXiv:0706.0377v1 [math.NT], 56pp.

[Col98] P. Colmez, Théorie d'Iwasawa des représentations de de Rham d'un corps local, *Ann. of Math. (2)*, **148** (1998) 485–571.

[Dum] N. Dummigan, Level-lowering for higher congruences of modular forms, preprint.

[FP94] J.M. Fontaine and B. Perrin-Riou, Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L, in: *Motives (Seattle, WA, 1991)*, *Proc. Sympos. Pure Math.* **55** (1994) 599–706.

[Jet] D. Jetchev, Global divisibility of Heegner points and Tamagawa numbers, to appear in *Compositio Math.*

[Kato99] K. Kato, Euler systems, Iwasawa theory, and Selmer groups, *Kodai Math. J.* **22** (1999) 313–372.

[Kat04] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, in: *Cohomologies p-adiques et applications arithmétiques. III* , *Astérisque* **295** (2004) ix, 117–290.

[Kol90] V.A. Kolyvagin, Euler systems, in: *The Grothendieck Festschrift, Vol. II* , *Progr. Math.* **87** (1990) 435–483.

[MR04] B. Mazur and K. Rubin, Kolyvagin systems, *Mem. Amer. Math. Soc.* **168(799)** (2004).

[PR98] B. Perrin-Riou, Systèmes d'Euler p-adiques et théorie d'Iwasawa, *Ann. Inst. Fourier (Grenoble)* **48** (1998) 1231–1307.

[Rib90] K. Ribet, On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms, *Invent. Math.* **100** (1990) 431–476.

[Rub98] K. Rubin, Euler systems and modular elliptic curves, in: *Galois representations in arithmetic algebraic geometry (Durham, 1996)* , *London Math. Soc. Lecture Note Ser.* **254** (1998) 351–367.

[Rub00] K. Rubin, Euler systems, *Annals of Mathematics Studies* **147** (2000) Hermann Weyl Lectures. The Institute for Advanced Study.

[Ser87] J-P. Serre, Sur les représentations modulaires de degré 2 de Gal($\overline{\mathbf{Q}}/\mathbf{Q}$), *Duke Math. J.* **54** 1987 179-230.

[Sch98] A.J. Scholl, An introduction to Kato's Euler systems, in: *Galois representations in arithmetic algebraic geometry (Durham, 1996)* , *London Math. Soc. Lecture Note Ser.* **254** (1998) 379–460.

[Sil92] J. Silverman, The arithmetic of elliptic curves, *Graduate Texts in Mathematics* **106** (Springer-Verlag, New York, 1992).

[Wil95] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. (2) **141** (1995) 443–551.