

The Birch and Swinnerton-Dyer formula for elliptic curves of analytic rank one

DIMITAR JETCHEV^{*}, CHRISTOPHER SKINNER[†], AND XIN WAN[‡]

Let E/\mathbb{Q} be a semistable elliptic curve such that $\text{ord}_{s=1}L(E, s) = 1$. We prove the p -part of the Birch and Swinnerton-Dyer formula for E/\mathbb{Q} for each prime $p \geq 5$ of good reduction such that $E[p]$ is irreducible:

$$\text{ord}_p \left(\frac{L'(E, 1)}{\Omega_E \cdot \text{Reg}(E/\mathbb{Q})} \right) = \text{ord}_p \left(\#\text{III}(E/\mathbb{Q}) \prod_{\ell \leq \infty} c_\ell(E/\mathbb{Q}) \right).$$

This formula also holds for $p = 3$ provided $a_p(E) = 0$ if E has supersingular reduction at p .

1. Introduction

1.1. The Birch and Swinnerton-Dyer conjecture

Let E/\mathbb{Q} be an elliptic curve. The Birch and Swinnerton-Dyer Conjecture for E , as stated by Tate [50, Conj. 4] (see also [49] and [4, (I)-(IV)]) is the following:

Conjecture 1.1.1 (Birch and Swinnerton-Dyer Conjecture).

- (a) *The order of the zero at $s = 1$ of the Hasse–Weil L -function $L(E, s)$ is equal to the rank r of the Mordell–Weil group $E(\mathbb{Q})$.*

^{*}Supported by Swiss National Science Foundation professorship grant PP00P2-144658.

[†]Partially supported by the grants DMS-0758379 and DMS-1301842 from the National Science Foundation and by the Simons Investigator grant #376203 from the Simons Foundation.

[‡]Partially supported by the Chinese Academy of Science grant Y729025EE1, NSFC grant 11688101, 11621061 and an NSFC grant associated to the “Recruitment Program of Global Experts”.

(b) Let $\text{Reg}(E/\mathbb{Q})$ be the regulator of $E(\mathbb{Q})$ (the discriminant of the Néron-Tate height-pairing on $E(\mathbb{Q})$), $\text{III}(E/\mathbb{Q})$ the Tate-Shafarevich group of E , $c_\ell(E/\mathbb{Q})$ the Tamagawa number of E at a prime ℓ , and $\Omega_E = \int_{E(\mathbb{R})} |\omega_E|$ for ω_E a Néron differential (a \mathbb{Z} -basis for the differentials of the Néron model of E over \mathbb{Z}). Then

$$(1.1.a) \quad \frac{L^{(r)}(E, 1)}{r! \cdot \Omega_E \cdot \text{Reg}(E/\mathbb{Q})} = \frac{\#\text{III}(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{\text{tor}})^2} \prod_{\ell} c_\ell(E/\mathbb{Q}),$$

We call the formula (1.1.a) in (b) the *BSD formula for E* .

1.2. Main result

Let E/\mathbb{Q} be a semistable elliptic curve of conductor N (so N is square-free). Let $p \geq 3$ be a prime of good reduction (i.e., $p \nmid N$) such that the mod p Galois representation $\bar{\rho}_{E,p}: \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Aut}(E[p])$ is irreducible. Suppose that $\text{ord}_{s=1} L(E/\mathbb{Q}, s) = 1$. In this case the work of Gross and Zagier [18] and of Kolyvagin [29, 30, 31] (see also [19]) implies that $\text{rk}_{\mathbb{Z}} E(\mathbb{Q}) = 1$ and $\#\text{III}(E/\mathbb{Q}) < \infty$. In particular, part (a) of Conjecture 1.1.1 holds for E . In this paper we prove that the p -part of the BSD formula (1.1.a) holds for E :

Theorem 1.2.1 (*p -part of the Birch and Swinnerton-Dyer formula*). *If $p \geq 5$, then*

$$(1.2.a) \quad \text{ord}_p \left(\frac{L'(E, 1)}{\text{Reg}(E/\mathbb{Q}) \cdot \Omega_E} \right) = \text{ord}_p \left(\#\text{III}(E/\mathbb{Q}) \prod_{\ell \nmid \infty} c_\ell(E/\mathbb{Q}) \right).$$

If $p = 3$, then (1.2.a) holds provided $a_p(E) = 0$ when E has supersingular reduction at p .

It is a consequence of the Gross–Zagier formula that $\frac{L'(E/\mathbb{Q}, 1)}{\text{Reg}(E/\mathbb{Q}) \cdot \Omega_E} \in \mathbb{Q}^\times$ (see [18, Thm.7.3]), so the p -adic valuation of the left-hand side of (1.2.a) makes sense.

Particular cases of Theorem 1.2.1 have been obtained by Zhang [58] and by Bertini, Bertolini, and Venerucci [2], for $p \geq 5$ a prime of good ordinary reduction. In particular, [58, Thm. 7.3] also has the extra assumption that for any $\ell \parallel N$ for which $\ell \equiv \pm 1 \pmod p$, $\bar{\rho}_{E,p}$ is ramified at ℓ (equivalently, that $p \nmid c_\ell(E/\mathbb{Q})$), and [2, Thm. A] also assumes that p is not anomalous (that is, $p \nmid \#E(\mathbb{F}_p)$) and that p does not divide any of the Tamagawa factors $c_\ell(E/\mathbb{Q})$. In contrast, Theorem 1.2.1 is general – including both the ordinary

and supersingular cases, as well as the cases where there are Tamagawa numbers divisible by p – aside from the extra hypothesis that $a_p(E) = 0$ when E has supersingular reduction at p if $p = 3$.

If p is a prime of supersingular reduction for E and $a_p(E) = 0$ (which is always the case for supersingular $p \geq 5$), then the conclusion of Theorem 1.2.1 follows from combining the work of Kobayashi on the p -adic Gross–Zagier formula and the non-vanishing of the p -adic height of the Heegner point [28, Thm. 1.1 and Cor. 4.9] with Wan’s recent work on Kobayashi’s supersingular variant of the Iwasawa main conjecture for E [53]; cf. [28, Cor. 1.3]. This argument does not apply in the case where E has ordinary reduction at p as the p -adic height of the Heegner point is then not known to be non-zero. The proof of Theorem 1.2.1 in this paper treats the ordinary and supersingular cases the same and also applies to GL_2 -type modular abelian varieties.

If E has complex multiplication (in which case E is not semistable and N is not square-free), the equality (1.2.a) similarly follows from the p -adic Gross–Zagier formula together with the non-vanishing of the p -adic height of the Heegner point and the Iwasawa main conjectures for E ; see [28, Cor. 1.4].

When $\mathrm{ord}_{s=1} L(E, s) = 0$ (that is, $L(E, 1) \neq 0$) then the p -part of the Birch and Swinnerton-Dyer conjectural formula is also known. In fact, the equality in this case is an important ingredient in our proof of Theorem 1.2.1 as well as the proofs of all the results described above. For more on what is known in this case see Theorem 7.2.1 below.

1.3. Outline of the proof

Theorem 1.2.1 is proved in this paper by separately establishing the upper and lower bounds predicted by (1.1.a) for the order $\#\mathrm{III}(E/\mathbb{Q})[p^\infty]$ of the p -primary part of the Tate–Shafarevich group.

To prove the exact lower bounds we use anticyclotomic Iwasawa theory. For a suitable imaginary quadratic field $\mathcal{K}' = \mathbb{Q}(\sqrt{D'})$ of discriminant $D' < 0$, using arguments similar to [16, §4] we prove a control theorem, Theorem 3.3.1, that compares a specialization of a certain Λ -cotorsion Selmer group (here $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(\mathcal{K}'_\infty/\mathcal{K}')]]$ is the Iwasawa algebra for the anticyclotomic \mathbb{Z}_p -extension \mathcal{K}'_∞ of \mathcal{K}') to a certain \mathbb{Z}_p -cotorsion Selmer group that is closely related to the p -primary part $\mathrm{III}(E/\mathcal{K}') [p^\infty]$ of the Tate–Shafarevich group. This comparison is stated as an explicit formula involving the Tamagawa numbers of E at primes that split in \mathcal{K}' . The Λ -cotorsion Selmer group is the Selmer group related via an anticyclotomic main conjecture to a p -adic L -function recently constructed for modular curves by Bertolini,

Darmon and Prasanna [3] and extended to Shimura curves by Brooks [7] and Liu, Zhang, and Zhang [32]. This p -adic L -function is also a specialization of a two-variable p -adic L -function constructed by Hida, as explained in Section 5. We note that the anticyclotomic main conjecture that we use is different from the classical anticyclotomic main conjecture of Perrin-Riou formulated in [38] (see also [23, p.3]): the p -adic L -functions in the two cases have different ranges of interpolation. Using an extension of the methods of [46], Wan [52, 53] has proved that this p -adic L -function divides the characteristic ideal of the Λ -cotorsion Selmer group up to a power of p (see Section 5 for the definitions of the relevant p -adic L -functions and Section 6 for the precise statement of the main conjecture). To extend this to an unambiguous divisibility in Λ and to pass from this divisibility to lower bounds on $\#\text{III}(E/\mathcal{K}') [p^\infty]$ in terms of the index of a suitable Heegner point, we need two key ingredients: 1) a recent result of Burungale [8] on the vanishing of the corresponding analytic μ -invariant, and 2) a central value formula due to Brooks [7, Thm.1.1] generalizing a recent formula of Bertolini, Darmon and Prasanna relating the p -adic L -function at a point outside of the range of interpolation to the p -adic logarithm of a Heegner point $z_{\mathcal{K}'} \in E(\mathcal{K}')$. The result is the inequality

(1.3.a)

$$\text{ord}_p(\#\text{III}(E/\mathcal{K}') [p^\infty]) \geq \text{ord}_p \left([E(\mathcal{K}') : \mathbb{Z} \cdot z_{\mathcal{K}'}]^2 \prod_{\substack{w|N \\ w \text{ a split prime of } \mathcal{K}'}} c_w(E/\mathcal{K}') \right)$$

The Heegner point $z_{\mathcal{K}'}$ appearing in this formula (and also appearing in the formula of Brooks) comes from a parametrization of E by a Shimura curve X_{N^+, N^-} , $N^+ N^- = N$, of level N^+ attached to a quaternion algebra $B = B_{N^-}$ of discriminant N^- . In order to appeal to the known results about the anticyclotomic main conjecture of interest, it is necessary to take $N^- > 1$ (so this is not the classical Heegner point setting). To pass from the inequality (1.3.a) to one where the right-hand side is replaced with an L -value, we combine the inequality with the general Gross–Zagier formula for the point $z'_{\mathcal{K}'}$, due to Zhang [56] and Yuan, Zhang, and Zhang [55]. The result is the exact lower bound for $\#\text{III}(E/\mathcal{K}') [p^\infty]$ predicted by the BSD formula for E/\mathcal{K}' (see Conjecture 7.1.1). We note that the Tamagawa numbers at the non-split primes of \mathcal{K}' now appear, coming into the Gross–Zagier formula as the ratio of the degree of the usual modular parametrization and the degree of the Shimura curve parametrization (this is essentially due to Ribet and Takahashi [40]). Finally, to obtain the expected lower bound on $\#\text{III}(E/\mathbb{Q}) [p^\infty]$ we express both sides of the resulting inequality for $\#\text{III}(E/\mathcal{K}') [p^\infty]$ in terms

of E/\mathbb{Q} and its \mathcal{K}' -twist $E^{D'}/\mathbb{Q}$. We then exploit the fact that Kato has proved that the predicted *upper bound* holds for $\#\text{III}(E^{D'}/\mathbb{Q})[p^\infty]$ (as \mathcal{K}' is chosen so that $L(E^{D'}, 1) \neq 0$).

Upper bounds on $\#\text{III}(E/\mathbb{Q})[p^\infty]$ are typically achieved by an Euler system argument via the method developed by Kolyvagin [29], which applies since E/\mathbb{Q} is assumed to have analytic rank one. Kolyvagin’s method uses the Euler system constructed from Heegner points that are the images of CM moduli via the usual modular parametrization $X_0(N) \rightarrow E$. As explained in [26], this has a drawback in the sense that it will only give the precise upper bounds on the p -primary part of the Tate-Shafarevich group (for E over a suitable imaginary quadratic field) if at most one Tamagawa number of E is divisible by p . To get around this problem we again consider a parametrization of E by a general Shimura curve X_{N^+, N^-} , $N^+N^- = N$. As explained in Section 7.4.2, it is possible to choose this parametrization so that no Tamagawa number at a prime dividing N^+ is divisible by p . We then choose an imaginary quadratic field $\mathcal{K}'' = \mathbb{Q}(\sqrt{D''})$, $D'' < 0$, such that each prime dividing N^+ splits in \mathcal{K}'' and each prime dividing N^- is inert in \mathcal{K}'' (this will generally be a different field than the \mathcal{K}' used to establish the lower bound). Kolyvagin’s method applied to the Heegner points obtained from the parametrization by X_{N^+, N^-} and the field \mathcal{K}'' then yields an inequality in the direction opposite of (1.3.a):

$$(1.3.b) \quad \text{ord}_p(\#\text{III}(E/\mathcal{K}'')[p^\infty]) \leq \text{ord}_p([E(\mathcal{K}'') : \mathbb{Z} \cdot z_{\mathcal{K}''}]^2).$$

Appealing to the general Gross–Zagier formula for $z_{\mathcal{K}''}$ we then get the upper bound on $\#\text{III}(E/\mathcal{K}'')[p^\infty]$ predicted by the BSD formula for E/\mathcal{K}'' . To pass from this to the expected upper bound for $\#\text{III}(E/\mathbb{Q})[p^\infty]$ we make use of the fact that the predicted *lower bound* for $\#\text{III}(E^{D''}/\mathbb{Q})[p^\infty]$ is known. This lower bound follows from the proved cases of the cyclotomic main conjectures for $E^{D''}$ (see [46, Thm.2(a)] and [45, Thm.C] for the ordinary case and [54, Thm.1.3] for the supersingular case).

It is only at the final step, where we invoke the p -part of the BSD formula for $L(E^{D''}, 1)$, that we need to assume that $a_p(E) = 0$ if E has supersingular reduction at p , which is only a real condition when $p = 3$. Furthermore, most of our arguments apply more generally to the situation where E is replaced by a newform of weight 2, square-free level, and trivial character (see also Section 7.4.4 for additional comments on the general case).

1.4. Organization of the paper

In section 2 we recall some relevant background on Galois representations, local conditions and Selmer modules (generalizations of classical Selmer

groups), as well as the specific cases arising from newforms and modular abelian varieties. In Section 3 we prove the control theorems for the relevant anticyclotomic Selmer groups. In Section 4 we include the relevant background on quaternion algebras, Shimura curves, CM points, and the Kolyvagin system coming from a Shimura curve, and we recall the upper bounds on $\#\text{III}(E/\mathcal{K})[p^\infty]$ obtained from Kolyvagin's argument in the setting of Shimura curves. Section 5 is about p -adic L -functions and various comparisons. In it we recall the p -adic anticyclotomic L -function constructed by Brooks [7] and compare it to a specialization of Hida's two variable p -adic L -function [22]. Section 5 also includes the statement of Burungale's result on the vanishing of the analytic anticyclotomic μ -invariants and the statement of Brooks' result expressing a certain value of the anticyclotomic p -adic L -function in terms of a p -adic logarithm of a Heegner point. In Section 6 we discuss the relevant anticyclotomic main conjectures and recent progress on proving them. We complete the proof of our main result, Theorem 1.2.1, in Section 7.

2. Preliminaries

Let $\overline{\mathbb{Q}} \subset \mathbb{C}$ be the algebraic closure of \mathbb{Q} . For any number field $F \subset \overline{\mathbb{Q}}$, let $G_F = \text{Gal}(\overline{\mathbb{Q}}/F)$. For each place v of F , fix an algebraic closure \overline{F}_v of F_v and an F -embedding $\iota_v: \overline{\mathbb{Q}} \hookrightarrow \overline{F}_v$ to get an identification of $G_{F_v} = \text{Gal}(\overline{F}_v/F_v)$ with a decomposition group for v in G_F . For each finite place v , let $I_v \subset G_{F_v}$ be the inertia subgroup and $\text{Frob}_v \in G_{F_v}/I_v$ a geometric¹ Frobenius element. Let \mathbb{F}_v be the residue field of v and $\overline{\mathbb{F}}_v$ an algebraic closure of \mathbb{F}_v . Then there is a canonical identification $G_{F_v}/I_v = \text{Gal}(\overline{\mathbb{F}}_v/\mathbb{F}_v)$.

Throughout, let $p \geq 3$ be a fixed prime and let $\epsilon: G_{\mathbb{Q}} \rightarrow \mathbb{Z}_p^\times$ be the p -adic cyclotomic character.

2.1. Galois representations

Let F be a number field (for much of this paper F will be either \mathbb{Q} or an imaginary quadratic field \mathcal{K}). By a p -adic Galois representation of G_F we will always mean a finite-dimensional vector space V over a finite extension L/\mathbb{Q}_p that is equipped with a continuous L -linear G_F -action. Such a representation

¹Throughout this paper we take geometric normalizations (e.g., for Frobenius elements, for the reciprocity maps of class field theory, for Hodge–Tate weights, for L -functions of Galois representations).

V will be understood to come with a scalar field L . We will always assume that

(geom) V is geometric

in the sense introduced by Fontaine and Mazur [13]: V is unramified away from a finite set of places and potentially semistable at all places $w \mid p$ of F . We will further assume that

(pure) V is pure.

In particular, this means that there is some integer m such that for any finite place w of F at which V is unramified, all the eigenvalues of Frob_w are Weil numbers of absolute value $(\#\mathbb{F}_w)^{m/2}$. More generally, (pure) means that for all finite places w , the Frobenius semi-simplification of the Weil–Deligne representation $WD_w(V)$ associated² with $V|_{G_{F_w}}$ is pure of weight m in the sense defined by Taylor and Yoshida [51].

Let $\mathcal{O} \subset L$ be the ring of integers of L . We will generally choose a G_F -stable \mathcal{O} -lattice $T \subset V$ and let $W = V/T$. The latter is a discrete \mathcal{O} -divisible G_F -module; it is canonically identified with $T \otimes_{\mathcal{O}} L/\mathcal{O}$. Note that the isomorphism class of T , and hence also that of W , is not necessarily uniquely determined. In what follows we will often fix such a triple (V, T, W) .

Let $\mathfrak{m} \subset \mathcal{O}$ be the maximal ideal and $\kappa = \mathcal{O}/\mathfrak{m}$ the residue field. Let \overline{V} be the semi-simplification of the finite-dimensional κ -representation $T/\mathfrak{m}T$. Then \overline{V} is uniquely-determined up to isomorphism; it is independent of the choice of T . Furthermore, if \overline{V} is irreducible, then all lattices $T \subset V$ are homothetic (and so the isomorphism class of T is unique). Note that while our definition of \overline{V} commutes with extension of the scalars κ , the property of being irreducible may not.

²For $w \mid p$ this was defined by Fontaine via p -adic Hodge theory: Let

$$D_{pst}(V) = \bigcup_{E/F_w} (V \otimes B_{st})^{G_E},$$

with E running over all finite extensions of F_w and B_{st} being Fontaine’s ring of semistable p -adic periods. This is a free $L \otimes_{\mathbb{Q}_p} F_w^{\text{ur}}$ -module of rank two with an induced action of the monodromy operator N and Frobenius φ of B_{st} . The Weil–Deligne representation associated to $V|_{G_{F_w}}$ by Fontaine is $WD_w(V) = D_{pst}(V) \otimes_{L \otimes_{\mathbb{Q}_p} F_w^{\text{ur}}} \overline{\mathbb{Q}}_p$ (choose any embedding $F_w^{\text{ur}} \hookrightarrow \overline{\mathbb{Q}}_p$) with the induced action of N . The action of the Weil group $W_{F_w} \subset G_{F_w}$ is defined by twisting its L -linear, F_w^{ur} -semilinear action r_{sl} on $D_{pst}(V)$. An element $g \in W_{F_w}$ acts on $WD_w(V)$ as $r_{sl}(g)\varphi^{\nu(g)}$, where $\nu : W_{F_w} \rightarrow \mathbb{Z}$ is the normalized valuation map.

2.2. Local conditions

Let F be a number field and let (V, T, W) be as in Section 2.1. Let M be an \mathcal{O} -module with a continuous G_F -action. By a local condition for M at a place w of F we mean a subgroup of the local cohomology group $H^1(F_w, M)$. We discuss several local conditions that will be used throughout.

2.2.1. The unramified local condition. For a finite place w of F , the unramified local condition is defined as

$$H_{\text{ur}}^1(F_w, M) = \ker\{H^1(F_w, M) \rightarrow H^1(I_w, M)\},$$

where $I_w \subset G_{F_w}$ is the inertia group at w . Note that we also have

$$H_{\text{ur}}^1(F_w, M) = H^1(\mathbb{F}_w, M^{I_w}).$$

2.2.2. The finite local condition. Following Bloch and Kato [5], for a finite place w of F we define the finite local condition for V to be

$$H_f^1(F_w, V) = \begin{cases} H_{\text{ur}}^1(F_w, V) & w \nmid p\infty \\ \ker\{H^1(F_w, V) \rightarrow H^1(F_w, V \otimes_{\mathbb{Q}_p} B_{\text{cris}})\} & w \mid p \\ 0 & w \mid \infty. \end{cases}$$

The finite local condition for V can be propagated to T and W via the exact sequence $0 \rightarrow T \rightarrow V \rightarrow W \rightarrow 0$. The resulting local conditions are

$$H_f^1(F_w, T) = \text{preimage of } H_f^1(F_w, V) \text{ under the map } H^1(F_w, T) \rightarrow H^1(F_w, V)$$

and

$$H_f^1(F_w, W) = \text{the image of } H_f^1(F_w, V) \text{ under the map } H^1(F_w, V) \rightarrow H^1(F_w, W).$$

Note that for $w \nmid p$ we have

$$H_{\text{ur}}^1(F_w, T) \subset H_f^1(F_w, T) \quad \text{and} \quad H_f^1(F_w, W) \subset H_{\text{ur}}^1(F_w, W)$$

and that neither inclusion need be an equality.

We note for later use that if $\dim_L V = 2$ and V is pure of weight different from 0 and 1, then for $w \nmid p$, $H_f^1(F_w, V) = H_{\text{ur}}^1(F_w, V) = 0$, and

so $H_f^1(F_w, W) = 0$ and $H_f^1(F_w, T) = H^1(F_w, T)_{\text{tor}}$. In fact, in this case we have $H^0(F_w, V) = 0 = H^0(F_w, V^\vee(1))$ (here, $V^\vee = \text{Hom}_L(V, L)$), so $H^1(F_w, V) = 0$ (by Tate’s local duality) and hence $H^1(F_w, T)$ and $H^1(F_w, W)$ both have finite order.

2.2.3. The anticyclotomic local condition. Suppose now that $F = \mathcal{K}$ is an imaginary quadratic field. Suppose also that p splits in \mathcal{K} as $p = v\bar{v}$. By abuse of notation, if w is a place of \mathcal{K} such that the rational prime below w is split in \mathcal{K} (equivalently, if w is of degree one) then we say that w is split in \mathcal{K} . We define the anticyclotomic local condition for V as

$$H_{\text{ac}}^1(\mathcal{K}_w, V) = \begin{cases} H^1(\mathcal{K}_{\bar{v}}, V) & \text{if } w = \bar{v}, \\ H_f^1(\mathcal{K}_w, V) & \text{if } w \nmid p\infty \text{ is split in } \mathcal{K}, \\ 0 & \text{else.} \end{cases}$$

Note that this definition involves the choice of a prime v of \mathcal{K} above p .

We propagate the anticyclotomic local condition via $0 \rightarrow T \rightarrow V \rightarrow W \rightarrow 0$, getting anticyclotomic local conditions for T and W . In particular,

$$H_{\text{ac}}^1(\mathcal{K}_w, W) = \begin{cases} H^1(\mathcal{K}_{\bar{v}}, W)_{\text{div}} & \text{if } w = \bar{v}, \\ H_f^1(\mathcal{K}_w, W) & \text{if } w \nmid p\infty \text{ is split in } \mathcal{K}, \\ 0 & \text{else.} \end{cases}$$

As noted in Section 2.2.2, if $\dim_L V = 2$ and V is pure of weight different from 0 or 1, then the conditions at $w \nmid p\infty$ agree in the split and non-split cases (the local condition is just 0).

2.3. Selmer structures and Selmer modules

Following [33, Ch.2], a Selmer structure \mathcal{F} on M is a choice of a local condition $H_{\mathcal{F}}^1(F_w, M) \subseteq H^1(F_w, M)$ for each place w of F such that for all but finitely many w , $H_{\mathcal{F}}^1(F_w, M) = H_{\text{ur}}^1(F_w, M)$. A Selmer structure \mathcal{F} on M has an associated Selmer module defined as

$$H_{\mathcal{F}}^1(F, M) := \ker \left\{ H^1(F, M) \rightarrow \bigoplus_w H^1(F_w, M) / H_{\mathcal{F}}^1(F_w, M) \right\},$$

where the sum is taken over all places w of F .

If \mathcal{F} is a Selmer structure on M , then we define the dual Selmer structure \mathcal{F}^* on

$$M^* = \text{Hom}_{\text{cont}}(M, \mathbb{Q}_p/\mathbb{Z}_p(1)),$$

the arithmetic dual of M , as

$$H_{\mathcal{F}^*}^1(F_w, M^*) = \text{the annihilator of } H_{\mathcal{F}}^1(F_w, M) \text{ via local duality.}$$

For the purpose of this paper, if S and S' are two finite sets of finite places of \mathcal{K} for which $S \cap S' = \emptyset$ then $\mathcal{F}_S^{S'}$ will denote the Selmer structure obtained from \mathcal{F} by replacing the local conditions at the places in S with the trivial local conditions and the local conditions at the places in S' with the relaxed local conditions (i.e., $H_{\mathcal{F}_S^{S'}}^1(\mathcal{K}_w, M) = H^1(\mathcal{K}_w, M)$ for $w \in S'$ and $H_{\mathcal{F}_S^{S'}}^1(\mathcal{K}_w, M) = 0$ for $w \in S$).

2.3.1. A consequence of Poitou-Tate duality. If \mathcal{F} and \mathcal{G} are two Selmer structures on M , we write $\mathcal{F} \preceq \mathcal{G}$ if $H_{\mathcal{F}}^1(F_w, M) \subseteq H_{\mathcal{G}}^1(F_w, M)$ for every place w of F . If $\mathcal{F} \preceq \mathcal{G}$, there is a perfect bilinear pairing

$$\frac{H_{\mathcal{G}}^1(F_w, M)}{H_{\mathcal{F}}^1(F_w, M)} \times \frac{H_{\mathcal{F}^*}^1(F_w, M^*)}{H_{\mathcal{G}^*}^1(F_w, M^*)} \rightarrow \mathbb{Q}/\mathbb{Z}$$

that is induced from the Tate local pairing.

The following theorem is a consequence of the Poitou–Tate global duality theorem (see [42, Thm.1.7.3], [35, Thm.I.4.10] and [48, Thm.3.1]):

Theorem 2.3.2. *Let $\mathcal{F} \preceq \mathcal{G}$ be two Selmer structures on M and consider the exact sequences*

$$0 \rightarrow H_{\mathcal{F}}^1(F, M) \hookrightarrow H_{\mathcal{G}}^1(F, M) \xrightarrow{\text{loc}_{\mathcal{F}}^{\mathcal{G}}} \left(\bigoplus_w \frac{H_{\mathcal{G}}^1(F_w, M)}{H_{\mathcal{F}}^1(F_w, M)} \right)$$

and

$$0 \rightarrow H_{\mathcal{G}^*}^1(F, M^*) \hookrightarrow H_{\mathcal{F}^*}^1(F, M^*) \xrightarrow{\text{loc}_{\mathcal{G}^*}^{\mathcal{F}^*}} \left(\bigoplus_w \frac{H_{\mathcal{F}^*}^1(F_w, M^*)}{H_{\mathcal{G}^*}^1(F_w, M^*)} \right),$$

where $\text{loc}_{\mathcal{F}}^{\mathcal{G}}$ and $\text{loc}_{\mathcal{G}^*}^{\mathcal{F}^*}$ are the natural restriction maps and the sum is over all places w , for which $H_{\mathcal{F}}^1(F_w, M) \subsetneq H_{\mathcal{G}}^1(F_w, M)$. The images of $\text{loc}_{\mathcal{F}}^{\mathcal{G}}$ and $\text{loc}_{\mathcal{G}^*}^{\mathcal{F}^*}$ are orthogonal complements with respect to the pairing $\sum_w \langle -, - \rangle_w$ obtained from the local Tate pairings on the local cohomology groups.

2.3.3. The finite and anticyclotomic Selmer structures. Let (V, T, W) be as in Section 2.1 and let M be one of $T, V,$ or W . The finite (or Bloch-Kato) Selmer structure \mathcal{F}_{BK} is defined by the finite local conditions

$$H^1_{\mathcal{F}_{\text{BK}}}(F_w, M) = H^1_f(F_w, M).$$

Note that $\mathcal{F}_{\text{BK}}^*$ is just the finite Selmer structure on M^* (see [5, Prop.3.8]). If $F = \mathcal{K}$ is an imaginary quadratic field in which p splits as $p = v\bar{v}$, then the anticyclotomic Selmer structure \mathcal{F}_{ac} is defined by the anticyclotomic local conditions

$$H^1_{\mathcal{F}_{\text{ac}}}(\mathcal{K}_w, M) = H^1_{\text{ac}}(\mathcal{K}_w, M).$$

2.3.4. Iwasawa-theoretic Selmer structures. Let \mathcal{K} be an imaginary quadratic field and let F_∞ denote either the anticyclotomic \mathbb{Z}_p -extension or the \mathbb{Z}_p^2 -extension of \mathcal{K} . As before, we assume that p splits in \mathcal{K} , i.e., $p = v\bar{v}$. Let $R = \mathcal{O}[[\text{Gal}(F_\infty/\mathcal{K})]]$ be the associated Iwasawa algebra and consider the R -module $M = T \otimes_{\mathcal{O}} \widehat{R}$ where $\widehat{R} = \text{Hom}_{\mathcal{O}, \text{cont}}(R, L/\mathcal{O})$. The module M is equipped with a $G_{\mathcal{K}}$ -action given by $\rho \otimes \Psi^{-1}$ where $\rho: G_{\mathcal{K}} \rightarrow \text{Aut}(T)$ is the representation of $G_{\mathcal{K}}$ on T and $\Psi: G_{\mathcal{K}} \rightarrow R^\times$ is the character naturally defined by the projection $G_{\mathcal{K}} \twoheadrightarrow \text{Gal}(F_\infty/\mathcal{K})$.

We define two Selmer structures \mathcal{F}_{ac} and \mathcal{F}_{Gr} on M that we refer to as the anticyclotomic and the Greenberg Selmer structures, respectively. The anticyclotomic Selmer structure $H^1_{\mathcal{F}_{\text{ac}}}(\mathcal{K}_w, M)$ is defined by

$$H^1_{\mathcal{F}_{\text{ac}}}(\mathcal{K}_w, M) = \begin{cases} H^1(\mathcal{K}_{\bar{v}}, M) & \text{if } w = \bar{v} \\ H^1_{\text{ur}}(\mathcal{K}_w, M) & \text{if } w \nmid p\infty \text{ is split,} \\ 0 & \text{else.} \end{cases}$$

The Greenberg Selmer structure is defined by

$$H^1_{\mathcal{F}_{\text{Gr}}}(\mathcal{K}_w, M) = \begin{cases} H^1(\mathcal{K}_{\bar{v}}, M) & \text{if } w = \bar{v}, \\ H^1_{\text{ur}}(\mathcal{K}_w, M) & \text{else.} \end{cases}$$

Remark 2.3.5. When F_∞ is the anticyclotomic \mathbb{Z}_p -extension of \mathcal{K} , the anticyclotomic Selmer structure gives rise to a global Selmer module $H^1_{\mathcal{F}_{\text{ac}}}(\mathcal{K}, M)$ whose Pontrjagin dual $X_{\text{ac}}(M) = \text{Hom}_{\mathcal{O}}(H^1_{\mathcal{F}_{\text{ac}}}(\mathcal{K}, M), L/\mathcal{O})$ appears in the statement of the anticyclotomic main conjecture that will be relevant to our argument (see Section 6.1 for more details).

Remark 2.3.6. For the particular modules $M = T \otimes_{\mathcal{O}} \widehat{R}$ that we will consider later, the $G_{\mathcal{K}}$ -module $T \otimes_{\mathcal{O}} R$ can be viewed as a p -adic family of motivic p -adic Galois representations. Moreover, the inductions of these representations to $G_{\mathbb{Q}}$ satisfy the Panchishkin condition at p (see [15, p. 211]). In this case, the Greenberg Selmer condition above can be identified with a special case of the Selmer conditions defined by Greenberg [15]. When F_{∞} is the \mathbb{Z}_p^2 -extension of \mathcal{K} , the Iwasawa–Greenberg conjecture [15, Conj. 4.1] relates the characteristic ideal of $X_{\text{Gr}}(M) = \text{Hom}_{\mathcal{O}}(\mathbb{H}_{\text{Gr}}^1(\mathcal{K}, M), L/\mathcal{O})$ to the two-variable p -adic L -function constructed by Hida [22] (see Section 5.2 for details).

2.4. Newforms, their Galois representations, and modular abelian varieties

We introduce notation for and recall basic properties of newforms and their associated p -adic Galois representations.

2.4.1. Newforms. Let $f \in S_{2k}(\Gamma_0(N))$ be a normalized newform of weight $2k$, level N , and trivial Nebentypus. Let $f = \sum_{n=1}^{\infty} a_n(f)q^n$ be its q -expansion at the cusp ∞ . The Fourier coefficients $a_n(f)$ generate a finite extension $\mathbb{Q}(f) \subset \mathbb{C}$ of \mathbb{Q} . Fix an embedding $\mathbb{Q}(f) \hookrightarrow \overline{\mathbb{Q}_p}$ and let $L \subset \overline{\mathbb{Q}_p}$ be a finite extension of \mathbb{Q}_p containing the image $\mathbb{Q}(f)$. Let \mathcal{O} be the ring of integers of L .

2.4.2. Galois representations associated to newforms. Associated to f , L and the fixed embedding $\mathbb{Q}(f) \hookrightarrow L$ is a two-dimensional L -space V_f with a continuous, absolutely irreducible L -linear $G_{\mathbb{Q}}$ -action that is characterized by the equality of L -functions³:

$$L(V_f^{\vee}, s) = L(f, s),$$

where V_f^{\vee} is the L -dual⁴ of the $G_{\mathbb{Q}}$ -representation V_f . This equality of L -functions can be refined as follows. Let $\pi = \otimes_{\ell \leq \infty} \pi_{\ell}$ be the cuspidal automorphic representation such that $L(\pi, s - 1/2) = L(f, s)$. Then the Frobenius-semisimplification of the Weil–Deligne representation $WD_{\ell}(V_f^{\vee})$ associated

³Following our convention of using geometric normalizations, the Euler factors of a Galois representation (or a Weil–Deligne representation) are defined via the action of geometric Frobenius on inertia invariants; Euler factors at p are defined using the Weil–Deligne representation associated with $V_f^{\vee}|_{G_{\mathbb{Q}_p}}$.

⁴We have adopted the conventions here so if f is associated with an elliptic curve E/\mathbb{Q} , then V_f is just the \mathbb{Q}_p -Tate module of E (or an extension of scalars thereof).

with each local Galois representation $V_f^\vee|_{G_{\mathbb{Q}_\ell}}$ is, after extending scalars from L to $\overline{\mathbb{Q}_p}$ and fixing a $\mathbb{Q}(f)$ -isomorphism $\mathbb{C} \cong \overline{\mathbb{Q}_p}$, the Weil–Deligne representation associated with $\pi_\ell \otimes |\cdot|_\ell^{-1/2}$ via the local Langlands correspondence. An important feature of the Galois representation V_f is that it is geometric and pure of weight $1 - 2k$.

2.4.3. Modular abelian varieties. Associated to a newform $f \in S_2(\Gamma_0(N))$ of weight 2 is an isogeny class of abelian varieties whose endomorphism rings contain an order in the ring of integers $\mathbb{Z}(f)$ of $\mathbb{Q}(f)$. Let A_f be an abelian variety in this isogeny class such that $\mathbb{Z}(f) \hookrightarrow \text{End}_{\mathbb{Q}} A_f$ (such an A_f always exists). The p -adic Tate module $T_p A_f$ is a free $\mathbb{Z}(f) \otimes \mathbb{Z}_p$ -module of rank two. Let \mathfrak{p} be a prime of $\mathbb{Z}(f)$ containing p and let $T_{\mathfrak{p}} A_f = T_p A_f \otimes_{\mathbb{Z}(f) \otimes \mathbb{Z}_p} \mathbb{Z}(f)_{\mathfrak{p}}$; this is the \mathfrak{p} -adic Tate-module of A_f . Let $V_{\mathfrak{p}} A_f = T_{\mathfrak{p}} A_f \otimes_{\mathbb{Z}(f)_{\mathfrak{p}}} \mathbb{Q}(f)_{\mathfrak{p}}$. The quotient $V_{\mathfrak{p}} A_f / T_{\mathfrak{p}} A_f \cong T_{\mathfrak{p}} A_f \otimes_{\mathbb{Z}(f)_{\mathfrak{p}}} \mathbb{Q}(f)_{\mathfrak{p}} / \mathbb{Z}(f)_{\mathfrak{p}}$ is naturally identified with $A_f[\mathfrak{p}^\infty]$; this identifies $A_f[\mathfrak{p}^n]$ with $T_{\mathfrak{p}} A_f / \mathfrak{p}^n T_{\mathfrak{p}} A_f$ for each $n \geq 1$. For $L = \mathbb{Q}(f)_{\mathfrak{p}}$ and $\mathcal{O} = \mathbb{Z}(f)_{\mathfrak{p}}$, $V_{\mathfrak{p}} A_f$ is just the V_f of Section 2.4.2, and $(V_{\mathfrak{p}} A_f, T_{\mathfrak{p}} A_f, A_f[\mathfrak{p}^\infty])$ is an example of a triple (V, T, W) as in Section 2.1.

2.4.4. Selmer groups of newforms and modular abelian varieties.

Let $f \in S_{2k}(\Gamma_0(N))$ be a newform and V_f an associated p -adic Galois representation as in Section 2.4.2. Let $T_f \subset V_f$ be an $G_{\mathbb{Q}}$ -stable \mathcal{O} -lattice and let $W_f = V_f / T_f$.

For a number field F , let $L(V_f^\vee / F, s)$ be the L -function of the G_F -representation V_f^\vee . Then $L(V_f^\vee / \mathbb{Q}, s)$ is just the usual L -function $L(f, s)$, and more generally $L(V_f^\vee / F, s)$ is the value at $s - 1/2$ of the L -function of the formal base change to GL_2 / F of the automorphic representation π of Section 2.4.2. The Bloch–Kato conjectures connect the central value $L(V_f^\vee / F, k)$ with the order of the Selmer module⁵ $H_{\mathcal{F}_{\text{BK}}}^1(F, W_f(1 - k))$.

Suppose that f has weight 2 and $(V_f, T_f, W_f) = (V_{\mathfrak{p}} A_f, T_{\mathfrak{p}} A_f, A_f[\mathfrak{p}^\infty])$. Then for any number field F , $H_{\mathcal{F}_{\text{BK}}}^1(F, W_f)$ is just the usual \mathfrak{p} -adic Selmer group of A_f :

$$(2.4.a) \quad H_{\mathcal{F}_{\text{BK}}}^1(F, W_f) = \text{Sel}_{\mathfrak{p}}(A_f / F) = \text{Sel}_p(A_f / F) \otimes_{\mathbb{Z}(f) \otimes \mathbb{Z}_p} \mathbb{Z}(f)_{\mathfrak{p}}.$$

Here $\text{Sel}_p(A_f / F)$ is the usual p -adic Selmer group of A_f / F and $\text{Sel}_{\mathfrak{p}}(A_f / F)$ is the usual \mathfrak{p} -adic Selmer group of A_f / F .

⁵Note the Tate-twist: if $V = V_f(1 - k)$, then $L(V_f^\vee / F, s) = L(V^* / F, s - k)$, so the central critical value is just $L(V^*, 0)$.

3. An anticyclotomic control theorem

Let \mathcal{K}/\mathbb{Q} be an imaginary quadratic field such that p splits in \mathcal{K} :

(split)
$$p = v\bar{v}.$$

Let $\tau \in \text{Gal}(\mathcal{K}/\mathbb{Q})$ be the nontrivial automorphism. Let \mathcal{K}_∞ be the anticyclotomic \mathbb{Z}_p -extension of \mathcal{K} and let $\Gamma = \text{Gal}(\mathcal{K}_\infty/\mathcal{K})$.

Let (V, T, W) , and so also L and \mathcal{O} , be as in Section 2.1. Let $\Lambda = \mathcal{O}[[\Gamma]]$ and put

$$M = T \otimes_{\mathcal{O}} \widehat{\Lambda}, \quad \widehat{\Lambda} = \text{Hom}_{\text{cont}}(\Lambda, \mathbb{Q}_p/\mathbb{Z}_p).$$

We equip M with an action of $G_{\mathcal{K}}$ via $\rho \otimes \Psi^{-1}$ where the projection $\Psi: G_{\mathcal{K}} \rightarrow \Gamma$ is viewed as a continuous Λ^\times -valued character of $G_{\mathcal{K}}$. Given a finite set Σ of finite places $w \nmid p$, let

$$X_{\text{ac}}^\Sigma(M) = \text{Hom}_{\mathcal{O}} \left(\mathbb{H}_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}, M), L/\mathcal{O} \right).$$

We begin this section by listing a few assumptions on the Galois representation V and the related Selmer modules that will be assumed to be in force in all that follows. Then under these assumptions we relate the order of the Selmer module $\mathbb{H}_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}, W)$ to the order of the Shafarevich–Tate group $\text{III}_{\text{BK}}(W/\mathcal{K})$, defined à la Bloch–Kato as

$$\text{III}_{\text{BK}}(W/\mathcal{K}) = \mathbb{H}_{\mathcal{F}_{\text{BK}}}^1(\mathcal{K}, W) / \mathbb{H}_{\mathcal{F}_{\text{BK}}}^1(\mathcal{K}, W)_{\text{div}}.$$

We then prove a control theorem providing a connection between the order of $\mathbb{H}_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}, W)$ and the characteristic ideal of $X_{\text{ac}}^\Sigma(M)$. The latter is linked to p -adic L -functions via the anticyclotomic main conjectures discussed in Section 6. Finally, we deduce some consequences for the Selmer groups associated with modular forms and modular abelian varieties.

3.1. A few assumptions on (V, T, W)

In addition to (geom) and (pure) we will assume that

(sst) V is semistable as a representation of $G_{\mathcal{K}_w}$ for all $w \mid p$

and that

(τ -dual)
$$T^* \cong T^\tau,$$

where T^τ denotes the $G_{\mathcal{K}}$ -module with same underlying space \mathcal{O} -module structure as T but with the $G_{\mathcal{K}}$ -action composed with conjugation by (a lift of) τ . This last hypothesis forces the weight of V to be -1 (that is, V is pure of weight -1). To slightly simplify some arguments we will additionally assume that

$$(2\text{-dim}) \quad \dim_L V = 2,$$

that

$$(HT) \quad \text{no non-zero Hodge-Tate weight of } V \text{ is } \equiv 0 \pmod{p-1},$$

and that

$$(\text{irred}_{\mathcal{K}}) \quad \bar{V} \text{ is an irreducible } \kappa\text{-representation of } G_{\mathcal{K}}.$$

We assume furthermore that

$$(\text{corank } 1) \quad H^1_{\mathcal{F}_{\text{BK}}}(\mathcal{K}, W)_{\text{div}} \cong L/\mathcal{O} \text{ and } H^1_f(\mathcal{K}_w, W) \cong L/\mathcal{O}, \ w \mid p,$$

and

$$(\text{sur}) \quad H^1_{\mathcal{F}_{\text{BK}}}(\mathcal{K}, W)_{\text{div}} \xrightarrow{\text{loc}_w} H^1_f(\mathcal{K}_w, W), \ w \mid p.$$

3.2. Relating $H^1_{\mathcal{F}_{\text{ac}}}(\mathcal{K}, W)$ to $\text{III}_{\text{BK}}(W/\mathcal{K})$

We will prove the following:

Proposition 3.2.1. *One has*

$$\# H^1_{\mathcal{F}_{\text{ac}}}(\mathcal{K}, W) = \#\text{III}_{\text{BK}}(W/\mathcal{K}) \cdot (\#\delta_v)^2,$$

where $\delta_v = \text{coker}\{H^1_{\mathcal{F}_{\text{BK}}}(\mathcal{K}, T) \xrightarrow{\text{loc}_v} H^1_f(\mathcal{K}_v, T)/H^1(\mathcal{K}_v, T)_{\text{tor}}\}$. In particular, $H^1_{\mathcal{F}_{\text{ac}}}(\mathcal{K}, W)$ has finite order.

Proof. Let $\mathcal{F} = \mathcal{F}_{\text{BK}}$. Consider the exact sequence

$$(3.2.a) \quad 0 \rightarrow H^1_{\mathcal{F}_v}(\mathcal{K}, W) \rightarrow H^1_{\mathcal{F}}(\mathcal{K}, W) \rightarrow H^1_f(\mathcal{K}_v, W)$$

and the dual exact sequence

$$(3.2.b) \quad 0 \rightarrow H^1_{\mathcal{F}}(\mathcal{K}, W^*) \rightarrow H^1_{\mathcal{F}_v}(\mathcal{K}, W^*) \rightarrow H^1(\mathcal{K}_v, W^*)/H^1_f(\mathcal{K}_v, W^*).$$

By the assumption (sur), (3.2.a) is surjective on the right. It then follows from Theorem 2.3.2 that the image of the map $H_{\mathcal{F}_v}^1(\mathcal{K}, W^*) \rightarrow H^1(\mathcal{K}_v, W^*)/H_f^1(\mathcal{K}_v, W^*)$ in (3.2.b) is 0, and so

$$(3.2.c) \quad H_{\mathcal{F}}^1(\mathcal{K}, W^*) = H_{\mathcal{F}_v}^1(\mathcal{K}, W^*).$$

By (3.2.a) and (sur) we have a map of short exact sequences

$$\begin{array}{ccccccc} 0 & \longrightarrow & H_{\mathcal{F}_v}^1(\mathcal{K}, W) \cap H_{\mathcal{F}}^1(\mathcal{K}, W)_{\text{div}} & \longrightarrow & H_{\mathcal{F}}^1(\mathcal{K}, W)_{\text{div}} & \longrightarrow & H_f^1(\mathcal{K}_v, W) \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow = \\ 0 & \longrightarrow & H_{\mathcal{F}_v}^1(\mathcal{K}, W) & \longrightarrow & H_{\mathcal{F}}^1(\mathcal{K}, W) & \longrightarrow & H_f^1(\mathcal{K}_v, W) \longrightarrow 0 \end{array}$$

As $H_{\mathcal{F}_v}^1(\mathcal{K}, W) \cap H_{\mathcal{F}}^1(\mathcal{K}, W)_{\text{div}} = \ker\{H_{\mathcal{F}}^1(\mathcal{K}, W)_{\text{div}} \rightarrow H_f^1(\mathcal{K}_v, W)\}$, by applying the snake lemma to the preceding diagram we conclude that

$$(3.2.d) \quad \begin{aligned} \# H_{\mathcal{F}_v}^1(\mathcal{K}, W) &= \#\text{III}_{\text{BK}}(W/\mathcal{K}) \cdot \#\ker\{H_{\mathcal{F}}^1(\mathcal{K}, W)_{\text{div}} \rightarrow H_f^1(\mathcal{K}_v, W)\} \\ &= \#\text{III}_{\text{BK}}(W/\mathcal{K}) \cdot \#\delta_v. \end{aligned}$$

The last equality requires an explanation which we now provide: first, the hypothesis (corank 1) implies that both

$$H_{\mathcal{F}}^1(\mathcal{K}, T)/H_{\mathcal{F}}^1(\mathcal{K}, T)_{\text{tors}} \quad \text{and} \quad H_{\mathcal{F}}^1(\mathcal{K}_v, T)/H_{\mathcal{F}}^1(\mathcal{K}_v, T)_{\text{tors}}$$

are free \mathcal{O} -modules of rank one, so the localization map

$$H_{\mathcal{F}}^1(\mathcal{K}, T)/H_{\mathcal{F}}^1(\mathcal{K}, T)_{\text{tors}} \rightarrow H_{\mathcal{F}}^1(\mathcal{K}_v, T)/H_{\mathcal{F}}^1(\mathcal{K}_v, T)_{\text{tors}}$$

is injective. Next, hypothesis (sur) implies the short exact sequence

$$0 \rightarrow H_{\mathcal{F}}^1(\mathcal{K}, T)/H_{\mathcal{F}}^1(\mathcal{K}, T)_{\text{tor}} \rightarrow H_f^1(\mathcal{K}_v, T)/H^1(\mathcal{K}_v, T)_{\text{tor}} \rightarrow \delta_v \rightarrow 0,$$

and that δ_v has finite order. Finally, using that $H_{\mathcal{F}}^1(\mathcal{K}, T) \otimes L/\mathcal{O} \cong H_{\mathcal{F}}^1(\mathcal{K}, W)_{\text{div}}$ and tensoring the above exact sequence with L/\mathcal{O} , we obtain

$$\#\ker\{H_{\mathcal{F}}^1(\mathcal{K}, W)_{\text{div}} \rightarrow H_f^1(\mathcal{K}_v, W)\} = \#\delta_v.$$

It now follows from V being pure of weight different from 0 or 1 that we have an exact sequence

$$0 \rightarrow H_{\mathcal{F}_v}^1(\mathcal{K}, W) \rightarrow H_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}, W) \xrightarrow{\alpha} H^1(\mathcal{K}_{\bar{v}}, W)_{\text{div}}/H_f^1(\mathcal{K}_{\bar{v}}, W)$$

(cf. Section 2.2.2) with dual exact sequence

$$0 \rightarrow H^1_{(\mathcal{F}_{ac})^*}(\mathcal{K}, W^*) \rightarrow H^1_{\mathcal{F}_v}(\mathcal{K}, W^*) \xrightarrow{\beta} H^1_f(\mathcal{K}_{\bar{v}}, W^*)/H^1(\mathcal{K}_{\bar{v}}, W^*)_{\text{tor}}.$$

We then have

$$(3.2.e) \quad \# H^1_{\mathcal{F}_{ac}}(\mathcal{K}, W) = \# \ker(\alpha) \cdot \# \text{im}(\alpha) = \# \ker(\alpha) \cdot \# \text{coker}(\beta),$$

where the second equality follows from Theorem 2.3.2. It then follows from (3.2.c) that

$$\text{coker}(\beta) = \text{coker}\{H^1_{\mathcal{F}}(\mathcal{K}, W^*) \rightarrow H^1_f(\mathcal{K}_{\bar{v}}, W^*)/H^1(\mathcal{K}_{\bar{v}}, W^*)_{\text{tor}}\}.$$

The hypotheses (τ -dual) and (irred \mathcal{K}) imply that $W^* \cong T^\tau$, so conjugating by the automorphism τ identifies $\text{coker}(\beta)$ with

$$\text{coker}\{H^1_{\mathcal{F}}(\mathcal{K}, T) \rightarrow H^1_f(\mathcal{K}_v, T)/H^1(\mathcal{K}_v, T)_{\text{tor}}\} = \delta_v.$$

Hence combining (3.2.d) and (3.2.e) yields

$$\begin{aligned} \# H^1_{\mathcal{F}_{ac}}(\mathcal{K}, W) &= \# \ker(\alpha) \cdot \# \text{coker}\beta = \# H^1_{\mathcal{F}_v}(\mathcal{K}, W) \cdot \# \delta_v \\ &= \#\text{III}_{\text{BK}}(W/\mathcal{K}) \cdot (\#\delta_v)^2. \end{aligned}$$

Since δ_v has finite order, $H^1_{\mathcal{F}_{ac}}(\mathcal{K}, W)$ has finite order. □

Remark 3.2.2. (a) Note that neither of the assumptions (sst) and (HT) is used in this proof. (b) Clearly, (irred \mathcal{K}) is not essential to the proof of the finiteness of $H^1_{\mathcal{F}_{ac}}(\mathcal{K}, W)$. It is only used to ensure that $W^* \cong T^\tau$, so that δ_v can be identified with the cokernel $\text{coker}\{H^1_{\mathcal{F}}(\mathcal{K}, W^*) \rightarrow H^1_f(\mathcal{K}_{\bar{v}}, W^*)/H^1(\mathcal{K}_{\bar{v}}, W^*)_{\text{tor}}\}$. Under certain circumstances, such as $T = T_p A_f$, we have $W^* \cong T^\tau$ without assuming (irred \mathcal{K}).

3.3. The anticyclotomic control theorem

Let S be a finite set of places of \mathcal{K} including all those at which V is ramified and let $S_p \subset S$ be the subset of those not dividing p . Let $\Sigma \subset S_p$. Fix a topological generator $\gamma \in \Gamma$. We identify $\mathcal{O}[[T]]$ with $\Lambda = \mathcal{O}[[\Gamma]]$ via the continuous \mathcal{O} -algebra map sending $1 + T \mapsto \gamma$. We will prove the following theorem:

Theorem 3.3.1 (Anticyclotomic Control Theorem). *The Λ -module $X_{\text{ac}}^\Sigma(M)$ is Λ -torsion, and if $f_{\text{ac}}^\Sigma(T)$ is a generator of its characteristic Λ -ideal $\text{char}(X_{\text{ac}}^\Sigma(M))$, then*

$$\#\mathcal{O}/f_{\text{ac}}^\Sigma(0) = \#H_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}, W) \cdot C^\Sigma(W),$$

where

$$C^\Sigma(W) = \#H^0(\mathcal{K}_v, W) \cdot \#H^0(\mathcal{K}_{\bar{v}}, W) \cdot \prod_{\substack{w \in S_p \setminus \Sigma \\ w \text{ split}}} \#H_{\text{ur}}^1(\mathcal{K}_w, W) \cdot \prod_{w \in \Sigma} \#H^1(\mathcal{K}_w, W).$$

Our proof of Theorem 3.3.1 follows the arguments of Greenberg in [16, §4].

3.3.2. Surjectivity of the localization maps. For a finite set S' of finite places of \mathcal{K} let

$$\mathcal{P}_{\mathcal{F}_{\text{ac}}}(M; S') = \prod_{w \in S'} \frac{H^1(\mathcal{K}_w, M)}{H_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}_w, M)} \quad \text{and} \quad \mathcal{P}_{\mathcal{F}_{\text{ac}}}(W; S') = \prod_{w \in S'} \frac{H^1(\mathcal{K}_w, W)}{H_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}_w, W)}.$$

The key to our result relating $H_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}_\infty, M)^\Gamma$ to $H^1(\mathcal{K}^S/\mathcal{K}, W)$ is understanding the images of

$$(3.3.a) \quad H^1(\mathcal{K}^S/\mathcal{K}, M) \xrightarrow{\text{loc}_S} \mathcal{P}_{\mathcal{F}_{\text{ac}}}(M; S)$$

and

$$(3.3.b) \quad H^1(\mathcal{K}^S/\mathcal{K}, W) \xrightarrow{\text{loc}_S} \mathcal{P}_{\mathcal{F}_{\text{ac}}}(W; S).$$

Here $\mathcal{K}^S/\mathcal{K}$ is the maximal extension unramified at all finite places not in S .

Proposition 3.3.3. *The restriction maps (3.3.a) and (3.3.b) are surjective.*

Proof. Note that (τ -dual) implies that the arithmetic dual M^* of M is just $T \otimes_{\mathcal{O}} \Lambda$ with $G_{\mathcal{K}}$ -action given by $\rho \otimes \Psi$. Recall that

$$H_{(\mathcal{F}_{\text{ac}}^S)_{\bar{v}}}^1(\mathcal{K}, M^*) = \{c \in H_{\mathcal{F}_{\text{ac}}^S}^1(\mathcal{K}, M^*) : \text{loc}_{\bar{v}}c = 0\}.$$

By Theorem 2.3.2 the dual of the cokernel of (3.3.a) is identified with a quotient of $H_{(\mathcal{F}_{\text{ac}}^S)_{\bar{v}}}^1(\mathcal{K}, M^*)$. Therefore, to prove the desired surjectivity of (3.3.a), it suffices to show that $H_{(\mathcal{F}_{\text{ac}}^S)_{\bar{v}}}^1(\mathcal{K}, M^*) = 0$.

Note that $M^*/(\gamma - 1)M^* \xrightarrow{\sim} T$. We claim that the natural injection

$$H^1(\mathcal{K}^S/\mathcal{K}, M^*)/(\gamma - 1)H^1(\mathcal{K}^S/\mathcal{K}, M^*) \hookrightarrow H^1(\mathcal{K}^S/\mathcal{K}, T)$$

induces an injection

$$H^1_{(\mathcal{F}_{ac}^S)^*}(\mathcal{K}^S/\mathcal{K}, M^*)/(\gamma - 1)H^1_{(\mathcal{F}_{ac}^S)^*}(\mathcal{K}^S/\mathcal{K}, M^*) \hookrightarrow H^1_{(\mathcal{F}_{ac}^S)_{\bar{v}}}(\mathcal{K}, T).$$

For this, suppose $c \in H^1_{(\mathcal{F}_{ac}^S)^*}(\mathcal{K}^S/\mathcal{K}, M^*)$ has trivial image in $H^1_{(\mathcal{F}_{ac}^S)_{\bar{v}}}(\mathcal{K}, T)$. Then $c = (\gamma - 1)d$ for some $d \in H^1(\mathcal{K}^S/\mathcal{K}, M^*)$ such that $(\gamma - 1)d = 0$ in $H^1(\mathcal{K}_{\bar{v}}, M^*)$. But the kernel of multiplication by $\gamma - 1$ on $H^1(\mathcal{K}_{\bar{v}}, M^*)$ is the image of $H^0(\mathcal{K}_{\bar{v}}, T)$. The vanishing of the latter follows from $H^0(\mathcal{K}_{\bar{v}}, V) = 0$ (which is true as V is pure of weight different from 0 or 1: $V^{G_{\kappa_{\bar{v}}}} \neq 0$ would imply that 1 was an eigenvalue of Frobenius on $WD_{\bar{v}}(V)^{N=0}$, which would contradict purity if the weight is not 0 or 1).

Next we note that the canonical isomorphism $T \otimes_{\mathcal{O}} L/\mathcal{O} \cong W$ induces an injection

$$H^1_{(\mathcal{F}_{ac}^S)_{\bar{v}}}(\mathcal{K}, T) \otimes_{\mathcal{O}} L/\mathcal{O} \hookrightarrow H^1_{(\mathcal{F}_{ac}^S)_{\bar{v}}}(\mathcal{K}, W).$$

It follows from Proposition 3.2.1 that the right-hand side is finite (reversing the roles of v and \bar{v} and using that $H^1(K_w, W)$ is finite for $w \nmid p$ (cf. Section 2.2.2)). As (irred $_{\mathcal{K}}$) implies $H^1_{(\mathcal{F}_{ac}^S)_{\bar{v}}}(\mathcal{K}, T)$ is torsion-free, it follows from the finiteness of $H^1_{(\mathcal{F}_{ac}^S)_{\bar{v}}}(\mathcal{K}, W)$ that $H^1_{(\mathcal{F}_{ac}^S)_{\bar{v}}}(\mathcal{K}, T) = 0$. Hence

$$H^1_{(\mathcal{F}_{ac}^S)_{\bar{v}}}(\mathcal{K}, M^*)/(\gamma - 1)H^1_{(\mathcal{F}_{ac}^S)_{\bar{v}}}(\mathcal{K}, M^*) = 0,$$

and so, by Nakayama’s lemma, $H^1_{(\mathcal{F}_{ac}^S)_{\bar{v}}}(\mathcal{K}, M^*) = 0$. This completes the proof of the surjectivity of (3.3.a). The proof of the surjectivity of (3.3.b) is similar: Poitou–Tate duality identifies the cokernel with a quotient of $H^1_{(\mathcal{F}_{ac}^S)_{\bar{v}}}(\mathcal{K}, T)$, which we have already seen to be 0. \square

3.3.4. Trivial coinvariants. We now show that $H^1(\mathcal{K}^S/\mathcal{K}, M)_{\Gamma}$ and $H^1_{\mathcal{F}_{ac}^S}(\mathcal{K}, M)_{\Gamma}$ both vanish:

Lemma 3.3.5. *We have $H^1(\mathcal{K}^S/\mathcal{K}, M)_{\Gamma} = 0$ and $H^1_{\mathcal{F}_{ac}^S}(\mathcal{K}, M)_{\Gamma} = 0$.*

Proof. The long exact sequence on Galois cohomology associated to the short exact sequence $0 \rightarrow W \rightarrow M \xrightarrow{\gamma-1} M \rightarrow 0$ yields an injection $H^1(\mathcal{K}^S/\mathcal{K}, M)_{\Gamma} \hookrightarrow H^2(\mathcal{K}^S/\mathcal{K}, W)$. The local cohomology group $H^2(\mathcal{K}_w, W)$ is dual to $H^0(\mathcal{K}_w, T)$, and the latter is 0; for $w \mid p$ this was explained in the

proof of Proposition 3.3.3, and for $w \nmid p$ this was explained in Section 2.2.2. Consequently (using the notation of [35, §4]),

$$H^2(\mathcal{K}^S/\mathcal{K}, W) = \text{III}_S^2(\mathcal{K}, W) = \{c \in H^2(\mathcal{K}^S/\mathcal{K}, W) : \text{loc}_w c = 0 \ \forall w \in S\}.$$

By Poitou-Tate duality [35, Thm.4.10(a)], this group is dual to

$$\text{III}_S^1(\mathcal{K}, T) = \{c \in H^1(\mathcal{K}^S/\mathcal{K}, T) : \text{loc}_w c = 0 \ \forall w \in S\},$$

and the latter is trivial. Indeed, (irred $_{\mathcal{K}}$) implies that $\text{III}_S^1(\mathcal{K}, T)$ is torsion-free while (corank 1) and (sur) imply that $\text{III}_S^1(\mathcal{K}, T)$ is torsion and thus, $H^1(\mathcal{K}^S/\mathcal{K}, M)_{\Gamma} = 0$.

To show that $H_{\mathcal{F}_{ac}}^1(\mathcal{K}, M)_{\Gamma} = 0$, consider the exact sequence

$$0 \rightarrow H_{\mathcal{F}_{ac}}^1(\mathcal{K}, M) \rightarrow H^1(\mathcal{K}^S/\mathcal{K}, M) \rightarrow \mathcal{P}_{\mathcal{F}_{ac}}(M; S \setminus \Sigma) \rightarrow 0.$$

The exactness on the right is a consequence of Proposition 3.3.3. Multiplying by $\gamma - 1$, we obtain from the snake lemma the exact sequence

$$\begin{aligned} H^1(\mathcal{K}^S/\mathcal{K}, W) &= H^1(\mathcal{K}^S/\mathcal{K}, M)_{\Gamma} \rightarrow \mathcal{P}_{\mathcal{F}_{ac}}(M; S \setminus \Sigma)_{\Gamma} \\ &\rightarrow H_{\mathcal{F}_{ac}}^1(\mathcal{K}, M)_{\Gamma} \rightarrow H^1(\mathcal{K}^S/\mathcal{K}, M)_{\Gamma}. \end{aligned}$$

The map $H^1(\mathcal{K}^S/\mathcal{K}, W) \rightarrow \mathcal{P}_{\mathcal{F}_{ac}}(M; S \setminus \Sigma)_{\Gamma}$ is the composite of the restriction map $H^1(\mathcal{K}^S/\mathcal{K}, W) \rightarrow \mathcal{P}_{\mathcal{F}_{ac}}(W; S \setminus \Sigma)$, which is surjective by Proposition 3.3.3, and the map $\mathcal{P}_{\mathcal{F}_{ac}}(W; S \setminus \Sigma) \rightarrow \mathcal{P}_{\mathcal{F}_{ac}}(M; S \setminus \Sigma)_{\Gamma}$, which is also surjective (as the maps $H^1(\mathcal{K}_w, W) \rightarrow H^1(\mathcal{K}_w, M)_{\Gamma}$ are surjective). It follows that $H_{\mathcal{F}_{ac}}^1(\mathcal{K}, M)_{\Gamma}$ injects into $H^1(\mathcal{K}^S/\mathcal{K}, M)_{\Gamma}$. But we have already shown the latter to be trivial. \square

3.3.6. Computing $\# \ker(r)$. We now calculate the order of the kernel of the map

$$r : \mathcal{P}_{\mathcal{F}_{ac}}(W; S \setminus \Sigma) \rightarrow \mathcal{P}_{\mathcal{F}_{ac}}(M; S \setminus \Sigma)_{\Gamma}.$$

Proposition 3.3.7. *The kernel of r has order*

$$(3.3.c) \quad \# \ker(r) = \# H^0(\mathcal{K}_v, W) \cdot \# H^0(\mathcal{K}_{\bar{v}}, W) \cdot \prod_{\substack{w \in S_p \setminus \Sigma \\ w \text{ split}}} c_w^{(p)}(W),$$

where $c_w^{(p)}(W) := [H_{\text{ur}}^1(\mathcal{K}_w, W) : H_f^1(\mathcal{K}_w, W)] = \# H_{\text{ur}}^1(\mathcal{K}_w, W)$ are the p -parts of the local Tamagawa numbers.

Proof. Let w be a place of \mathcal{K} . By the long exact sequence on Galois cohomology associated to the short sequence

$$0 \rightarrow W \rightarrow M \xrightarrow{\times(\gamma-1)} M \rightarrow 0,$$

the kernel of the restriction map $r_w : H^1(\mathcal{K}_w, W) \rightarrow H^1(\mathcal{K}_w, M)^\Gamma$ is the image of $M^{G_{\mathcal{K}_w}}/(\gamma-1)M^{G_{\mathcal{K}_w}}$ under the coboundary map. Let ℓ be the prime below w . Unlike the cyclotomic case over \mathbb{Q} treated in [16, §3] where every prime w is finitely decomposed in the \mathbb{Z}_p -extension, we need to consider the cases of ℓ being split or non-split in \mathcal{K} separately.

Case 1(a): $w \nmid p$, W is ramified at w and ℓ is split in \mathcal{K} . We have a commutative diagram

$$\begin{CD} 0 @>>> H_{\text{ur}}^1(\mathcal{K}_w, W) @>>> H^1(\mathcal{K}_w, W) @>>> H^1(I_w, W)^{G_{\mathcal{K}_w}} @>>> 0 \\ @. @VVV @VVV @VVV \\ 0 @>>> H_{\text{ur}}^1(\mathcal{K}_w, M) @>>> H^1(\mathcal{K}_w, M) @>>> H^1(I_w, M) @>>> 0 \end{CD}$$

The kernel of the right-most map is just the image of $(M^{I_w}/(\gamma-1)M^{I_w})^{G_{\mathcal{K}_w}}$. Since Ψ is not ramified at w , M^{I_w} is $(\gamma-1)$ -divisible, hence this kernel is trivial. It follows that the map $H^1(\mathcal{K}_w, W)/H_{\text{ur}}^1(\mathcal{K}_w, W) \rightarrow H^1(\mathcal{K}_w, M)/H_{\text{ur}}^1(\mathcal{K}_w, M)$ is injective and hence that the kernel of the map $r_w : H^1(\mathcal{K}_w, W)/H_f^1(\mathcal{K}_w, W) \rightarrow H^1(\mathcal{K}_w, M)/H_{\text{ur}}^1(\mathcal{K}_w, M)$, is isomorphic to $H_{\text{ur}}^1(\mathcal{K}_w, W)/H_f^1(\mathcal{K}_w, W)$. But the order of the latter is exactly the p -part $c_w^{(p)}(W)$ of the Tamagawa number at w .

Case 1(b): $w \nmid p$, W is ramified at w and ℓ is not split in \mathcal{K} . In this case ℓ is inert or ramified in \mathcal{K} , and by the definition of the anticyclotomic Selmer structure both $H_{\mathcal{F}_{\text{ac}}}^1(K_w, W)$ and $H_{\mathcal{F}_{\text{ac}}}^1(K_w, M)$ are trivial. Hence $\ker(r_w) = \ker\{H^1(\mathcal{K}_w, W) \twoheadrightarrow H^1(\mathcal{K}_w, M)[\gamma-1]\}$ and so equals the image of $M^{G_{\mathcal{K}_w}}/(\gamma-1)M^{G_{\mathcal{K}_w}} \hookrightarrow H^1(\mathcal{K}_w, W)$. However, since w is not split, Ψ is trivial on $G_{\mathcal{K}_w}$ and hence, $M^{G_{\mathcal{K}_w}}$ is divisible by $\gamma-1$. It follows that $\ker(r_w) = 0$.

Case 2(a): $w \nmid p$, W is unramified at w and ℓ is split in \mathcal{K} . Similarly to Case 1(a), we obtain $\ker(r_w) \cong H_{\text{ur}}^1(K_w, W)/H_f^1(K_w, W)$ which is trivial since the two local conditions coincide (see [42, Lem.I.3.5(iv)]).

Case 2(b): $w \nmid p$, W is unramified at w and ℓ is not split in \mathcal{K} . Exactly the same argument as employed for Case 1(b) shows that $\ker(r_w) = 0$.

Case 3(a): $w = \bar{v}$. We have $\ker(r_{\bar{v}}) = H^1(\mathcal{K}_{\bar{v}}, W)/H^1(\mathcal{K}_{\bar{v}}, W)_{\text{div}}$. By Tate local duality $H^1(\mathcal{K}_{\bar{v}}, W)/H^1(\mathcal{K}_{\bar{v}}, W)_{\text{div}}$ is dual to $H^1(\mathcal{K}_{\bar{v}}, T)_{\text{tor}}$, which is just $\ker\{H^1(\mathcal{K}_{\bar{v}}, T) \rightarrow H^1(\mathcal{K}_{\bar{v}}, V)\} \cong H^0(\mathcal{K}_{\bar{v}}, W)/H^0(\mathcal{K}_{\bar{v}}, W)_{\text{div}}$. But $H^0(\mathcal{K}_{\bar{v}}, V) = 0$ (as noted in the proof of Proposition 3.3.3, this is a consequence of being pure of weight different from 0 or 1), so $H^0(\mathcal{K}_{\bar{v}}, W)_{\text{div}} = 0$ and $\#\ker(r_{\bar{v}}) = \#H^0(\mathcal{K}_{\bar{v}}, W)$.

Case 3(b): $w = v$. In this case the map is $r_v: H^1(\mathcal{K}_v, W) \rightarrow H^1(\mathcal{K}_v, M)^\Gamma$ and we have

$$\ker(r_v) \cong M^{G_{\mathcal{K}_v}}/(\gamma - 1)M^{G_{\mathcal{K}_v}} \hookrightarrow H^1(\mathcal{K}_v, W).$$

Let $P_v = \ker \Psi|_{G_{\mathcal{K}_v}}$ and $\Gamma_v = G_{\mathcal{K}_v}/P_v \hookrightarrow \Gamma$, where Ψ is as in the beginning of Section 3. Then Γ_v has finite index in Γ , and the image of I_v in Γ_v also has finite index. Let $\gamma_v \in \Gamma_v$ be a topological generator. Let $T^\vee = \text{Hom}_{\mathbb{Z}_p}(T, \mathbb{Z}_p)$ and let $T_{P_v}^\vee$ be its P_v -coinvariants. Then $M = T \otimes_{\mathcal{O}} \widehat{\Lambda} \cong \text{Hom}_{\text{cont}}(T^\vee \otimes_{\mathcal{O}} \Lambda, \mathbb{Q}_p/\mathbb{Z}_p)$ and so $M^{P_v} \cong \text{Hom}_{\text{cont}}(T_{P_v}^\vee \otimes_{\mathcal{O}} \Lambda, \mathbb{Q}_p/\mathbb{Z}_p)$. If $\#T_{P_v}^\vee$ is finite, then $M^{G_{\mathcal{K}_v}}$ is therefore isomorphic to a submodule of $\text{Hom}_{\mathbb{Z}_p}(T_{P_v}^\vee \otimes_{\mathcal{O}} \Lambda/(\gamma_v^{p^t} - 1), \mathbb{Q}_p/\mathbb{Z}_p)$, which has finite order. Here $t > 0$ is such that $\gamma_v^{p^t}$ acts trivially on $T_{P_v}^\vee$. This shows that $M^{G_{\mathcal{K}_v}}$ has finite order if $\#T_{P_v}^\vee$ is finite, in which case

$$\#M^{G_{\mathcal{K}_v}}/(\gamma - 1)M^{G_{\mathcal{K}_v}} = \#M^{G_{\mathcal{K}_v}}[\gamma - 1] = \#M[\gamma - 1]^{G_{\mathcal{K}_v}} = \#H^0(\mathcal{K}_v, W).$$

It remains to show that $\#T_{P_v}^\vee$ is finite, which we will do by arguing by contradiction. Assume that $\#T_{P_v}^\vee$ is not finite. Then $T^{P_v} \neq 0$ and hence $V^{P_v} \neq 0$. As V is two-dimensional and semistable, there are two cases to consider: (i) V is crystalline and (ii) V is non-crystalline and hence a non-split extension of the form $0 \rightarrow L(\epsilon\alpha) \rightarrow V \rightarrow L(\alpha) \rightarrow 0$ with α unramified. In case (i), V^{P_v} would have to be, possibly after a finite extension of scalars, a sum of one-dimensional crystalline representations of weight -1 . Such a crystalline character must be of the form $\epsilon^a\alpha$ for some integer a and some unramified character α , while the condition of being weight -1 means that $\alpha(\text{Frob}_v)$ is a Weil number of absolute value $p^{-1/2+a}$. However, since $\epsilon^a\alpha$ factors through a pro- p -group, so must $\epsilon^a|_{I_v} = \epsilon^a\alpha|_{I_v}$. But this only happens if $a \equiv 0 \pmod{p-1}$. As a is a Hodge-Tate weight of V , it follows from (HT) that we must have $a = 0$. Then α must factor through the quotient of Γ_v by the image of I_v . This quotient is finite, so α must have finite order, contradicting it being a character of weight -1 . On the other hand, if V is as in case (ii), then $V|_{P_v}$ is also a non-split extension of P_v , and so if $V^{P_v} \neq 0$,

then again $\epsilon\alpha$, α unramified, must factor through Γ_v , which we have already seen to be impossible. This contradiction completes the last case and hence proves the lemma. \square

Remark 3.3.8. The proof of Case 3(b) above is the only place where the hypothesis (HT) is invoked.

3.3.9. An application of the snake lemma. There is a commutative diagram

$$\begin{array}{ccccccc}
 0 & \longrightarrow & H^1_{\mathcal{F}_{ac}^\Sigma}(\mathcal{K}, W) & \longrightarrow & H^1(\mathcal{K}^S/\mathcal{K}, W) & \longrightarrow & \mathcal{P}_{\mathcal{F}_{ac}}(W; S \setminus \Sigma) \longrightarrow 0 \\
 & & \downarrow s & & \downarrow h & & \downarrow r \\
 0 & \longrightarrow & H^1_{\mathcal{F}_{ac}^\Sigma}(\mathcal{K}, M)^\Gamma & \longrightarrow & H^1(\mathcal{K}^S/\mathcal{K}, M)^\Gamma & \longrightarrow & \mathcal{P}_{\mathcal{F}_{ac}}(M; S \setminus \Sigma)^\Gamma
 \end{array}$$

(note that exactness of the top row follows from Proposition 3.3.3), and the snake lemma yields an exact sequence

$$0 \rightarrow \ker(s) \rightarrow \ker(h) \rightarrow \ker(r) \rightarrow \operatorname{coker}(s) \rightarrow \operatorname{coker}(h) \rightarrow \operatorname{coker}(r).$$

However, $\operatorname{coker}(h) = 0$ and hence there is an exact sequence

$$0 \rightarrow \ker(s) \rightarrow \ker(h) \rightarrow \ker(r) \rightarrow \operatorname{coker}(s) \rightarrow 0.$$

By Proposition 3.2.1, $H^1_{\mathcal{F}_{ac}^\Sigma}(\mathcal{K}, W)$ is finite and hence,

$$\frac{\# H^1_{\mathcal{F}_{ac}^\Sigma}(\mathcal{K}, M)^\Gamma}{\# H^1_{\mathcal{F}_{ac}^\Sigma}(\mathcal{K}, W)} = \frac{\#\operatorname{coker}(s)}{\#\ker(s)} = \frac{\#\ker(r)}{\#\ker(h)}.$$

The order of $\ker(r)$ was computed in Proposition 3.3.7 while

$$\ker(h) = M^{G\kappa}/(\gamma - 1)M^{G\kappa} = M^{G\kappa} = H^0(\mathcal{K}, W)$$

which vanishes by (irred \mathcal{K}). It follows that

$$(3.3.d) \quad \# H^1_{\mathcal{F}_{ac}^\Sigma}(\mathcal{K}, M)^\Gamma = \# H^1_{\mathcal{F}_{ac}^\Sigma}(\mathcal{K}, W) \cdot \# H^0(\mathcal{K}_v, W) \cdot \# H^0(\mathcal{K}_{\bar{v}}, W) \cdot \prod_{\substack{w \in S_p \setminus \Sigma \\ w \text{ split}}} c_w^{(p)}(W).$$

It also follows from the surjectivity of (3.3.b) that there is an exact sequence

$$0 \rightarrow H^1_{\mathcal{F}_{ac}}(\mathcal{K}, W) \rightarrow H^1_{\mathcal{F}_{ac}^\Sigma}(\mathcal{K}, W) \rightarrow \mathcal{P}_{\mathcal{F}_{ac}}(W; \Sigma) \rightarrow 0.$$

As $H_f^1(\mathcal{K}_w, W) = 0$ (see Section 2.2.2), we have

$$\# H_{\mathcal{F}_{ac}}^1(\mathcal{K}, W) = \# H_{\mathcal{F}_{ac}}^1(\mathcal{K}, W) \cdot \prod_{w \in \Sigma} \# H^1(\mathcal{K}_w, W).$$

Combining this with (3.3.d) yields

$$(3.3.e) \quad \# H_{\mathcal{F}_{ac}}^1(\mathcal{K}, M)^\Gamma = \# H_{\mathcal{F}_{ac}}^1(\mathcal{K}, W) \cdot C^\Sigma(W).$$

3.3.10. Proof of Theorem 3.3.1: torsionness of $X_{ac}^\Sigma(M)$. Since $H_{\mathcal{F}_{ac}}^1(\mathcal{K}, M)^\Gamma$ has finite order, so does $X_{ac}^\Sigma(M)_\Gamma = \text{Hom}_{\mathcal{O}}(H_{\mathcal{F}_{ac}}^1(\mathcal{K}, M)^\Gamma, L/\mathcal{O})$. It follows easily that $X_{ac}^\Sigma(M)$ must therefore be Λ -torsion.

3.3.11. Proof of Theorem 3.3.1: determining $\#\mathcal{O}/f_{ac}^\Sigma(0)$. To complete the proof of the control theorem, we use the relation between $H_{\mathcal{F}_{ac}}^1(\mathcal{K}, W)$ and $H_{\mathcal{F}_{ac}}^1(\mathcal{K}, M)^\Gamma$ to relate $\# H_{\mathcal{F}_{ac}}^1(\mathcal{K}, W)$ to $f_{ac}(0)$. The key to the comparison is the following proposition on the non-existence of pseudo-null submodules of the Λ -module $X_{ac}^\Sigma(M)$:

Proposition 3.3.12. *The Selmer module $H_{\mathcal{F}_{ac}}^1(\mathcal{K}, M)$ has no proper Λ -submodule of finite index. Equivalently, the Λ -module $X_{ac}^\Sigma(M)$ has no non-trivial pseudo-null Λ -submodule.*

Proof. Recall that $H_{\mathcal{F}_{ac}}^1(\mathcal{K}, M)_\Gamma = 0$ by Lemma 3.3.5. If $X \subset X_{ac}^\Sigma(M)$ is a Λ -submodule of finite order, then its dual X^* is a finite order quotient of $H_{\mathcal{F}_{ac}}^1(\mathcal{K}, M)$, so $X^*/(\gamma - 1)X^*$ is a quotient of $H_{\mathcal{F}_{ac}}^1(\mathcal{K}, M)_\Gamma$ and therefore 0. But X^* is a finite Λ -module and so, by Nakayama’s Lemma, $X^* = 0$ and hence $X = 0$. □

We can now establish the comparison result:

Lemma 3.3.13. *We have*

$$\#\mathcal{O}/f_{ac}^\Sigma(0) = \#\Lambda/(T, f_{ac}^\Sigma(T)) = \# H_{\mathcal{F}_{ac}}^1(\mathcal{K}, W) \cdot C^\Sigma(W).$$

Proof. Let $X = X_{ac}^\Sigma(M)$. Then $\#X_\Gamma = \# H_{\mathcal{F}_{ac}}^1(\mathcal{K}, M)^\Gamma$. Since X is Λ -torsion, X is pseudoisomorphic to a Λ -module $Y = \prod_{i=1}^r \Lambda/(f_i)$ for distinguished polynomials $f_i \neq T$ (the latter restriction being a consequence of the finiteness of X_Γ). By Proposition 3.3.12, X has no pseudo-null submodule so we obtain an exact sequence $0 \rightarrow X \rightarrow Y \rightarrow K \rightarrow 0$, where K

is a pseudo-null Λ -module. Applying the snake lemma to the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & K & \longrightarrow & 0 \\ & & \downarrow \gamma-1 & & \downarrow \gamma-1 & & \downarrow \gamma-1 & & \\ 0 & \longrightarrow & X & \longrightarrow & Y & \longrightarrow & K & \longrightarrow & 0, \end{array}$$

we obtain

$$\#X_\Gamma = \#Y_\Gamma = \prod \#\Lambda/(T, f_i(T)) = \prod \#\mathcal{O}/(f_i(0)) = \#\Lambda/(T, f_{ac}^\Sigma(T)),$$

where $f_{ac}^\Sigma(T) \sim f_1(T) \cdots f_r(T)$ is a generator of the characteristic ideal of X . Equation (3.3.e) thus implies that

$$\#\mathcal{O}/f_{ac}^\Sigma(0) = \#H_{\mathcal{F}_{ac}^\Sigma}^1(\mathcal{K}, W) = \#H_{\mathcal{F}_{ac}}^1(\mathcal{K}, W) \cdot C^\Sigma(W),$$

which proves the claim. □

This completes the proof of Theorem 3.3.1.

3.4. Comparison with Selmer groups over \mathbb{Z}_p^2 -extensions

In order to deduce what we will need from the existing theorems in Iwasawa theory, it is necessary to consider Selmer groups for Galois extensions larger than $\mathcal{K}_\infty/\mathcal{K}$. Let $\mathbb{K}_\infty/\mathcal{K}$ be the composite of all \mathbb{Z}_p -extensions of \mathcal{K} in $\overline{\mathbb{Q}}$. Let $\Gamma_\mathcal{K} = \text{Gal}(\mathbb{K}_\infty/\mathcal{K}) \cong \mathbb{Z}_p^2$. The Galois group $\text{Gal}(\mathcal{K}/\mathbb{Q})$ acts on $\Gamma_\mathcal{K}$, which decomposes under this action as $\Gamma_\mathcal{K} = \Gamma_\mathcal{K}^+ \oplus \Gamma_\mathcal{K}^-$ with the superscript \pm denoting the subgroup on which $\tau \in \text{Gal}(\mathcal{K}/\mathbb{Q})$ acts as ± 1 ; then $\Gamma_\mathcal{K}^+$ is the kernel of the natural surjection $\Gamma_\mathcal{K} \twoheadrightarrow \Gamma$. Let $\Lambda_\mathcal{K} = \mathcal{O}[[\Gamma_\mathcal{K}]]$. Let $\Psi_\mathcal{K}: G_\mathcal{K} \twoheadrightarrow \Gamma_\mathcal{K}$ be the natural surjection; this is also a continuous $\Lambda_\mathcal{K}^\times$ -valued character of $G_\mathcal{K}$. Let $\mathcal{M} = T \otimes_{\mathcal{O}} \widehat{\Lambda}_\mathcal{K}$ with $G_\mathcal{K}$ -action given by $\rho \otimes \Psi_\mathcal{K}^{-1}$. Here, $\widehat{\Lambda}_\mathcal{K} = \text{Hom}_{\text{cont}}(\Lambda_\mathcal{K}, \mathbb{Q}_p/\mathbb{Z}_p)$ is the Pontrjagin dual equipped with the structure of a $\Lambda_\mathcal{K}$ -module via $(\lambda \cdot f)(x) = f(\lambda \cdot x)$, $\forall \lambda, x \in \Lambda_\mathcal{K}$ and $f \in \widehat{\Lambda}_\mathcal{K}$, thus making $\widehat{\Lambda}_\mathcal{K}$ into a $G_\mathcal{K}$ -module. Consider the Selmer module $H_{\mathcal{F}_{Gr}^\Sigma}^1(\mathcal{K}, \mathcal{M})$ and its Pontrjagin dual $X_{Gr}^\Sigma(\mathcal{M}) = \text{Hom}_{\mathcal{O}}(H_{\mathcal{F}_{Gr}^\Sigma}^1(\mathcal{K}, \mathcal{M}), L/\mathcal{O})$ which is a finite $\Lambda_\mathcal{K}$ -module. Let $\text{char}(X_{Gr}^\Sigma(\mathcal{M})) \subset \Lambda_\mathcal{K}$ be its $\Lambda_\mathcal{K}$ -characteristic ideal. Since $\Lambda_\mathcal{K}$ is a UFD, $\text{char}(X_{Gr}^\Sigma(\mathcal{M}))$ is a principal ideal, and it is nonzero if and only if $X_{Gr}^\Sigma(\mathcal{M})$ is a torsion $\Lambda_\mathcal{K}$ -module.

Let $\gamma_\pm \in \Gamma_\mathcal{K}^\pm \cong \mathbb{Z}_p$ be fixed topological generators; we assume that $\gamma_- \mapsto \gamma$ under the projection $\Gamma_\mathcal{K} \twoheadrightarrow \Gamma$. We have $M = \mathcal{M}[\gamma_+ - 1]$ and, by

(*irred* \mathcal{K}),

$$H^1(\mathcal{K}^S/\mathcal{K}, M) \xrightarrow{\sim} H^1(\mathcal{K}^S/\mathcal{K}, \mathcal{M})[\gamma_+ - 1],$$

which induces maps

$$(3.4.a) \quad \begin{aligned} H^1_{\mathcal{F}^{\Sigma}_{ac}}(\mathcal{K}, M) &\hookrightarrow H^1_{\mathcal{F}^{\Sigma}_{Gr}}(\mathcal{K}, \mathcal{M})[\gamma_+ - 1] \quad \text{and} \\ X^{\Sigma}_{Gr}(\mathcal{M})/(\gamma_+ - 1)X^{\Sigma}_{Gr}(\mathcal{M}) &\rightarrow X^{\Sigma}_{ac}(M). \end{aligned}$$

Lemma 3.4.1. *Suppose Σ contains all the finite places $w \nmid p$ at which V is ramified. Then the maps in (3.4.a) have finite cokernel and kernel, respectively.*

Proof. The identification $M = \mathcal{M}[\gamma_+ - 1]$ yields a short exact sequence

$$\mathcal{M}^{G_{\mathcal{K}_v}}/(\gamma_+ - 1)\mathcal{M}^{G_{\mathcal{K}_v}} \hookrightarrow H^1(\mathcal{K}_v, M) \twoheadrightarrow H^1(\mathcal{K}_v, \mathcal{M})[\gamma_+ - 1].$$

Since the image of $G_{\mathcal{K}_v}$ in $\Gamma_{\mathcal{K}}$ has finite index, the argument used in the Case 3(b) of the proof of Proposition 3.3.7 to show that $M^{G_{\mathcal{K}_v}}$ has finite order can be easily adapted to prove that $\mathcal{M}^{G_{\mathcal{K}_v}}$ has finite order by replacing P_v with $\ker \Psi_K|_{G_{\mathcal{K}_v}}$. It follows that

$$\#\mathcal{M}^{G_{\mathcal{K}_v}}/(\gamma_+ - 1)\mathcal{M}^{G_{\mathcal{K}_v}} = \#\mathcal{M}^{G_{\mathcal{K}_v}}[\gamma_+ - 1] < \infty.$$

Since the cokernel of the map $H^1_{\mathcal{F}^{\Sigma}_{ac}}(\mathcal{K}, M) \hookrightarrow H^1_{\mathcal{F}^{\Sigma}_{Gr}}(\mathcal{K}, \mathcal{M})[\gamma_+ - 1]$ is a quotient of $\mathcal{M}^{G_{\mathcal{K}_v}}/(\gamma_+ - 1)\mathcal{M}^{G_{\mathcal{K}_v}}$, it is therefore finite, and so, too, is the kernel of the dual map. \square

Corollary 3.4.2. *Suppose Σ contains all the finite place $w \nmid p$ at which V is ramified. Then*

$$\text{char}(X^{\Sigma}_{ac}(M)) \subset \text{char}(X^{\Sigma}_{Gr}(\mathcal{M})) \pmod{(\gamma_+ - 1)}.$$

Proof. Let $F^{\Sigma}_{Gr}(\mathcal{M})$ be the $\Lambda_{\mathcal{K}}$ -fitting ideal of $X^{\Sigma}_{Gr}(\mathcal{M})$ and $F^{\Sigma}_{ac}(M)$ the Λ -fitting ideal of $X^{\Sigma}_{ac}(M)$. Then $F^{\Sigma}_{Gr}(\mathcal{M}) \subset \text{char}(X^{\Sigma}_{Gr}(\mathcal{M}))$. Since the kernel of the surjection map $X^{\Sigma}_{Gr}(\mathcal{M})/(\gamma_+ - 1)X^{\Sigma}_{Gr}(\mathcal{M}) \twoheadrightarrow X^{\Sigma}_{ac}(M)$ has finite order and since the source has Λ -Fitting ideal equal to $F^{\Sigma}_{Gr}(\mathcal{M})$ modulo $(\gamma_+ - 1)$, there is some $c > 0$ such that $F^{\Sigma}_{ac}(M)\mathfrak{m}_{\Lambda}^c \subset F^{\Sigma}_{Gr}(\mathcal{M}) \pmod{(\gamma_+ - 1)}$, where $\mathfrak{m}_{\Lambda} = (\gamma - 1, \mathfrak{m})$ is the maximal ideal of Λ . It follows that

$$F^{\Sigma}_{ac}(M)\mathfrak{m}_{\Lambda}^c \subset \text{char}(X^{\Sigma}_{Gr}(\mathcal{M})) \pmod{(\gamma_+ - 1)}.$$

Since the right-hand side is a principal ideal, it follows that $F^{\Sigma}_{ac}(M)$ is contained in $\text{char}(X^{\Sigma}_{Gr}(\mathcal{M})) \pmod{(\gamma_+ - 1)}$. And since $\text{char}(X^{\Sigma}_{ac}(M))$ is

the smallest principal ideal containing $F_{ac}^\Sigma(M)$, we must also have that $\text{char}(X_{ac}^\Sigma(M))$ is contained in $\text{char}(X_{Gr}^\Sigma(\mathcal{M})) \pmod{(\gamma_+ - 1)}$. \square

3.5. Applications to newforms and modular abelian varieties A_f

We return to the notation of Section 2.4. Let $f \in S_{2k}(\Gamma_0(N))$ be a newform, and let (V_f, T_f, W_f) be as in Section 2.4.4.

Let

$$(V, T, W) = (V_f(1 - k), T_f(1 - k), W_f(1 - k)).$$

Note that $V^* \cong V$. It is a theorem of Saito [43], building on work of Deligne, Langlands, Carayol, and others, that V is geometric and pure of weight -1 . So (geom), (pure), (τ -dual), and (2-dim) all hold for V . Furthermore, it follows that if

$$(p\text{-sst}) \quad \text{ord}_p(N) \leq 1,$$

then V is semistable at p , that is, (sst) also holds. As the Hodge-Tate weights of V are $k - 1$ and $-k$, (HT) holds if and only if neither k nor $k - 1$ (when $k \neq 1$) are divisible by $p - 1$; in particular, (HT) always holds for $2k = 2$.

Suppose now that f has weight 2 and that

$$(V, T, W) = (V_f, T_f, W_f) = (V_{\mathfrak{p}}A_f, T_{\mathfrak{p}}A_f, A_f[\mathfrak{p}^\infty])$$

as in Section 2.4.3. The Mordell-Weil group $A_f(F)$ is a $\mathbb{Z}(f)$ -module and

$$\text{rank}_{\mathbb{Z}}A_f(F) = [\mathbb{Q}(f) : \mathbb{Q}] \cdot \text{rank}_{\mathcal{O}}(A_f(F) \otimes_{\mathbb{Z}(f)} \mathcal{O}).$$

Suppose

$$(\text{rank } 1) \quad \text{rank}_{\mathcal{O}}(A_f(\mathcal{K}) \otimes_{\mathbb{Z}(f)} \mathcal{O}) = 1$$

or, equivalently, $\text{rank}_{\mathbb{Z}}A_f(\mathcal{K}) = [\mathbb{Q}(f) : \mathbb{Q}]$. The Tate-Shafarevich group $\text{III}(A_f/\mathcal{K})$ is also a $\mathbb{Z}(f)$ -module and satisfies $\text{III}(A_f/\mathcal{K})[\mathfrak{p}^\infty] \otimes_{\mathbb{Z}(f)} \mathcal{O} = \text{III}(A_f/\mathcal{K})[\mathfrak{p}^\infty]$. Suppose

$$(\text{III } \mathfrak{p}\text{-finite}) \quad \#\text{III}(A_f/\mathcal{K})[\mathfrak{p}^\infty] < \infty.$$

Note that in this case $\text{III}_{BK}(W_f/\mathcal{K}) = \text{III}(A_f/\mathcal{K})[\mathfrak{p}^\infty]$. Under the assumptions (rank 1) and (III \mathfrak{p} -finite), it follows from the exact sequence

$$(\text{FES}) \quad A_f(\mathcal{K}) \otimes_{\mathbb{Z}(f)} L/\mathcal{O} \hookrightarrow \text{Sel}_{\mathfrak{p}^\infty}(A_f/\mathcal{K}) \twoheadrightarrow \text{III}(A_f/\mathcal{K})[\mathfrak{p}^\infty],$$

that (corank 1) holds for $H_{\mathcal{F}_{\text{BK}}}^1(\mathcal{K}, W_f) = \text{Sel}_{p^\infty}(A_f/\mathcal{K})$ (the equality of the two Selmer groups is explained in detail in [5, §3, §5]). If furthermore

(p-irred) $A_f[\mathfrak{p}]$ is an irreducible $G_{\mathcal{K}}$ -representation,

then

$$A_f(\mathcal{K}) \otimes_{\mathbb{Z}(f)} \mathcal{O} \xrightarrow{\sim} H_f^1(\mathcal{K}, T) \cong \mathcal{O}.$$

If $w \mid p$ is a place of \mathcal{K} then $A_f(\mathcal{K}_w)$ is a finitely generated \mathbb{Z}_p -module of rank equal to $[\mathcal{K}_w : \mathbb{Q}_p] \cdot [\mathbb{Z}(f) : \mathbb{Z}]$ (there is a natural $\mathbb{Z}(f)$ -injection of $\mathbb{Z}(f) \otimes \mathcal{O}_{\mathcal{K}_w}$ into the compact Lie group $A_f(\mathcal{K}_w)$, with image having finite index; this is just the exp map from a neighborhood of zero in the tangent space at the origin). In particular, if p splits in \mathcal{K} (so $\mathbb{Q}_p \xrightarrow{\sim} \mathcal{K}_w$), we have that $A_f(\mathcal{K}_w) \otimes_{\mathbb{Z}(f)} L/\mathcal{O} \cong L/\mathcal{O}$. Furthermore, since $A_f(\mathcal{K}) \subset A_f(\mathcal{K}_w)$, if (rank 1) holds, then we also have that

$$A(\mathcal{K}) \otimes_{\mathbb{Z}(f)} L/\mathcal{O} \cong L/\mathcal{O} \twoheadrightarrow A(\mathcal{K}_w) \otimes_{\mathbb{Z}(f)} L/\mathcal{O} \cong L/\mathcal{O}.$$

That is, (sur) also holds. This shows that if (split), (rank 1), (III p-finite), and (p-irred) hold, then so do (corank 1), (sur), and (irred $_{\mathcal{K}}$).

Still assuming that p splits in \mathcal{K} , we also have $A_f(\mathcal{K}_v) \otimes_{\mathbb{Z}(f) \otimes \mathbb{Z}_p} \mathcal{O} \xrightarrow{\sim} H_f^1(\mathcal{K}_v, T)$ is a finite \mathcal{O} -module of rank one. Let $A_f(\mathcal{K}_v)_{/\text{tor}} = A_f(\mathcal{K}_v)/A_f(\mathcal{K}_v)_{\text{tor}}$ (this is then a free $\mathbb{Z}(f) \otimes \mathbb{Z}_p$ -module), so $A_f(\mathcal{K}_v)_{/\text{tor}} \otimes_{\mathbb{Z}(f) \otimes \mathbb{Z}_p} \mathcal{O} \xrightarrow{\sim} H_f^1(\mathcal{K}_v, T)/H^1(\mathcal{K}_v, T)_{\text{tor}}$. Then

$$(3.5.a) \quad \begin{aligned} \#\delta_v &= \#\text{coker}\{H_f^1(\mathcal{K}, T) \xrightarrow{\text{loc}_v} H_f^1(\mathcal{K}_v, T)/H^1(\mathcal{K}_v, T)_{\text{tor}}\} \\ &= \#[A_f(\mathcal{K}_v)_{/\text{tor}} \otimes_{\mathbb{Z}(f) \otimes \mathbb{Z}_p} \mathcal{O} : A_f(\mathcal{K}) \otimes_{\mathbb{Z}(f)} \mathcal{O}]. \end{aligned}$$

Let $P \in A_f(\mathcal{K})$ be any point of infinite order. The \mathcal{O} -module $\mathcal{O} \cdot P \subset A_f(\mathcal{K}) \otimes_{\mathbb{Z}(f)} \mathcal{O}$ generated by P has finite index, and it follows that

$$\#\delta_v = \frac{[A_f(\mathcal{K}_v)_{/\text{tor}} \otimes_{\mathbb{Z}(f) \otimes \mathbb{Z}_p} \mathcal{O} : \mathcal{O} \cdot P]}{[A_f(\mathcal{K}) \otimes_{\mathbb{Z}(f)} \mathcal{O} : \mathcal{O} \cdot P]}.$$

In particular, it then follows from Proposition 3.2.1 that

$$(3.5.b) \quad \#H_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}, W_f) = \#\text{III}_{\text{BK}}(W_f/\mathcal{K}) \cdot \frac{[A_f(\mathcal{K}_v)_{/\text{tor}} \otimes_{\mathbb{Z}(f) \otimes \mathbb{Z}_p} \mathcal{O} : \mathcal{O} \cdot P]^2}{[A_f(\mathcal{K}) \otimes_{\mathbb{Z}(f)} \mathcal{O} : \mathcal{O} \cdot P]^2}.$$

Suppose now that

(good) $p \nmid N$.

Then A_f has good reduction at p and so extends to an abelian scheme over $\mathbb{Z}_{(p)}$. Let $A_f^1(\mathbb{Q}_p) \subset A_f(\mathbb{Q}_p)$ be the kernel of reduction modulo p . Let $\Omega^1(A_f/\mathbb{Z}_p)^\vee = \text{Hom}_{\mathbb{Z}_p}(\Omega^1(A_f/\mathbb{Z}_p), \mathbb{Z}_p)$. The formal group logarithm defines a $\mathbb{Z}(f) \otimes_{\mathbb{Z}_p}$ -isomorphism $\log : A_f^1(\mathbb{Q}_p) \rightarrow p\Omega^1(A_f/\mathbb{Z}_p)^\vee$, which extends to an injective $\mathbb{Z}(f) \otimes_{\mathbb{Z}_p}$ -homomorphism $\log : A_f(\mathbb{Q}_p)_{/\text{tor}} \hookrightarrow \Omega^1(A_f/\mathbb{Z}_p)^\vee$. Recall that $\mathcal{O} = \mathbb{Z}(f)_{\mathfrak{p}}$ for a chosen prime $\mathfrak{p} \mid p$ of $\mathbb{Z}(f)$. Let $\omega_f \in \Omega^1(A_f/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathcal{O}$ be an \mathcal{O} -basis element such that the action of each $\alpha \in \mathbb{Z}(f)$ on A_f induces $\alpha^*\omega_f = \alpha \cdot \omega_f$ (multiplication by the scalar $\alpha \in \mathcal{O}$). Then composition of \log with evaluation on ω_f defines an \mathcal{O} -homomorphism

$$\log_{\omega_f} : A_f(\mathbb{Q}_p)_{/\text{tor}} \otimes_{\mathbb{Z}_p} \mathcal{O} \rightarrow \mathcal{O}$$

that maps $A_f^1(\mathbb{Q}_p) \otimes_{\mathbb{Z}_p} \mathcal{O}$ surjectively onto $p\mathcal{O}$. By the choice of ω_f , the map \log_{ω_f} factors through $A_f(\mathbb{Q}_p)_{/\text{tor}} \otimes_{\mathbb{Z}(f) \otimes_{\mathbb{Z}_p}} \mathcal{O}$. The induced homomorphism $A_f(\mathbb{Q}_p)_{/\text{tor}} \otimes_{\mathbb{Z}(f) \otimes_{\mathbb{Z}_p}} \mathcal{O} \hookrightarrow \mathcal{O}$ is injective and maps $A_f^1(\mathbb{Q}_p) \otimes_{\mathbb{Z}(f) \otimes_{\mathbb{Z}_p}} \mathcal{O}$ isomorphically onto $p\mathcal{O}$; this follows from $A_f(\mathbb{Q}_p)_{/\text{tor}} \otimes_{\mathbb{Z}(f) \otimes_{\mathbb{Z}_p}} \mathcal{O}$ and $A_f^1(\mathbb{Q}_p) \otimes_{\mathbb{Z}(f) \otimes_{\mathbb{Z}_p}} \mathcal{O}$ both being free \mathcal{O} -modules of rank one and the surjective mapping of the latter onto $p\mathcal{O}$. As $\mathcal{K}_v = \mathbb{Q}_p$ (since p splits in \mathcal{K}) it easily follows from this that

$$\begin{aligned} & [A_f(\mathcal{K}_v)_{/\text{tor}} \otimes_{\mathbb{Z}(f) \otimes_{\mathbb{Z}_p}} \mathcal{O} : \mathcal{O} \cdot P] \\ &= \frac{\#\mathcal{O}/(\log_{\omega_f} P)}{\#\mathcal{O}/(\log_{\omega_f}(A_f(\mathbb{Q}_p)_{/\text{tor}} \otimes_{\mathbb{Z}_p} \mathcal{O}))} \\ &= \frac{\#\mathcal{O}/(\log_{\omega_f} P) \cdot \#(A_f(\mathbb{Q}_p)_{/\text{tor}}/A_f^1(\mathbb{Q}_p) \otimes_{\mathbb{Z}(f) \otimes_{\mathbb{Z}_p}} \mathcal{O})}{\#\mathcal{O}/p\mathcal{O}} \\ &= \frac{\#\mathcal{O}/(\log_{\omega_f} P) \cdot \#(A_f(\mathbb{Q}_p)/A_f^1(\mathbb{Q}_p) \otimes_{\mathbb{Z}(f)} \mathcal{O})}{\#\mathcal{O}/p\mathcal{O} \cdot \#(A_f(\mathbb{Q}_p)_{\text{tor}} \otimes_{\mathbb{Z}(f)} \mathcal{O})}. \end{aligned}$$

Since reduction modulo p yields an isomorphism $A_f(\mathbb{Q}_p)/A_f^1(\mathbb{Q}_p) \xrightarrow{\sim} A_f(\mathbb{F}_p)$, we have $A_f(\mathbb{Q}_p)/A_f^1(\mathbb{Q}_p) \otimes_{\mathbb{Z}(f)} \mathcal{O} \xrightarrow{\sim} A_f(\mathbb{F}_p) \otimes_{\mathbb{Z}(f)} \mathcal{O} = A_f[\mathfrak{p}^\infty](\mathbb{F}_p)$. The latter group is trivial unless f is ordinary with respect to \mathfrak{p} (that is, $\mathfrak{p} \nmid a_p$) in which case it is isomorphic to $\mathcal{O}/(1 - a_p + p)$. Hence

$$\#A_f(\mathbb{Q}_p)/A_f^1(\mathbb{Q}_p) \otimes_{\mathbb{Z}(f)} \mathcal{O} = \#\mathcal{O}/(1 - a_p + p).$$

Also, $A_f(\mathbb{Q}_p)_{\text{tor}} \otimes_{\mathbb{Z}_p} = H^0(\mathbb{Q}_p, A_f[p^\infty])$ so $A_f(\mathbb{Q}_p) \otimes_{\mathbb{Z}(f) \otimes_{\mathbb{Z}_p}} \mathcal{O} = H^0(\mathbb{Q}_p, W_f)$, hence

$$\#A_f(\mathbb{Q}_p)_{\text{tor}} \otimes_{\mathbb{Z}_p} = \#H^0(\mathbb{Q}_p, W_f),$$

Putting this together with the preceding formula for $[A_f(\mathcal{K}_v)_{/\text{tor}} \otimes_{\mathbb{Z}(f) \otimes \mathbb{Z}_p} \mathcal{O} : \mathcal{O} \cdot P]$ we find

$$\begin{aligned}
 [A_f(\mathcal{K}_v)_{/\text{tor}} \otimes_{\mathbb{Z}(f) \otimes \mathbb{Z}_p} \mathcal{O} : \mathcal{O} \cdot P] &= \frac{\#\mathcal{O}/(\log_{\omega_f} P) \cdot \#\mathcal{O}/(1 - a_p + p)}{\#\mathcal{O}/p\mathcal{O} \cdot \#\mathrm{H}^0(\mathcal{K}_v, W_f)} \\
 &= \frac{\#\mathcal{O}/((\frac{1-a_p+p}{p}) \log_{\omega_f} P)}{\#\mathrm{H}^0(\mathcal{K}_v, W_f)}.
 \end{aligned}$$

Combining this last equality with (3.5.a) we get

$$\#\delta_v = \frac{\#\mathcal{O}/((\frac{1-a_p+p}{p}) \log_{\omega_f} P)}{[A_f(\mathcal{K}) \otimes_{\mathbb{Z}(f)} \mathcal{O} : \mathcal{O} \cdot P] \cdot \#\mathrm{H}^0(\mathcal{K}_v, W_f)},$$

which, when substituted into (3.5.b), yields

$$\begin{aligned}
 (3.5.c) \quad \#\mathrm{H}_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}, W_f) &= \#\mathrm{III}_{\text{BK}}(W_f/\mathcal{K}) \cdot \left(\frac{\#\mathcal{O}/((\frac{1-a_p+p}{p}) \log_{\omega_f} P)}{[A_f(\mathcal{K}) \otimes_{\mathbb{Z}(f)} \mathcal{O} : \mathcal{O} \cdot P] \cdot \#\mathrm{H}^0(\mathcal{K}_v, W_f)} \right)^2
 \end{aligned}$$

In the special case that $A_f = E$ is an elliptic curve (i.e., f has rational coefficients), p is a prime of good reduction, $\mathcal{O} = \mathbb{Z}_p$, and $P \in E(\mathcal{K})$ has infinite order, we can rewrite the formula for $\#\delta_v$ as

$$\#\delta_v = \frac{\#\mathbb{Z}_p/((\frac{1-a_p(E)+p}{p}) \log_{\omega_E} P)}{[E(\mathcal{K}) : \mathbb{Z} \cdot P]_p \cdot \#\mathrm{H}^0(\mathcal{K}_v, E[p^\infty])},$$

where $[-, -]_p$ denotes the p -part of the index and we have taken for ω_f the Néron differential $\omega_E \in \Omega^1(E/\mathbb{Z}_{(p)})$. In this case (3.5.c) then becomes

$$(3.5.d) \quad \#\mathrm{H}_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}, E[p^\infty]) = \#\mathrm{III}(E/\mathcal{K})[p^\infty] \cdot \left(\frac{\#\mathbb{Z}_p/((\frac{1-a_p(E)+p}{p}) \log_{\omega_E} P)}{[E(\mathcal{K}) : \mathbb{Z} \cdot P]_p \cdot \#\mathrm{H}^0(\mathcal{K}_v, E[p^\infty])} \right)^2.$$

4. CM points, CM periods and upper bounds on III

In this section we recall the definition of Heegner points on certain Shimura curves and their Jacobians. The Shimura curves considered are moduli spaces for false elliptic curves and the Heegner points correspond to false elliptic

curves with complex multiplication. These Heegner points give rise to cohomology classes for the Tate module of an optimal quotient of the Jacobian of the Shimura curve. The Euler system method of Kolyvagin yields an upper bound on the order of the Tate–Shafarevich group of this optimal quotient in terms of the indices of certain of these classes. This upper bound is recalled in [26]. It is an essential ingredient in our proof of the main theorem of this paper. For use in comparing p -adic L -functions in Section 5, we also explain how the complex and p -adic periods of false CM elliptic curves are identified with complex and p -adic periods of (true) CM elliptic curves.

Let \mathcal{K} be an imaginary quadratic field such that (split) holds. Let $-D_{\mathcal{K}} < 0$ be the discriminant of \mathcal{K} .

4.1. The Heegner hypothesis

Let N be an integer. We will also assume that N satisfies at least one of the two Heegner-type hypotheses recalled below. The first of these is:

- (H)
 - $N = N^+N^-$ with $(N^+, N^-) = 1$;
 - $\ell \mid N^+$ if and only if ℓ splits in \mathcal{K} ;
 - $\ell \mid N^-$ if and only if ℓ is inert in \mathcal{K} ;
 - N^- is squarefree with an even number of prime factors.

Implicit in these assumptions is that the discriminant $-D_{\mathcal{K}} < 0$ of \mathcal{K} satisfies

(coprime) $(N, D_{\mathcal{K}}) = 1.$

If $N^- = 1$, then (H) is just the usual Heegner hypothesis. For some of the arguments that follow, we also need a more general Heegner-type hypothesis:

- (gen-H)
 - $N = N^+N^-$ with $(N^+, N^-) = 1$;
 - $\ell \mid N^+$ if and only if ℓ is split or ramified in \mathcal{K} ;
 - $\ell \mid N^-$ if and only if ℓ is inert in \mathcal{K} ;
 - N^- is squarefree with an even number of prime factors.

Note that the only difference between the hypotheses (H) and (gen-H) is in the latter the primes dividing N^+ are allowed to be ramified in \mathcal{K} (so (coprime) may not hold).

Let $f \in S_{2k}(\Gamma_0(N))$ be a newform and π the associated cuspidal representation of $\mathrm{GL}_2(\mathbb{A})$ as in Section 2.4.2. According to [57, §6] (see also [19, §5] and [57, p.81]), the third and fourth assumption of either Heegner-type

hypothesis implies that the epsilon factor $\epsilon(\pi, \mathcal{K}, s)$ of the base change of π to $\mathrm{GL}_2(\mathbb{A}_{\mathcal{K}})$ satisfies

$$(\text{sign } -1) \quad \epsilon(\pi, \mathcal{K}, 1/2) = -1.$$

4.2. The quaternion algebra B and the Shimura curve X_{N^+, N^-}

Suppose N satisfies (gen-H). Let B be the indefinite quaternion algebra of discriminant N^- . Let \mathcal{O}_B be a maximal order of B and let $R \subset \mathcal{O}_B$ be an Eichler order of level N^+ . Fix an isomorphism of \mathbb{R} -algebras

$$(4.2.a) \quad B \otimes \mathbb{R} \xrightarrow{\sim} M_2(\mathbb{R})$$

and an isomorphism of $\mathbb{A}^{\infty N^-}$ -algebras

$$(4.2.b) \quad B \otimes \mathbb{A}^{\infty N^-} \xrightarrow{\sim} M_2(\mathbb{A}^{\infty N^-})$$

that identifies $R \otimes \widehat{\mathbb{Z}}^{N^-}$ with the order $\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\widehat{\mathbb{Z}}^{N^-}) : N^+ \mid c \}$. Here, as usual, $\mathbb{A}^{\infty N^-}$ (resp. $\widehat{\mathbb{Z}}^{N^-}$) denotes the restricted product of \mathbb{Q}_{ℓ} (resp. the product of \mathbb{Z}_{ℓ}) for $\ell \nmid \infty N^-$.

In order to compare later statements with results in [7], we assume (without loss of generality) that the isomorphism (4.2.a) and the fixed isomorphisms $R \otimes \mathbb{Z}_{\ell} \cong M_2(\mathbb{Z}_{\ell})$ for $\ell \mid N^+ p$ all arise from the choice of a real quadratic field $\mathcal{M} = \mathbb{Q}(\sqrt{p_0}) \subset B$, $p_0 \nmid pND_{\mathcal{K}}$, in which the primes $\ell \mid pN^+$ split and from an identification

$$\iota_{\mathcal{M}} : B \otimes \mathcal{M} \xrightarrow{\sim} M_2(\mathcal{M}).$$

In particular, the chosen isomorphisms are induced from $\iota_{\mathcal{M}}$ by fixing an inclusion $\mathcal{M} \hookrightarrow \mathbb{R}$ and a prime of \mathcal{M} above each $\ell \mid pN^+$. Furthermore, we fix an idempotent $e \in \mathcal{O}_B \otimes \mathcal{O}_{\mathcal{M}}[\frac{1}{2p_0}]$ as in [7, p.7] such that

$$\iota_{\mathcal{M}}(e) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

Let G be the algebraic group over \mathbb{Q} such that $G(S) = (B \otimes S)^{\times}$ for each \mathbb{Q} -algebra S . Using the identification (4.2.a) we define a homomorphism,

$$h_0 : \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(\mathbb{G}_m) \rightarrow G_{/\mathbb{R}}, \quad x + iy \mapsto \begin{pmatrix} x & y \\ -y & x \end{pmatrix},$$

and let X be the $G(\mathbb{R})$ -conjugacy class of h_0 . The set X has a natural complex structure and the map $X \xrightarrow{\sim} \mathfrak{h}^{\pm} := \mathbb{C} - \mathbb{R}$, $\mathrm{Ad}(g)h_0 \mapsto g(i)$, is a

$G(\mathbb{R})$ -equivariant holomorphic isomorphism. The action of $G(\mathbb{R})$ on \mathfrak{h}^\pm is via (4.2.a) and the usual action of $GL_2(\mathbb{R})$.

Let X_{N^+,N^-} be the Shimura curve associated with the Shimura datum (G, X) and the open compact subgroup $K = (R \otimes \widehat{\mathbb{Z}})^\times \subset \widehat{B}^\times = (B \otimes \mathbb{A}^\infty)^\times = G(\mathbb{A}^\infty)$. This curve has a canonical model over \mathbb{Q} with complex uniformization

$$(4.2.c) \quad X_{N^+,N^-}(\mathbb{C}) = B^\times \backslash (X \times \widehat{B}^\times / K)$$

It even has the structure of a coarse moduli space [27], [9], [21]; the solution of the moduli problem yields a smooth regular model over $\mathbb{Z}[1/N^-]$ which, in particular, is smooth at p if

$$(good) \quad p \nmid N$$

holds.

To describe the moduli problem represented by X_{N^+,N^-} we recall that a *false elliptic curve* over a scheme S is a pair (A, ι) with A an abelian surface over S and $\iota : \mathcal{O}_B \hookrightarrow \text{End}_S(A)$ an injective homomorphism. A full level- N^+ structure on (A, i) is an isomorphism of group schemes $t : A[N^+] \xrightarrow{\sim} \mathcal{O}_B \otimes (\mathbb{Z}/N\mathbb{Z})_S$ commuting with the \mathcal{O}_B -action on both sides, and a K -level structure is a K -equivalence class of such full level N^+ structures. Then X_{N^+,N^-} represents the coarse moduli scheme over $\mathbb{Z}[1/N]$ for the moduli problem classifying isomorphism classes of triples (A, ι, t) where (A, ι) is a false elliptic curve over S and t is a K -level structure⁶. In terms of the complex uniformization, $[h, 1]$, $h \in X$, represents the isomorphism class of the triple $(A_h, \iota_{can}, t_{can})$, where

- $A_h = (\mathcal{O}_B \otimes \mathbb{R}) / \mathcal{O}_B$, where the complex structure on $\mathcal{O}_B \otimes \mathbb{R}$ is defined by right multiplication by $h(z)$, $z \in \mathbb{C}$;
- ι_{can} is the action of \mathcal{O}_B arising from left multiplication;
- t_{can} is the K -equivalence class of the canonical isomorphism $A_h[N^+] = \frac{1}{N^+} \mathcal{O}_B / \mathcal{O}_B$.

⁶When $N^- = 1$ (so $B = M_2(\mathbb{Q})$ and $G = GL_2$) the usual moduli interpretation of the modular curve $X_{1,N} = X_0(N)$ classifies elliptic curves E together with a $\Gamma_0(N)$ -equivalence class of isomorphisms $\alpha : E[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})_S^2$. The two moduli problems are isomorphic, with the class of (E, α) being identified with the class of $A = E \times E$ together with the obvious action of $\mathcal{O}_B = M_2(\mathbb{Z})$ and the K -level structure $\alpha \times \alpha$.

When $N^- = 1$ (so $B = M_2(\mathbb{Q})$) X_{N^+,N^-} is not proper, but a proper model X_{N^+,N^-}^* is obtained by adding cusps; this extends to a regular model over $\mathbb{Z}_{(p)}$, which is still smooth if (good) holds. If $N^- \neq 1$, then X_{N^+,N^-} is already proper, but to unify notation we also write X_{N^+,N^-}^* for X_{N^+,N^-} in this case.

Let $\ell_0 \nmid Npp_0$ be a prime (to be chosen later). Associated with ℓ_0 is the Hecke correspondence T_{ℓ_0} for X_{N^+,N^-}^* . The degree of this correspondence is $\ell_0 + 1$, so for any $x \in X_{N^+,N^-}^*$ the divisor

$$(T_{\ell_0} - \ell_0 - 1)[x] \in \text{Div}^0(X_{N^+,N^-}^*)$$

has degree 0.

Let $J(X_{N^+,N^-}^*)/\mathbb{Q}$ be the Jacobian of X_{N^+,N^-}^* . We define a finite morphism

$$(4.2.d) \quad \iota_{N^+,N^-} : X_{N^+,N^-}^* \rightarrow J(X_{N^+,N^-}^*), \quad x \mapsto (T_{\ell_0} - \ell_0 - 1)[x].$$

Remark 4.2.1. To compare with formulas in [10] (and ultimately with those in [55]), we also consider a different embedding. Let $\delta_{N^+,N^-} \in \text{Pic}(X_{N^+,N^-}^*)$ be defined as follows. If $N^- = 1$, then let m be an integer that annihilates the cuspidal subgroup of $\text{Pic}^0(X_{N^+,N^-}^*)$ (which is finite by the theorem of Manin-Drinfeld) and $\delta_{N^+,N^-} = m[\infty]$, where $[\infty]$ is the divisor of the cusp at infinity. If $N^- \neq 1$, then let $\delta_{N^+,N^-} = \xi(\widetilde{X_{N^+,N^-}^*})$ be the Hodge class defined in [57, §6.2] and let $m \geq 1$ be its degree. In all cases, the action of any Hecke correspondences on δ_{N^+,N^-} is just multiplication by the degree of the correspondence (in particular, the action is Eisenstein). We define a finite morphism (over \mathbb{Q}):

$$(4.2.e) \quad \tilde{\iota}_{N^+,N^-} : X_{N^+,N^-}^* \rightarrow J(X_{N^+,N^-}^*), \quad x \mapsto m[x] - \delta_{N^+,N^-}.$$

As δ_{N^+,N^-} is Eisenstein we then have

$$(4.2.f) \quad (T_{\ell_0} - \ell_0 - 1) \cdot \tilde{\iota}_{N^+,N^-}(x) = m \cdot \iota_{N^+,N^-}(x).$$

4.3. CM points on X_{N^+,N^-}^*

A reference for this section is [37, §1]. Let $\iota_{\mathcal{K}} : \mathcal{K} \hookrightarrow B$ be an optimal embedding with respect to R , in the sense that $\iota_{\mathcal{K}}(\mathcal{K}) \cap R = \mathcal{O}_{\mathcal{K}}$. Each of the hypotheses (H) and (gen-H) ensures that such an embedding exists.

There exists a unique point $h \in X$ such that $h \in \mathfrak{h}^+$ and $\iota_{\mathcal{K}}(\mathcal{K}^\times)$ fixes h . Moreover, the subgroup of B^\times fixing h is just $\iota_{\mathcal{K}}(\mathcal{K}^\times)$. Replacing the choice of

$\iota_{\mathcal{K}}$ with $\iota_{\mathcal{K} \circ \tau}$ if necessary (this does not change the point h), we may assume that the homomorphism $h: \mathbb{C} \rightarrow G(\mathbb{R})$ is such that $h(i) = \iota_{\mathcal{K}}(\sqrt{-D_{\mathcal{K}}}) \otimes \frac{1}{\sqrt{D_{\mathcal{K}}}}$ and that the action of $\iota_{\mathcal{K}}(k)$, $k \in \mathcal{K}^{\times}$, on $\begin{bmatrix} h \\ 1 \end{bmatrix}$ is just multiplication by k .

The set of CM points of X_{N^+, N^-}^* is, in terms of the complex uniformization (4.2.c),

$$\text{CM}(X_{N^+, N^-}^*) = \{[h, b] \in X_{N^+, N^-}(\mathbb{C}) : b \in \widehat{B}^{\times}\}.$$

This set does not depend on $\iota_{\mathcal{K}}$ since any two embeddings $\mathcal{K} \hookrightarrow B$ are B^{\times} -conjugate. In addition, the fixed optimal embedding $\iota_{\mathcal{K}}$ induces a bijection

$$(4.3.a) \quad \text{CM}(X_{N^+, N^-}^*) \simeq \mathcal{K}^{\times} \backslash G(\mathbb{A}^{\infty}) / \widehat{R}^{\times}.$$

Shimura’s reciprocity law shows that $\text{CM}(X_{N^+, N^-}^*) \subset X_{N^+, N^-}^*(\mathcal{K}^{ab})$ and that the action of $\text{Gal}(\mathcal{K}^{ab}/\mathcal{K})$ is described in terms of the reciprocity map $\mathcal{K}^{\times} \backslash \mathbb{A}_{\mathcal{K}, f}^{\times} \xrightarrow{\text{rec}_{\mathcal{K}}} \text{Gal}(\mathcal{K}^{ab}/\mathcal{K})$ by

$$\text{rec}_{\mathcal{K}}(t)[h, b] = [h, \iota_{\mathcal{K}}(t)b].$$

In particular, since $\iota_{\mathcal{K}}$ is an optimal embedding, the point $x = [h, 1]$ is defined over the Hilbert class field H of \mathcal{K} . Let

$$x_{\mathcal{K}}^{N^+, N^-} = \sum_{\sigma \in \text{Gal}(H/\mathcal{K})} \iota_{N^+, N^-}(x)^{\sigma} \in J(X_{N^+, N^-}^*)(\mathcal{K}).$$

Note that $x_{\mathcal{K}}^{N^+, N^-}$ depends on the auxiliary prime ℓ_0 (to be chosen later).

Let $f \in S_2(\Gamma_0(N))$ be a newform. Then the modular abelian variety A_f is a quotient of $J(X_{N^+, N^-}^*)$. Let $\pi: J(X_{N^+, N^-}^*) \rightarrow A_f$ be such a quotient map (in later applications we will choose a π with nice properties at p). We then obtain a Heegner point

$$y_{\mathcal{K}}^{N^+, N^-} = \pi(x_{\mathcal{K}}^{N^+, N^-}) \in A_f(K).$$

Let \mathfrak{p} be a prime of $\mathbb{Z}(f)$ containing p . Suppose that

$$(\ell_0\text{-good}) \quad \mathfrak{p} \nmid (a_{\ell_0}(f) - \ell_0 - 1).$$

Then

$$z_{\mathcal{K}}^{N^+, N^-} = \frac{1}{a_{\ell_0}(f) - \ell_0 - 1} y_{\mathcal{K}}^{N^+, N^-} \in A_f(\mathcal{K}) \otimes_{\mathbb{Z}(f)} \mathbb{Z}(f)_{\mathfrak{p}}$$

is independent of the choice of ℓ_0 .

Remark 4.3.1. If (irred \mathcal{K}) holds for the residual representation modulo the prime \mathfrak{p} , then there is a positive proportion of primes $\ell_0 \nmid Npp_0$ for which (ℓ_0 -good) holds.

4.4. Upper bounds on $\#\text{III}(E/\mathcal{K})[p^\infty]$

Suppose now that $A_f = E$ is an elliptic curve (equivalently, that $\mathbb{Q}(f) = \mathbb{Q}$). Here, we recall a consequence of Kolyvagin’s theorem on the structure of $\text{III}(E/\mathcal{K})[p^\infty]$ extended to the case of elliptic curve quotients of Jacobians of Shimura curves. The following result is a direct consequence of [37, Thm.3.2]:

Theorem 4.4.1. *Suppose that $E[p]$ is an irreducible $G_{\mathbb{Q}}$ -representation. Suppose that hypothesis (H) holds for the imaginary quadratic field \mathcal{K} and the conductor N of E . Then*

$$(4.4.a) \quad \#\text{III}(E/\mathcal{K})[p^\infty] \leq p^{2m_0^{N^+,N^-}},$$

where $m_0^{N^+,N^-} = \text{ord}_p[E(\mathcal{K}) \otimes_{\mathbb{Z}} \mathbb{Z}_p : \mathbb{Z}z_{\mathcal{K}}^{N^+,N^-}]$.

Remark 4.4.2. In fact, one can deduce from the work of [31] (see also [34]) and its generalizations to Shimura curves by Nekovář [37] a more precise result:

$$(4.4.b) \quad \#\text{III}(E/\mathcal{K})[p^\infty] = p^{2(m_0^{N^+,N^-} - m_\infty^{N^+,N^-})},$$

where $m_\infty^{N^+,N^-}$ is the maximal non-negative integer m such that p^m divides all the cohomology classes constructed by Kolyvagin (see [26] for more details in the case of modular curves).

4.5. Comparisons of CM periods

In the following we recall the complex and p -adic periods of CM elliptic curves and explain how they can be identified with periods of ‘false’ CM elliptic curves.

4.5.1. Complex and p -adic periods of CM elliptic curves. Suppose that p splits in \mathcal{K} . Let H/\mathcal{K} be the Hilbert class field of \mathcal{K} and let F be a finite extension of H and let E_0/F be an elliptic curve with complex multiplication (CM) by an order \mathfrak{D} in the imaginary quadratic field \mathcal{K} . We assume that $\mathfrak{D} \otimes_{\mathbb{Z}(p)} \mathbb{Z}(p)$ is a maximal $\mathbb{Z}(p)$ -order. Fix a complex uniformization $E_0(\mathbb{C}) \cong \mathbb{C}/\mathfrak{a}$, where \mathfrak{a} is a non-zero ideal of $\mathfrak{D} = \text{End}(E_0)$. By enlarging F if necessary

we may assume that E_0 has good reduction at all primes above p and so extends to an elliptic scheme $\mathcal{E}_0/\mathcal{O}_{F,(p)}$. We are interested in $\Omega^1(\mathcal{E}_0/\mathcal{O}_{F,(p)})$, which is a free $\mathcal{O}_{F,(p)}$ -module of rank one. Write $\Omega^1(\mathcal{E}_0/\mathcal{O}_{F,(p)}) = \mathcal{O}_{F,(p)} \cdot \omega_{E_0}$ for some differential $\omega_{E_0} \in \Omega^1(\mathcal{E}_0/\mathcal{O}_{F,(p)})$.

We define the complex period of E_0 as follows. We consider \mathbb{C} to be an F -algebra via the fixed inclusion $\iota_\infty : \overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Then

$$\Omega^1(\mathcal{E}_0/\mathcal{O}_{F,(p)}) \otimes_{\mathcal{O}_{F,(p)}} \mathbb{C} = \Omega^1(E_0/\mathbb{C}).$$

As the invariant differential $\omega_{\mathbb{C}} = dz$ on the complex torus $E_0(\mathbb{C}) \cong \mathbb{C}/\mathfrak{a}$ gives a generator for $\Omega^1(E_0/\mathbb{C})$, there exists a scalar $\Omega_\infty \in \mathbb{C}^\times$ such that $\omega_{E_0} = \Omega_\infty \cdot (2\pi i) \cdot \omega_{\mathbb{C}}$. This agrees with the definition of the complex period of the CM elliptic curve that is given in, e.g., [3, p.1132].

We define the p -adic period of E_0 in much the same way, following [3, p.1134]. Recall that $p = v\bar{v}$ splits in \mathcal{K} . We take the place v to be that determined by the fixed embedding $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ and $\iota_v : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathcal{K}}_v = \overline{\mathbb{Q}}_p$ to just be ι_p . Denote also by v the place of F determined by the embedding ι_v ; so ι_v identifies F_v with a finite extension of $\mathcal{K}_v = \mathbb{Q}_p$ in $\overline{\mathbb{Q}}_p$. Let F_v^{ur} be the maximal unramified extension of F_v in $\overline{\mathbb{Q}}_p$ and let R be the ring of integers of F_v^{ur} . Considering the good integral model \mathcal{E}_0/R , let $\widehat{\mathcal{E}}_0$ be the formal completion over the identity section. As we are working over R , $\widehat{\mathcal{E}}_0$ is non-canonically isomorphic to $\widehat{\mathbb{G}}_m$. We fix such an isomorphism $\widehat{\mathcal{E}}_0 \xrightarrow{\sim} \widehat{\mathbb{G}}_m$. The latter is equivalent to fixing an isomorphism of p -divisible groups $\mathcal{E}_0[p^\infty]^0 = \mathcal{E}_0[\mathfrak{p}_v^\infty] \cong \mu_{p^\infty}$, which is uniquely determined up to the action of an element of \mathbb{Z}_p^\times . Here \mathfrak{p}_v is the prime ideal of \mathfrak{D} corresponding to v . The pullback of dt/t under the fixed isomorphism $\widehat{\mathcal{E}}_0 \xrightarrow{\sim} \widehat{\mathbb{G}}_m$ is an element

$$\omega_{\text{can}} \in \Omega^1(\mathcal{E}_0/R) = \Omega^1(\mathcal{E}/\mathcal{O}_{F,(p)}) \otimes_{\mathcal{O}_{F,(p)}} R.$$

We then define the p -adic period $\Omega_p \in R^\times$ by $\omega_{E_0} = \Omega_p \cdot \omega_{\text{can}}$.

Remark 4.5.2. Both Ω_∞ and Ω_p depend on the choice of ω_{E_0} . However, another choice of ω_{E_0} only replaces Ω_∞ and Ω_p with their multiples by the same scalar in $\mathcal{O}_{F,(p)}^\times$. The definition of Ω_∞ also depends on the choice of the complex uniformization. Composing with multiplication by a non-zero scalar $\alpha \in \mathbb{C}^\times$:

$$E_0(\mathbb{C}) \xrightarrow{\sim} \mathbb{C}/\mathfrak{a} \xrightarrow{\sim} \mathbb{C}/\alpha\mathfrak{a},$$

the complex period Ω_∞ gets multiplied by the scalar α . Similarly, Ω_p also depends on the choice of the isomorphism $\widehat{\mathcal{E}}_0 \cong \widehat{\mathbb{G}}_m$; changing this isomorphism replaces Ω_p with a \mathbb{Z}_p^\times -multiple.

4.5.3. Complex and p -adic periods of “false” CM elliptic curves.

To understand the complex and p -adic periods that appear in the formulas in [7], let A be a “false elliptic curve” as in Section 4.2. We take A and its endomorphisms to all be defined over a finite extension F of \mathcal{K} containing the real quadratic field M . We assume that A has good reduction at all places of F over p and we consider a good integral model $\mathcal{A}/\mathcal{O}_{F,(p)}$. Then $\Omega^1(\mathcal{A}/\mathcal{O}_{F,(p)})$ is free of rank two over $\mathcal{O}_{F,(p)}$. Let $e \in \mathcal{O}_B \otimes \mathcal{O}_{M,(p)}$ be an idempotent as in Section 4.2 and let ω_A be an $\mathcal{O}_{F,(p)}$ -generator of $e\Omega^1(\mathcal{A}/\mathcal{O}_{F,(p)})$, i.e., $e\Omega^1(\mathcal{A}/\mathcal{O}_{F,(p)}) = \mathcal{O}_{F,(p)} \cdot \omega_A$. To define a complex period, consider $\Omega^1(A/\mathbb{C}) = \Omega^1(\mathcal{A}/\mathcal{O}_{F,(p)}) \otimes_{\mathcal{O}_{F,(p)}} \mathbb{C}$. If we have a canonical basis element $\omega_{A,\mathbb{C}} \in e\Omega^1(A/\mathbb{C})$, we will then be able to compare it against ω_A to define a complex period. We would similarly get a p -adic period from comparison with a canonical R -basis element of $e\Omega^1(\mathcal{A}/R)$. In the next section, we explain how to obtain such canonical elements when A is a false elliptic curve obtained from a CM elliptic curve via Serre’s tensor product construction.

Remark 4.5.4. For the above, the only hypotheses on the real quadratic field M that is needed is that $B \otimes M$ is split and p splits in M . No additional hypotheses are needed on the idempotent e . The extra hypotheses imposed in Section 4.2 are assumed in the construction of Brooks [7] where they are used to obtain a certain explicit formula for the Maass–Shimura operators; they follow closely the choices made by Mori [36] and Hashimoto [20]. For the comparison between periods of CM elliptic curves and false elliptic curves in the next section we do not need to make these extra assumptions.

4.5.5. Serre’s tensor product construction.

To relate the periods of a CM elliptic curve to the periods of a false elliptic curve, we use Serre’s tensor product construction (see [12, §1.7.4]) which we briefly recall. If E_0/F is a CM elliptic curve as in Section 4.5.1 with complex multiplication by $\mathcal{O}_{\mathcal{K}}$, then by Serre’s tensor product construction applied to $\mathcal{O}_B \otimes_{\mathcal{O}_{\mathcal{K}}} E_0$, there exists a false elliptic scheme $\mathcal{A}/\mathcal{O}_{F,(p)}$ such that $\mathcal{A}(R) = \mathcal{O}_B \otimes_{\mathcal{O}_{\mathcal{K}}} \mathcal{E}_0(R)$ for any $\mathcal{O}_{F,(p)}$ -algebra R ; we let the false elliptic curve A/F be the generic fiber of \mathcal{A} . We will now relate the complex and p -adic periods of A to the complex and p -adic periods of E_0 , respectively.

We have

$$\Omega^1(\mathcal{A}/\mathcal{O}_{F,(p)}) = \mathcal{O}_B \otimes_{\mathcal{O}_{\mathcal{K}}} \Omega^1(\mathcal{E}_0/\mathcal{O}_{F,(p)}) = (\mathcal{O}_B \otimes_{\mathcal{O}_{\mathcal{K}}} \mathcal{O}_{F,(p)}) \otimes_{\mathcal{O}_{F,(p)}} \mathcal{O}_{F,(p)} \cdot \omega_{E_0}.$$

We continue to write e for the image in $\mathcal{O}_B \otimes_{\mathcal{O}_{\mathcal{K}}} \mathcal{O}_{F,(p)}$ of the idempotent $e \in \mathcal{O}_B \otimes \mathcal{O}_{F,(p)}$, and let $\omega_A = e \otimes \omega_{E_0} \in e\Omega^1(\mathcal{A}/\mathcal{O}_{F,(p)})$. Then ω_A is an

$\mathcal{O}_{F,(p)}$ -basis of $e\Omega^1(\mathcal{A}/\mathcal{O}_{F,(p)})$. On the other hand,

$$\Omega^1(A/\mathbb{C}) = \mathcal{O}_B \otimes_{\mathcal{O}_K} \Omega^1(E_0/\mathbb{C}) = (\mathcal{O}_B \otimes_{\mathcal{O}_K} \mathcal{O}_{F,(p)}) \otimes_{\mathcal{O}_{F,(p)}} \mathbb{C} \cdot \omega_{\mathbb{C}},$$

where $\omega_{\mathbb{C}} \in \Omega^1(E_0/\mathbb{C})$ is the 1-form defined in Section 4.5.1. Then $\omega_{A,\mathbb{C}} = e \otimes dz$ is a \mathbb{C} -basis of $e\Omega^1(A/\mathbb{C})$. The complex period $\Omega_{A,\infty} \in \mathbb{C}$ is then defined via $\omega_A = \Omega_{A,\infty} \cdot (2\pi i) \cdot \omega_{A,\mathbb{C}}$. It follows that $\Omega_{A,\infty} = \Omega_{\infty}$.

The comparison of the p -adic periods of E_0 and A is similar. We first note that over R we have

$$A[p^\infty]^0 = \mathcal{O}_B \otimes_{\mathcal{O}_K} \mathcal{E}_0[p^\infty]^0 = \mathcal{O}_B \otimes_{\mathcal{O}_K} \mathcal{E}_0[\mathfrak{p}_v^\infty] \cong (\mathcal{O}_B \otimes_{\mathcal{O}_K} \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mu_{p^\infty},$$

where \mathbb{Z}_p is a \mathcal{O}_K -module via $\mathcal{O}_K \hookrightarrow \mathcal{O}_{K,p} = \mathbb{Z}_p$. It follows that the pullback of $e \otimes dt/t$ is just $\omega_{A,\text{can}} = e \otimes \omega_{\text{can}} \in e\Omega(\mathcal{A}/R) = e(\mathcal{O}_B \otimes_{\mathcal{O}_K} \mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \Omega^1(\mathcal{E}_0/R)$. Here we have used the fixed embedding $M \hookrightarrow \mathbb{Q}_p$ to identify e with an element of $\mathcal{O}_B \otimes \mathbb{Z}_p$. The p -adic period $\Omega_{A,p} \in R^\times$ is then defined via $\omega_A = \Omega_{A,p} \cdot \omega_{A,\text{can}}$. Clearly, $\Omega_{A,p} = \Omega_p$.

5. Anticyclotomic p -adic L -functions

In this section we recall the p -adic L -functions that appear in the Iwasawa-Greenberg main conjectures for the Selmer groups $H^1_{\mathcal{F}_{\text{ac}}}(\mathcal{K}, M)$ and $H^1_{\mathcal{F}_{\text{ac}}}(\mathcal{K}, \mathcal{M})$ defined in Sections 2.3.4 and 3.4, respectively. These conjectures and their current status are recalled in the section following this one. We continue with most of the notation and conventions of the preceding discussion.

5.1. Anticyclotomic p -adic L -functions

Let \mathcal{K} be an imaginary quadratic field of discriminant $-D_{\mathcal{K}} < 0$ such that p splits in \mathcal{K} . Let Σ_{cc} be the set of those continuous characters $\psi : G_{\mathcal{K}} \rightarrow \mathbb{Q}_p^\times$ that satisfy

- $\psi^\tau = \psi^{-1}$;
- ψ factors through Γ ;
- ψ is crystalline at both v and \bar{v} ;
- ψ has Hodge–Tate weights $-n < 0$ and $n > 0$ at v and \bar{v} , respectively.

Such a character ψ is the p -adic avatar of an algebraic Hecke character ψ^{alg} of $\mathbb{A}_{\mathcal{K}}^\times$ as follows. Let $\text{rec}_{\mathcal{K}} : \mathbb{A}_{\mathcal{K}}^\times \rightarrow G_{\mathcal{K}}^{\text{ab}}$ be the reciprocity map of class

field theory, normalized so that uniformizers map to geometric Frobenius elements. Then ψ^{alg} is given by

$$\psi^{\text{alg}}(x) = \psi(\text{rec}_{\mathcal{K}}(x))x_v^{-n}x_{\bar{v}}^n x_{\infty}^n \bar{x}_{\infty}^{-n}.$$

To make sense of this expression we have to explain how this is to be seen as a \mathbb{C}^\times -valued character. The quantity $\psi(\text{rec}_{\mathcal{K}}(x))x_v^{-n}x_{\bar{v}}^n$, which is *a priori* in \mathbb{Q}_p^\times (since \mathcal{K}_v and $\mathcal{K}_{\bar{v}}$ are both just \mathbb{Q}_p), actually belongs to $\overline{\mathbb{Q}}^\times \subset \overline{\mathbb{Q}}_p$; we use the chosen embedding $\overline{\mathbb{Q}} = \overline{\mathcal{K}} \xrightarrow{\iota_v} \overline{\mathcal{K}}_v = \overline{\mathbb{Q}}_p$ to identify $\overline{\mathbb{Q}}^\times$ as a subgroup of $\overline{\mathbb{Q}}_p^\times$. We then use the fixed embedding $\overline{\mathbb{Q}} \subset \mathbb{C}$ to see $\psi(\text{rec}_{\mathcal{K}}(x))x_v^{-n}x_{\bar{v}}^n$ as \mathbb{C} -valued and to identify $\mathcal{K} \otimes \mathbb{R}$ with \mathbb{C} . The character ψ^{alg} then has infinity type $(n, -n)$ in the sense that $\psi_{\infty}^{\text{alg}}(z) = z^n \bar{z}^{-n}$.

Let $f \in S_2(\Gamma_0(N))$ be a newform and let \mathcal{O} and L be as in Section 2.4.1. We assume that **(gen-H)** holds for \mathcal{K} and N . Let B be the quaternion algebra of discriminant N^- and let $R \subset \mathcal{O}_B$ be the orders from Section 4.2. The Jacquet–Langlands correspondence [25] implies the existence of a classical holomorphic quaternionic modular form f_B (that is, a modular form for the arithmetic subgroup $\Gamma_0^B(N^+)$ defined by the units of the Eichler order R) of weight 2 and trivial character and having the same Hecke eigenvalues as f at all primes $\ell \nmid N^-$. Let $\mathfrak{p} \subset \mathbb{Z}(f)$ be the prime determined by the fixed embedding $\mathbb{Q}(f) \hookrightarrow \overline{\mathbb{Q}}_p$ (so L is a finite extension of $\mathbb{Q}(f)_{\mathfrak{p}}$). We now require that **(good)** holds; that is, $p \nmid N$. Then the form f_B can be normalized so that it is defined over $\mathbb{Z}(f)_{(\mathfrak{p})}$ – that is, it is identified with a global section ω_f of $\Omega^1(X_{N^+, N^-}^*/\mathbb{Z}(f)_{(\mathfrak{p})})$ – and non-zero modulo \mathfrak{p} .

Let \mathcal{R} be the completion of the ring of integers of the subfield of $\overline{\mathbb{Q}}_p$ generated by the p -adic field L from Section 2.4 and the maximal unramified extension $\mathbb{Q}_p^{ur} \subset \overline{\mathbb{Q}}_p$ of \mathbb{Q}_p . Note that \mathcal{R} is a complete DVR. As explained in [3], [7], and [8], under the hypotheses **(H)** and **(good)** there exists $L_p(f) \in \Lambda_{\mathcal{R}} := \Lambda \widehat{\otimes}_{\mathcal{O}} \mathcal{R} = \mathcal{R}[[\Gamma]]$ such that for $\psi \in \Sigma_{cc}$ with $n \equiv 0 \pmod{p-1}$, the image $L_p(f, \psi) := \widehat{\psi}(L_p(f)) \in \mathcal{R}$ of $L_p(f)$ under the \mathcal{R} -linear extension of the character ψ to a continuous homomorphism $\widehat{\psi} : \Lambda_{\mathcal{R}} \rightarrow \mathcal{R}$ satisfies

$$(5.1.a) \quad L_p(f, \psi) = E_{\bar{v}}(f, \psi)^2 \cdot t_{\mathcal{K}} \cdot \frac{C(f, \psi)}{\alpha(f, f_B)W(f, \psi)} \cdot \Omega_p^{4n} \cdot \frac{L(f, \psi^{\text{alg}}, 1)}{\Omega_{\infty}^{4n}}.$$

The various factors appearing in this expression are:

- $E_{\bar{v}}(f, \psi) = (1 - \psi^{\text{alg}}(\varpi_{\bar{v}})a_p p^{-1} + \psi^{\text{alg}}(\varpi_{\bar{v}})^2 p^{-1})$, with $\varpi_{\bar{v}} \in \mathcal{K}_{\bar{v}}$ a uniformizer;

- $t_{\mathcal{K}}$ is a power of 2 that depends only on \mathcal{K} (unimportant since p is assumed odd);
- $C(f, \psi) = \frac{1}{4} \pi^{2n-1} \Gamma(n) \Gamma(n+1) w_{\mathcal{K}} \sqrt{D_{\mathcal{K}}} \prod_{\ell|N^-} \frac{\ell-1}{\ell+1}$, where $w_{\mathcal{K}}$ is the number of roots of unity in \mathcal{K} ;
- $W(f, \psi) = W_f N_{\mathcal{K}/\mathbb{Q}}(\mathfrak{b}) \psi^{\text{alg}}(x_{\mathfrak{b}}) N^n b_N^{-2n}$, where $\mathfrak{b} \subset \mathcal{O}_{\mathcal{K}}$ and $b_N \in \mathcal{O}_{\mathcal{K}}$ are as in [7, Prop. 8.3], $x_{\mathfrak{b}} \in \mathbb{A}_{\mathcal{K}}^{\infty, \times}$ is such that $\text{ord}_w(x_{\mathfrak{b}, w}) = \text{ord}_w(\mathfrak{b})$ for all finite places w of \mathcal{K} , and $W_f \in \mathbb{C}^{\times}$ is a complex number of norm one as in the remarks following the proof of Lemma 8.4 of [7]; both \mathfrak{b} and b_N can be taken to be coprime to p ;
- $\alpha(f, f_B) = \frac{\langle f, f \rangle_{\Gamma_0(N)}}{\langle f_B, f_B \rangle_{\Gamma_0^B(N+)}}$ is a ratio of Petersson norms, which are normalized so that $\langle g, g \rangle_{\Gamma} = \int_{\Gamma \backslash \mathfrak{h}} g(z) \overline{g(z)} \frac{dx dy}{y^2}$; in [7] this ratio was shown to belong to L ;
- $\Omega_p \in \mathcal{R}^{\times}$ and $\Omega_{\infty} \in \mathbb{C}^{\times}$ are, respectively, the p -adic and complex periods of a ‘false elliptic curve’ with CM by $\mathcal{O}_{\mathcal{K}}$ as defined at the start of [7, §8.4]; as explained in Section 4.5.5 these can be taken to be the respective p -adic and complex periods of an elliptic curve with complex multiplication by $\mathcal{O}_{\mathcal{K}}$;
- $L(f, \psi^{\text{alg}}, s) = L(\pi_{\mathcal{K}} \times \psi^{\text{alg}}, s - 1/2) = L(V_f^{\vee} \otimes \psi, s)$, where $\pi_{\mathcal{K}}$ is the base change of π to $\text{GL}_2(\mathbb{A}_{\mathcal{K}})$ and, following our earlier convention, we use geometric conventions for the L -function of the $G_{\mathcal{K}}$ -representation $V_f^{\vee} \otimes \psi$.

Remark 5.1.1.

- (a) To see the interpolated values $L_p(f, \psi)$ as belonging to \mathcal{R} , one first recognizes many of the quantities on the right-hand side of (5.1.a) as algebraic, that is, as belonging to $\overline{\mathbb{Q}} \subset \mathbb{C}$. These are then viewed as belonging to $\overline{\mathbb{Q}}_p$ via an embedding extending the fixed inclusion $\mathbb{Q}(f) \hookrightarrow L$.
- (b) To compare the interpolation formula (5.1.a) with that in [7] and [8], one should take $\chi^{-1} = \psi^{\text{alg}}|_{\cdot}|_{\mathbb{A}_{\mathcal{K}}}$ in the formulas in *loc. cit.* Note that χ has infinity type $(-2-j, j)$ with $j = n+1$ (this is infinity type $(2+j, -j)$ with the conventions of *loc. cit.*) and $L(f, \chi^{-1}, 0) = L(f, \psi^{\text{alg}}, 1)$.
- (c) In [3] and [7] the p -adic L -function is only constructed as a continuous function (though the construction clearly gives a measure). The measure is made explicit, for example, in [8].

In this paper we make use of two important results about $L_p(f)$, due to Burungale and Brooks, respectively. The first of these is the vanishing of

the μ -invariant of $L_p(f)$ and the second is a formula for the value $L_p(f, 1)$ under the trivial character (which does not belong to Σ_{cc}). We recall these results in the following two sections.

5.1.2. Vanishing of the anticyclotomic μ -invariant. The choice of topological generator $\gamma \in \Gamma$ determines a continuous isomorphism $\Lambda_{\mathcal{R}} \xrightarrow{\sim} \mathcal{R}[[T]]$ such that $\gamma - 1 \mapsto T$; we use this to identify each $\lambda \in \Lambda_{\mathcal{R}}$ with a power series $\lambda(T)$. Each element $\lambda \in \Lambda_{\mathcal{R}}$ has a unique expression $\lambda(T) = \varpi_{\mathcal{R}}^{\mu(\lambda)} p_{\lambda}(T) u_{\lambda}(T)$ with $\varpi_{\mathcal{R}} \in \mathcal{R}$ a fixed uniformizer, $\mu(\lambda) \in \mathbb{Z}$ a non-negative integer, p_{λ} a monic polynomial of minimal degree, and $u_{\lambda} \in \mathcal{R}[[T]]^{\times}$. The integer $\mu(\lambda)$ – the μ -invariant of λ – and the degree of p_{λ} are independent of the choices of γ and $\varpi_{\mathcal{R}}$.

Under the additional assumption that

(\square -free) N is squarefree

Burungale [8] has shown that the μ -invariant of $L_p(f)$ vanishes:

Proposition 5.1.3 ([8, Thm. B]). *If $p \geq 3$ and (irred $_{\mathcal{K}}$), (split), (H), (good), and (\square -free) hold, then $\mu(L_p(f)) = 0$.*

Let Σ be a finite set of places of \mathcal{K} that do not divide p . We also define an incomplete p -adic L -function $L_p^{\Sigma}(f)$ by removing the Euler factors at those places in Σ :

$$L_p^{\Sigma}(f) = L_p(f) \times \prod_{w \in \Sigma} P_w(\epsilon^{-1} \Psi^{-1}(\text{Frob}_w)) \in \mathcal{R}[[\Gamma]].$$

Then $L_p^{\Sigma}(f, \psi) := \widehat{\psi}(L_p^{\Sigma}(f))$, $\psi \in \Sigma_{cc}$, satisfies the interpolation formula (5.1.a) but with $L(f, \psi^{\text{alg}}, 1)$ replaced with the incomplete L -value $L^{\Sigma}(f, \psi^{\text{alg}}, 1)$ on the right-hand side.

Remark 5.1.4. If $w = (\ell)$ is an inert place in \mathcal{K} , then $\Psi(\text{Frob}_w) = 1$ and in this case $P_w(\epsilon^{-1} \Psi^{-1}(\text{Frob}_w)) = (1 - a_{\ell}(f)\ell^{-1} + \ell^{-1})(1 + a_{\ell}(f)\ell^{-1} + \ell^{-1})$, which can contribute to the μ -invariant of $L_p^{\Sigma}(f)$. In particular, the μ -invariant of the incomplete L -function $L_p^{\Sigma}(f)$ may be greater than that of $L_p(f)$. This does not happen for the usual cyclotomic p -adic L -function.

5.1.5. A formula for $L_p(f, 1)$. We recall Brooks' formula [7, Prop. 8.13] (see also [44, Prop.2.6.1]) for the value $L_p(f, 1)$ of $L_p(f)$ at the trivial character (which is outside the range of interpolation). Suppose that N and \mathcal{K}

satisfy (gen-H). Recall that there is a logarithm map

$$\log_{\omega_f} : J(X_{N^+,N^-}^*)(\mathcal{K}_v) \otimes_{\mathbb{Z}_p} \mathcal{O} \rightarrow \mathcal{K}_v$$

such that $d\log_{\omega_f} = \omega_f \in \Omega^1(J(X_{N^+,N^-}^*)/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathcal{O} = \Omega^1(J(X_{N^+,N^-}^*/\mathcal{O}))$. Recall that $\omega_f \in \Omega^1(J(X_{N^+,N^-}^*)/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathcal{O}$ is the \mathcal{O} -basis element associated with f_B , as defined above. Let $\ell_0 \nmid pN$ be a prime that splits in \mathcal{K} and such that $1 - a_{\ell_0} + \ell_0 \neq 0$ (there are a positive proportion of such ℓ_0). In Section 4.3 we defined a Heegner point $x_{\mathcal{K}}^{N^+,N^-} \in J(X_{N^+,N^-}^*)(\mathcal{K})$. Then Brooks' formula is:

Proposition 5.1.6 ([7, Prop. 8.13]). *Suppose (□-free) holds and N and \mathcal{K} satisfy (gen-H). Then*

$$L_p(f, 1) = \frac{1}{(1 - a_{\ell_0} + \ell_0)^2} \cdot \left(\frac{1 + p - a_p}{p} \right)^2 \left(\log_{\omega_f} x_{\mathcal{K}}^{N^+,N^-} \right)^2,$$

where the equality is up to a p -adic unit.

Brooks' formula is actually given in terms of the logarithm of a point

$$\tilde{x}_{\mathcal{K}}^{N^+,N^-} = \sum_{\sigma \in \text{Gal}(H/\mathcal{K})} \epsilon_f[x]^\sigma \in J(X_{N^+,N^-}^*)(\mathcal{K}') \otimes \mathbb{Z}(f),$$

where $[x]$ is as in the definition of $x_{\mathcal{K}}^{N^+,N^-}$ but ϵ_f is a certain projector in a ring of correspondences. As explained in [44, p.14], the relation with $x_{\mathcal{K}}^{N^+,N^-}$ is $\epsilon_f \cdot x_{\mathcal{K}}^{N^+,N^-} = (1 - a_{\ell_0} + \ell_0) \cdot \tilde{x}_{\mathcal{K}}^{N^+,N^-}$ from which we find

$$\log_{\omega_f} x_{\mathcal{K}}^{N^+,N^-} = \log_{\omega_f} \epsilon_f \cdot x_{\mathcal{K}}^{N^+,N^-} = (1 - a_{\ell_0} + \ell_0) \cdot \log_{\omega_f} \tilde{x}_{\mathcal{K}}^{N^+,N^-}.$$

We now rewrite Brook's formula in a form more directly comparable to the expression (3.5.c) at the end of Section 3. We do this in the case that \bar{V} is an irreducible κ -representation of $G_{\mathbb{Q}}$. Then we can – and do – take A_f and the quotient map $\pi : J(X_{N^+,N^-}^*) \rightarrow A_f$ to be $(\mathbb{Z}(f), \mathfrak{p})$ -optimal in the sense of [58]. This means that π is the composition of an optimal quotient $\pi_0 : J(X_{N^+,N^-}^*) \rightarrow A_0$ and an isogeny $\phi : A_0 \rightarrow A_f$ such that the image of the map $T_p A_0 \rightarrow T_p A_f$ induced by ϕ is not contained in $\mathfrak{p}T_p A_f$. We note that (irred $_{\mathcal{K}}$) also holds and that we may choose $\ell_0 \nmid pN$ such that ℓ_0 splits in \mathcal{K} and (ℓ_0 -good) holds. Then the formula in Proposition 5.1.6 can be expressed as:

Proposition 5.1.7. *Suppose (good) and (irred κ) hold. Then with the above choice of A_f and π , we have that $L_p(f, 1)$ equals*

$$\left(\frac{1+p-a_p}{p}\right)^2 \log_{\omega_{A_f}} \left(z_{\mathcal{K}}^{N^+, N^-}\right)^2,$$

up to a p -adic unit.

Proof. To prove this proposition it suffices to prove that $\pi^*(\omega_{A_f})$ is an \mathcal{O}^\times -multiple of ω_f . By the hypothesis (good), each of $J(X_{N^+, N^-}^*)$, A_0 , and A_f has good reduction at p . Let \mathcal{J} , \mathcal{A}_0 , and \mathcal{A} be their respective Néron models over \mathbb{Z}_p ; these are abelian schemes. The maps π , π_0 , and ϕ extend to morphisms of these Néron models. Furthermore, as π_0 is an optimal quotient (so the kernel of π_0 is also an abelian variety) and since $p-1 > 1$, the image of $\pi_0^* : \Omega^1(\mathcal{A}_0/\mathbb{Z}_p) \rightarrow \Omega^1(\mathcal{J}/\mathbb{Z}_p)$ is a \mathbb{Z}_p -direct summand; this follows from [6, Thm. 4, p. 187] (cf. [1, Cor. A.1]). So it suffices to show that $\phi^*(\omega_{A_f})$ is part of an \mathcal{O} -basis of $\Omega^1(\mathcal{A}_0/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathcal{O}$.

We have that

$$\Omega^1(\mathcal{A}_f/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathcal{O}/p = \Omega^1(\mathcal{A}_f/\mathbb{F}_p) \otimes_{\mathbb{Z}_p} \mathcal{O}/p = \text{Lie}_{\mathbb{F}_p}(\mathcal{A}_f[p]^0)^\vee \otimes_{\mathbb{Z}_p} \mathcal{O}/p.$$

Using the prime factorization $p\mathbb{Z}(f) = \prod_{\mathfrak{q}|p} \mathfrak{q}^{e_{\mathfrak{q}}}$, the right-hand side can be written as

$$\prod_{\mathfrak{q}|p} \text{Lie}_{\mathbb{F}_p}(\mathcal{A}_f[\mathfrak{q}^{e_{\mathfrak{q}}}]^0)^\vee \otimes_{\mathbb{Z}_p} \mathcal{O}/p.$$

By the choice of ω_{A_f} , the image of ω_{A_f} in $\Omega^1(\mathcal{A}_f/\mathbb{Z}_p) \otimes_{\mathbb{Z}_p} \mathcal{O}/p$ is identified with a \mathcal{O}/p -basis element of the \mathfrak{p} -summand (that is, for $\mathfrak{q} = \mathfrak{p}$). So it suffices to prove that ϕ^* induces an injection

$$\text{Lie}_{\mathbb{F}_p}(\mathcal{A}_f[\mathfrak{p}^{e_{\mathfrak{p}}}]^0)^\vee \otimes_{\mathbb{Z}_p} \mathcal{O}/p \hookrightarrow \text{Lie}_{\mathbb{F}_p}(\mathcal{A}_0[p]^0)^\vee \otimes_{\mathbb{Z}_p} \mathcal{O}/p.$$

For this, we note that since the image of $T_p A_0$ is not contained in $\mathfrak{p}T_p A_f$, and since $A_f[\mathfrak{p}]$ is an irreducible κ -representation of $G_{\mathbb{Q}}$, the induced homomorphism

$$A_0[p] = T_p A_0/pT_p A_0 \rightarrow T_p A_f/\mathfrak{p}^{e_{\mathfrak{p}}} T_p A_f = A_f[\mathfrak{p}^{e_{\mathfrak{p}}}]$$

is surjective. Hence the morphism $\mathcal{A}_0[p] \rightarrow \mathcal{A}_f[\mathfrak{p}^{e_{\mathfrak{p}}}]$ is surjective and so, too, is the induced map of the Lie algebras of their connected subgroups. \square

5.2. The two-variable Rankin–Selberg p -adic L -function

The p -adic L -function $L_p^\Sigma(f)$ is the specialization of a p -adic L -function $\mathcal{L}_p^\Sigma(f) \in \Lambda_{\mathcal{K}, \mathcal{R}} := \mathcal{R}[[\Gamma_{\mathcal{K}}]]$ first constructed by Hida [22]. In what follows we recall this p -adic L -function and explain its relation to $L_p^\Sigma(f)$.

Let $\Lambda^+ = \mathcal{O}[[\Gamma_{\mathcal{K}}^+]]$. Let

$$u = \epsilon(\gamma^+).$$

We say that a continuous \mathcal{O} -homomorphism $\lambda : \Lambda^+ \rightarrow \overline{\mathbb{Q}}_p$ is algebraic of weight n if $\lambda(\gamma_+) = u^{-n}$ for some integer $n \geq 0$. Let $\mathbb{K}_\infty^v \subset \mathbb{K}_\infty$ be the maximal subfield unramified at v , and let $\Gamma_v = \text{Gal}(\mathbb{K}_\infty^v/\mathcal{K})$. Then $\Gamma_v \cong \mathbb{Z}_p$. Let $\mathcal{I} = \mathcal{O}[[\Gamma_v]]$. The composite of the canonical homomorphisms $\Gamma_{\mathcal{K}}^+ \hookrightarrow \Gamma_{\mathcal{K}} \twoheadrightarrow \Gamma_v$ makes \mathcal{I} into a Λ^+ -homomorphism. We say that a continuous \mathcal{O} -homomorphism $\lambda : \mathcal{I} \rightarrow \overline{\mathbb{Q}}_p$ is algebraic of weight $k = 2n + 1 \geq 1$ if its restriction to Λ^+ is algebraic of weight n .

Let $\Theta_v : \mathbb{A}_{\mathcal{K}}^\times \rightarrow \Gamma_v$ be the composition of the reciprocity map $\text{rec}_{\mathcal{K}} : \mathbb{A}_{\mathcal{K}}^\times \rightarrow G_{\mathcal{K}}^{\text{ab}}$ of class field theory with the canonical projection $G_{\mathcal{K}}^{\text{ab}} \twoheadrightarrow \Gamma_v$. For each non-zero fractional ideal \mathfrak{a} of \mathcal{K} , we let $x_{\mathfrak{a}} \in \mathbb{A}_{\mathcal{K}}^{\infty, \times}$ be a finite idèle of \mathcal{K} such that $\text{ord}_w(x_{\mathfrak{a}, v}) = \text{ord}_w(\mathfrak{a})$ for all finite places w of \mathcal{K} . Then the formal q -expansion

$$\mathfrak{f} = \sum_{n=1}^{\infty} \mathfrak{b}(n)q^n \in \mathcal{I}[[q]], \quad \mathfrak{b}(n) = \sum_{\substack{\mathfrak{a} \subset \mathcal{O}_{\mathcal{K}}, N(\mathfrak{a})=n \\ (\mathfrak{a}, \mathfrak{p}_{\bar{v}})=1}} \Theta_v(x_{\mathfrak{a}}),$$

is an ordinary \mathcal{I} -adic eigenform of tame level $D_{\mathcal{K}}$, in the sense that if $\lambda : \mathcal{I} \rightarrow \overline{\mathbb{Q}}_p$ is an algebraic homomorphism of weight $k = 2n + 1$ with $n \equiv 0 \pmod{p-1}$, then $f_\lambda = \sum_{n=1}^{\infty} \lambda(\mathfrak{b}(n))q^n$ is the q -expansion of a p -ordinary p -stabilized newform of weight k and level $D_{\mathcal{K}}p$. The form f_λ can be identified as follows. The condition that λ be algebraic of weight k implies that $\rho_\lambda = \lambda|_{\Gamma_v}$, viewed as a continuous $\overline{\mathbb{Q}}_p^\times$ -valued character of $G_{\mathcal{K}}$, has Hodge–Tate weights 0 and $k-1$ at v and \bar{v} , respectively. Associated with ρ_λ is an algebraic Hecke character $\rho_\lambda^{\text{alg}}$ with infinity type $(0, 1-k)$ that is unramified at v and \bar{v} . The ordinary eigenform f_λ is the ordinary p -stabilization of the newform f_λ^0 of weight k and level $D_{\mathcal{K}}$ associated with $\rho_\lambda^{\text{alg}}$ (so, in particular, $L(f_\lambda^0, s) = L(\rho_\lambda^{\text{alg}}, s)$).

Let $\Lambda^{\text{Hida}} = \mathcal{O}[[1 + p\mathbb{Z}_p]]$ (this is denoted Λ in [22]). We give Λ^+ the structure of a Λ^{Hida} -algebra by $1 + \mathbb{Z}_p \ni u \mapsto u^{-1}\gamma_+^{-1} \in \Lambda^+$; this is an isomorphism. We also endow \mathcal{I} with the structure of a Λ^{Hida} -algebra by $1 + \mathbb{Z}_p \ni u \mapsto u\gamma_+^{-2} \in \mathcal{I}$. With the latter structure, our definition of an

algebraic homomorphism of weight k is consistent with that in [22]. Note that \mathcal{I} is a finite, flat Λ^{Hida} -algebra.

For a p -adic \mathcal{O} -algebra A , let $\mathcal{X}(A) = \text{Hom}_{\mathcal{O}\text{-alg}, \text{cts}}(A, \overline{\mathbb{Q}}_p)$ be the set of all continuous \mathcal{O} -algebra homomorphisms. Hida [22, Thm. 5.1b] has shown that there is an element D in the fraction ring of $\mathcal{I} \widehat{\otimes}_{\mathcal{O}} \Lambda^+$ that, when viewed as a p -adic analytic function on $\mathcal{X}(\mathcal{I}) \times \mathcal{X}(\Lambda^+)$, has the following properties. The function D is finite at each point $(\lambda, \lambda') \in \mathcal{X}(\mathcal{I}) \times \mathcal{X}(\Lambda^+)$ with λ and λ' algebraic homomorphisms of respective weights k and n and satisfying $1 \leq n \leq k - 1$, and if $k \equiv 1 \pmod{2(p - 1)}$ and $n \equiv 0 \pmod{p - 1}$, then

$$(5.2.a) \quad D(\lambda, \lambda') = (D_{\mathcal{K}} N)^{k/2} N^n \Gamma(n) \Gamma(n + 1) W_f \frac{E(1 + n)}{S(\lambda)} \frac{\mathcal{D}(1 + n, f_{\lambda}, f)}{\Omega(f_{\lambda}, f, n)},$$

where

- $S(\lambda) = (1 - p^{k-1} \rho_{\lambda}^{\text{alg}}(\varpi_v)^{-2})(1 - p^{k-2} \rho_{\lambda}^{\text{alg}}(\varpi_v)^{-2});$
- $E(s) = (1 - \rho_{\lambda}^{\text{alg}}(\varpi_v) a_p(f) p^{-s} + \rho_{\lambda}^{\text{alg}}(\varpi_v) p^{1-s});$
- $\mathcal{D}(f_{\lambda}, f, s) = \zeta^{pND_{\mathcal{K}}}(k + 2 - 2s - 2) \times \sum_{n=1}^{\infty} a_n(f_{\lambda}) a_n n^{-s}$
 $= E(s) L(f, (\rho_{\lambda}^{\text{alg}}), s);$
- $\Omega(f_{\lambda}, f, n) = (2\pi i)^{2n-1} (2i)^{k+1} \pi^2 \langle f_{\lambda}^0, f_{\lambda}^0 \rangle_{\Gamma_1(D_{\mathcal{K}})}.$

Let $\mathcal{I}_{\mathcal{R}} = \mathcal{I} \widehat{\otimes}_{\mathcal{O}} \mathcal{R} = \mathcal{R}[\Gamma_v]$ and let $L_p^-(\mathcal{K}) \in \mathcal{I}$ be the anticyclotomic p -adic L -function of the imaginary quadratic field K . The p -adic L -function $L_p^-(\mathcal{K})$ is a specialization of Katz’s two-variable p -adic L -function and satisfies the following interpolation property: for an integer $k \geq 0$ such that $k \equiv 1 \pmod{2(p - 1)}$ and $\lambda \in \mathcal{X}(\mathcal{I})$ an algebraic homomorphism of weight k ,

$$L_p^-(\mathcal{K}, \lambda) := \lambda(L_p^-(\mathcal{K})) = S(\lambda) \Omega_p^{2k-2} \frac{w_{\mathcal{K}} (2\pi)^{k-2} \Gamma(k)}{2D_{\mathcal{K}}^{(k-1)/2} \Omega_{\infty}^{2k-2}} L(\rho_{\lambda}^{\text{alg}} \rho_{\lambda}^{\text{alg}, -\tau}, 1).$$

Here the superscript ‘ $-\tau$ ’ denotes composing the inverse character with the action on $\mathbb{A}_{\mathcal{K}}^{\times}$ of the nontrivial automorphism τ of K . The complex and p -adic periods Ω and Ω_p are the periods of an elliptic curve with CM by $\mathcal{O}_{\mathcal{K}}$ and can be fixed to be the same as those appearing in (5.1.a). Appealing to the well-known relation

$$\begin{aligned} \langle f_{\lambda}^0, f_{\lambda}^0 \rangle_{\Gamma_1(D_{\mathcal{K}})} &= \Gamma(k) D_{\mathcal{K}}^2 2^{-2k} \pi^{-1-k} \cdot \text{res}_{s=k} \mathcal{D}(s, f_{\lambda}, f_{\lambda}^{\tau}) \\ &= \Gamma(k) D_{\mathcal{K}}^2 2^{-2k} \pi^{-1-k} \cdot \frac{2\pi h_{\mathcal{K}}}{w_{\mathcal{K}} D_{\mathcal{K}}^{1/2}} L(\rho_{\lambda}^{\text{alg}} \rho_{\lambda}^{\text{alg}, -\tau}, 1), \end{aligned}$$

where $h_{\mathcal{K}}$ is the class number of \mathcal{K} , the interpolation formula for $L_p^-(\mathcal{K})$ can be rewritten as

$$(5.2.b) \quad L_p^-(\mathcal{K}, \lambda) = w_{\mathcal{K}}^2 S(\lambda) \Omega_p^{2k-2} \frac{\pi^{2k-2} 2^{3k-4}}{h_{\mathcal{K}} D_{\mathcal{K}}^{k/2+1} \Omega_{\infty}^{2k-2}} \langle f_{\lambda}^0, f_{\lambda}^0 \rangle_{\Gamma_1(D_{\mathcal{K}})}.$$

Note that $\rho_{\lambda}^{\text{alg}} \rho_{\lambda}^{\text{alg}, -\tau}$ is an anticyclotomic character with infinity type $(k - 1, 1 - k)$.

Suppose

$$(units) \quad p \nmid w_{\mathcal{K}}.$$

We put

$$\mathcal{L}_p(f) = \left(\frac{h_{\mathcal{K}}}{w_{\mathcal{K}}} L_p^-(\mathcal{K}) \otimes 1 \right) D.$$

We consider $\mathcal{L}_p(f)$ as an element of the fraction field of $\Lambda_{\mathcal{K}} = \mathcal{O}[[\Gamma_{\mathcal{K}}]]$ via the isomorphism $\Gamma_{\mathcal{K}} \xrightarrow{\sim} \Gamma_v \oplus \Gamma_{\mathcal{K}}^+$ that is the direct sum of the canonical projections to Γ_v and $\Gamma_{\mathcal{K}}^+$, respectively. Then for a finite set Σ of finite places of K not dividing p we put

$$\mathcal{L}_p^{\Sigma}(f) = \mathcal{L}_p(f) \times \prod_{w \in \Sigma} P_w(\epsilon^{-1} \Psi_{\mathcal{K}}(\text{frob}_w)).$$

If Σ contains all places dividing $ND_{\mathcal{K}}$ that do not divide p , then Wan has shown that $\mathcal{L}_p^{\Sigma}(f) \in \Lambda_{\mathcal{K}}$ [52]. For such Σ we let $\mathcal{L}_p^{\Sigma}(f)^- \in \Lambda$ be the image of $\mathcal{L}_p^{\Sigma}(f)$ under the quotient map $\Lambda_{\mathcal{K}} \twoheadrightarrow \Lambda$ induced by the canonical projection $\Gamma_{\mathcal{K}} \twoheadrightarrow \Gamma$.

5.3. Relating $\mathcal{L}_p^{\Sigma}(f)^-$ to $L_p^{\Sigma}(f)$

Let $\psi \in \Sigma_{cc}$. By abuse of notation we also denote by $\widehat{\psi}$ the homomorphism of $\Lambda_{\mathcal{K}}$ obtained by composition with the projection $\Lambda_{\mathcal{K}} \twoheadrightarrow \Lambda$ and we put $\mathcal{L}_p^{\Sigma}(f, \psi)^- = \widehat{\psi}(\mathcal{L}_p^{\Sigma}(f))$. Then the homomorphism $\widehat{\psi} \in \mathcal{X}(\Lambda_{\mathcal{K}})$ corresponds via the isomorphism $\Lambda_{\mathcal{K}} \xrightarrow{\sim} \mathcal{I} \widehat{\otimes}_{\mathcal{O}} \Lambda^+$ to the point $(\lambda, \lambda') \in \mathcal{X}(\mathcal{I}) \times \mathcal{X}(\Lambda^+)$ with $\lambda|_{\Gamma_v} = \psi_n \epsilon^{-n}$ (and so algebraic of weight $2n + 1$) and with $\lambda'|_{\Gamma_{\mathcal{K}}^+} = \epsilon^n$ (and so algebraic of weight n). Here n is such that ψ^{alg} has infinity type $(n, -n)$. From the interpolation formulas for $D(\lambda, \lambda')$ and $L_p^-(\mathcal{K}, \lambda)$ we then find

$$\begin{aligned} \mathcal{L}_p^{\Sigma}(f, \psi)^- = \widehat{\psi}(\mathcal{L}_p^{\Sigma}(f)) &= w_{\mathcal{K}} N^{2n+1/2} D_{\mathcal{K}}^{-1} \Gamma(n) \Gamma(n+1) W_{f_i}^{-1} 2^{2n} \pi^{2n-1} \\ &\quad \times E_{\bar{v}}(f, \psi)^2 \Omega_p^{4n} \frac{L^{\Sigma}(f, \psi_n^{\text{alg}}, 1)}{\Omega^{4n}}. \end{aligned}$$

In particular, for $\psi \in \Sigma_{cc}$,

$$(5.3.a) \quad \mathcal{L}_p^\Sigma(f, \psi)^- = c(f, \psi)L_p(f, \psi),$$

where

$$c(f, \psi) = t_K^{-1} D_K^{-3/2} N^{3n+1/2} \cdot \prod_{\ell|N^-} \left(\frac{\ell + 1}{\ell - 1} \right) 2^{2n+2} i^{-1} N_{\mathcal{K}/\mathbb{Q}}(\mathbf{b}) \psi^{\text{alg}}(x_{\mathbf{p}}) b_N^{-2n} \alpha(f, f_{\mathbf{b}}).$$

The following lemma allows us to pass from (5.3.a) to a relation between $\mathcal{L}_p^\Sigma(f, \psi)^-$ and $L_p^\Sigma(f)$.

Lemma 5.3.1. *There exist $c \in R \left[\frac{1}{p} \right]^\times$ and $\mathcal{U} \in \Lambda^\times$ such that $c(f, \psi) = c\widehat{\psi}(\mathcal{U})$ for all $\psi \in \Sigma_{cc}$ with $n \equiv 0 \pmod{p-1}$.*

Proof. We let

$$c = t_K^{-1} D_K^{-3/2} N^{1/2} \prod_{\ell|N^-} \left(\frac{\ell + 1}{\ell - 1} \right) 2^{2} i^{-1} N_{\mathcal{K}/\mathbb{Q}}(\mathbf{b}) \alpha(f, f_B) \in R \left[\frac{1}{p} \right]^\times.$$

We can assume that $x_{\mathbf{b}}$ is chosen so that $x_{\mathbf{b},v} = 1 = x_{\mathbf{b},\bar{v}}$. Let $\gamma_{\mathbf{b}} \in \Gamma$ be the image of $\text{rec}_{\mathcal{K}}(x_{\mathbf{b}})$. Then $\psi^{\text{alg}}(x_{\mathbf{b}}) = \psi(\gamma_{\mathbf{b}})$. Let $\gamma_v \in \Gamma$ be a topological generator of the image of the inertia group I_v . For ψ to be crystalline at v with Hodge-Tate weight $-n$ means that $\psi(\gamma_v) = \epsilon(\gamma_v)^n$. Let $a_v \in \mathbb{Z}_p^\times$ such that $\epsilon(\gamma_v) = (1 + p)^{a_v}$ and put

$$\mathcal{U} = \gamma_v^{(2\log_p(2)+3\log_p(N)+\log_p(b_N))/a_v} \gamma_{\mathbf{b}} \in \Gamma \subset \Lambda^\times.$$

Here \log_p is the Iwasawa p -adic logarithm. Also, we are viewing $b_N \in \mathcal{O}_{\mathcal{K},(p)}^\times$ as an element of \mathbb{Z}_p^\times via the identification $\mathbb{Z}_p = \mathcal{O}_{\mathcal{K},v}$ (which comes from the hypothesis that p splits in \mathcal{K}). Then if $n \equiv 0 \pmod{p-1}$, \mathcal{U} satisfies

$$\widehat{\psi}(\mathcal{U}) = (1 + p)^{n(2\log_p(2)+3\log_p(N)+\log_p(b_N))} \psi^{\text{alg}}(x_{\mathbf{b}}) = 2^{2n} N^{3n} b_N^n \psi^{\text{alg}}(x_{\mathbf{b}}),$$

and so $c\widehat{\psi}(\mathcal{U}) = c(f, \psi)$. □

Combining Lemma 5.3.1 with (5.3.a) we find that $\mathcal{L}_p^\Sigma(f, \psi)^- = \widehat{\psi}(c\mathcal{U}L_p^\Sigma(f))$ for all $\psi \in \Sigma_{cc}$ with $n \equiv 0 \pmod{p-1}$. If Σ contains all the places dividing $ND_{\mathcal{K}}$ not dividing p , then $\mathcal{L}_p^\Sigma(f, \psi)^- = \widehat{\psi}(\mathcal{L}_p^\Sigma(f)^-)$

for all these ψ . Since the set of kernels of the homomorphisms $\widehat{\psi}$ of $\Lambda_{\mathcal{R}}$ for such ψ are Zariski dense in $\text{Spec}(\Lambda_{\mathcal{R}})$, we conclude that we then have $\mathcal{L}_p^\Sigma(f)^- = \mathcal{UL}_p(f)$ in $\Lambda_{\mathcal{R}}$. Hence:

Corollary 5.3.2. *If Σ contains all places of \mathcal{K} dividing $ND_{\mathcal{K}}$ that do not divide p , then $(L_p^\Sigma(f)) = (\mathcal{L}_p^\Sigma(f)^-)$ in $\Lambda_{\mathcal{R}} \left[\frac{1}{p} \right]$.*

Remark 5.3.3. It is possible to define $\mathcal{L}_p^\Sigma(f)^-$ for all finite sets Σ of places of \mathcal{K} not dividing p and to directly show, again making use of (5.3.a) and Lemma 5.3.1, that the conclusion of Corollary 5.3.2 holds for all such Σ . We will not need this.

6. Main conjectures

For the Selmer groups $H_{\mathcal{F}_{ac}^\Sigma}^1(\mathcal{K}, M)$ and $H_{\mathcal{F}_{Gr}^\Sigma}^1(\mathcal{K}, \mathcal{M})$ from Section 2.3.4, let

$$\begin{aligned} X_{ac}^\Sigma(M) &= \text{Hom}_{\mathcal{O}}(H_{\mathcal{F}_{ac}^\Sigma}^1(\mathcal{K}, M), L/\mathcal{O}) \quad \text{and} \\ X_{Gr}^\Sigma(\mathcal{M}) &= \text{Hom}_{\mathcal{O}}(H_{\mathcal{F}_{Gr}^\Sigma}^1(\mathcal{K}, \mathcal{M}), L/\mathcal{O}). \end{aligned}$$

We now recall the Iwasawa-Greenberg main conjectures for these groups together with some recent results towards proving these conjectures. To do this, recall that $\Lambda = \mathcal{O}[[\Gamma]]$ and $\Lambda_{\mathcal{K}} = \mathcal{O}[[\Gamma_{\mathcal{K}}]]$ and that \mathcal{R} is the valuation ring of the completion of the maximal unramified extension of L . Let $\Lambda_{\mathcal{R}} = \mathcal{R}[[\Gamma]]$ and $\Lambda_{\mathcal{K},\mathcal{R}} = \mathcal{R}[[\Gamma_{\mathcal{K}}]]$. The groups $X_{ac}^\Sigma(M)$ and $X_{Gr}^\Sigma(\mathcal{M})$ are, respectively, finite Λ - and $\Lambda_{\mathcal{K}}$ -modules.

6.1. The Iwasawa–Greenberg main conjectures

Let Σ be a finite set of finite places of \mathcal{K} that do not divide p . The main conjectures are easy to state:

Conjecture 6.1.1 (Main Conjecture for \mathcal{M}). *Let $\mathcal{L}_p^\Sigma(f)$ be Hida’s two variable p -adic L -function recalled in Section 5.2. Then*

$$\text{char}_{\Lambda_{\mathcal{K}}} (X_{Gr}^\Sigma(\mathcal{M})) \Lambda_{\mathcal{K},\mathcal{R}} = (\mathcal{L}_p^\Sigma(f)) \subset \Lambda_{\mathcal{K},\mathcal{R}}.$$

Note that implicit in the statement of this conjecture is that $\mathcal{L}_p^\Sigma(f)$ belongs to $\Lambda_{\mathcal{K},\mathcal{R}}$ and not just its field of fractions. In Section 5.2 this was explained to be known to hold when Σ is sufficiently large.

Conjecture 6.1.2 (Main Conjecture for M). *Let $L_p^\Sigma(f) \in \Lambda_{\mathcal{R}}$ be the p -adic L -function defined in Section 5.1. Then*

$$\text{char}_\Lambda (X_{\text{ac}}^\Sigma(M)) \Lambda_{\mathcal{R}} = (L_p^\Sigma(f)) \subset \Lambda_{\mathcal{R}}.$$

Remark 6.1.3. Note that we always have equalities of ideals

$$\text{char}_{\Lambda_{\mathcal{K}, \mathcal{R}}} (X_{\text{Gr}}^\Sigma(\mathcal{M}) \otimes_{\Lambda_{\mathcal{K}}} \Lambda_{\mathcal{K}, \mathcal{R}}) = \text{char}_{\Lambda_{\mathcal{K}}} (X_{\text{Gr}}^\Sigma(\mathcal{M})) \Lambda_{\mathcal{K}, \mathcal{R}}$$

and

$$\text{char}_{\Lambda_{\mathcal{R}}} (X_{\text{ac}}^\Sigma(M) \otimes_{\Lambda} \Lambda_{\mathcal{R}}) = \text{char}_\Lambda (X_{\text{ac}}^\Sigma(M)) \Lambda_{\mathcal{R}}.$$

Recently substantial progress has been made toward these conjectures in [52] and [53] by following the strategy from [46] of exploiting congruences between suitable Eisenstein series and cuspforms, this time on $\text{GU}(3, 1)$.

Theorem 6.1.4 ([52, Thm.1.1], [53, Thm.1.1]). *Suppose (irred $_{\mathcal{K}}$), (split), (gen-H), (good), and (\square -free) hold. Suppose also that there is at least one prime divisor of N non-split in \mathcal{K} and that Σ contains all places dividing $ND_{\mathcal{K}}$. Then*

$$\text{char}_{\Gamma_{\mathcal{K}}} (X_{\text{Gr}}^\Sigma(\mathcal{M})) \Lambda_{\mathcal{K}, \mathcal{R}} [1/p] \subseteq (\mathcal{L}_p^\Sigma(f)) \subset \Lambda_{\mathcal{K}, \mathcal{R}} [1/p].$$

Combining this with Corollary 3.4.2 and Corollary 5.3.2, we conclude:

Theorem 6.1.5. *Suppose (irred $_{\mathcal{K}}$), (split), (gen-H), (good), and (\square -free) hold. Suppose also that there is at least one prime divisor of N non-split in \mathcal{K} and that Σ contains all places dividing $ND_{\mathcal{K}}$. Then*

$$\text{char}_\Lambda (X_{\text{ac}}^\Sigma(M)) \Lambda_{\mathcal{R}} [1/p] \subset (L_p^\Sigma(f)) \subset \Lambda_{\mathcal{R}} [1/p].$$

This theorem can be strengthened upon combination with Proposition 3.3.3 (in particular, the surjectivity of (3.3.a)) and Burungale's $\mu = 0$ result of Proposition 5.1.3 (combined with a result of Hsieh [24] to also include the case when N may not be coprime to the discriminant of \mathcal{K}):

Theorem 6.1.6. *Suppose that (irred $_{\mathcal{K}}$), (split), (gen-H), (good), (corank 1), (sur) and (\square -free) hold. Suppose also that there is at least one prime divisor of N non-split in \mathcal{K} . Then*

$$\text{char}_\Lambda (X_{\text{ac}}^\Sigma(M)) \Lambda_{\mathcal{R}} \subset (L_p^\Sigma(f)) \subset \Lambda_{\mathcal{R}}.$$

Proof. Let $\Sigma_1 \subset \Sigma_2$ be two finite sets of places of \mathcal{K} dividing p and with Σ_2 containing all the places dividing $ND_{\mathcal{K}}$. Then the surjectivity of (3.3.a) yields

$$\begin{aligned} & \text{char}_{\Lambda} (X_{\text{ac}}^{\Sigma_2}(M)) \\ &= \text{char}_{\Lambda} (X_{\text{ac}}^{\Sigma_1}(M)) \text{char}_{\Lambda} \left(\prod_{w \in \Sigma_2 \setminus \Sigma_1} \text{Hom}_{\mathcal{O}} \left(\frac{H^1(\mathcal{K}_w, M)}{H_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}_w, M)}, L/\mathcal{O} \right) \right) \\ &= \text{char}_{\Lambda} (X_{\text{ac}}^{\Sigma_1}(M)) \prod_{w \in \Sigma_2 \setminus \Sigma_1} (P_w(\epsilon^{-1}\Psi^{-1}(\text{Frob}_w))). \end{aligned}$$

Here, we have used that $P_w(\epsilon^{-1}\Psi^{-1}(\text{Frob}_w))$ is a generator for the characteristic ideal of the Pontrjagin dual of $H^1(\mathcal{K}_w, M)/H_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}_w, M)$ (a consequence of [46, §4.3.13] and [17, Prop.2.4]). Comparing this with the definition of $L_p^{\Sigma_2}(f)$ we then see that the hypothesis that Σ contain the places dividing $ND_{\mathcal{K}}$ can be removed from Theorem 6.1.5. In the case where $\Sigma = \emptyset$ the resulting inclusion of ideals can then be improved to an inclusion in $\Lambda_{\mathcal{R}}$ in light of the $\mu = 0$ result of Proposition 5.1.3. The inclusion in $\Lambda_{\mathcal{R}}$ for any Σ then follows. \square

Remark 6.1.7. As a consequence of our results below, in some cases we will be able to improve the inclusion in Theorem 6.1.6 to an equality.

6.2. Consequences for the order of $H_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}, W)$

We can now record the key result connecting the value $L_p(f, 1)$ with the order of $H_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}, W)$.

Proposition 6.2.1. *Suppose (irred $_{\mathcal{K}}$), (split), (gen-H), (good), (corank 1), (sur) and (\square -free) hold. Suppose also that there is at least one prime divisor of N non-split in \mathcal{K} . Then $L_p(f, 1) \neq 0$ and*

$$\#\mathcal{O}/(L_p(f, 1)) \mid \#H_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}, W) \cdot C(W),$$

where $C(W) = C^{\emptyset}(W)$ is as in Theorem 3.3.1.

Proof. Let $(f_{\text{ac}}(T)) = \text{char}_{\Lambda} (X_{\text{ac}}(M))$ with $f_{\text{ac}}(T) \in \mathcal{O}[[T]] \cong \Lambda$, where the isomorphism identifies $1 + T$ with the chosen topological generator γ . Then by Theorem 6.1.6, $L_p(f)$ divides $f_{\text{ac}}(T)$ in $\mathcal{R}[[T]]$. In particular $f_{\text{ac}}(0)$ is an \mathcal{R} -multiple of $L_p(f, 1)$. On the other hand, by Theorem 3.3.1

$$\#\mathcal{O}/(f_{\text{ac}}(0)) = \#H_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}, W) \cdot C(W) < \infty.$$

(The finiteness of the right-hand side was established in Proposition 3.2.1.)
The proposition follows. \square

7. Proof of the main theorem

In this section we piece together the results from the previous sections to prove the main result of the paper, Theorem 1.2.1. We therefore take E/\mathbb{Q} to be an elliptic curve as in that theorem. In particular, we assume:

- E is a semistable elliptic curve with square-free conductor N ;
- E has good reduction at the prime p (i.e., $p \nmid N$);
- if $p = 3$ and E has supersingular reduction at p , then $a_p(E) = 0$;
- the residual representation $\bar{\rho}_{E,p} : G_{\mathbb{Q}} \rightarrow \text{Aut}(E[p])$ is irreducible;
- $\text{ord}_{s=1} L(E, s) = 1$.

The results of Gross–Zagier and Kolyvagin then imply that $\text{rk}_{\mathbb{Z}} E(\mathbb{Q}) = 1$ and $\text{III}(E/\mathbb{Q})$ is finite. To prove Theorem 1.2.1 we must show that the same power of p appears in both sides of (1.1.a). Since Conjecture 1.1.1 is isogeny invariant – more precisely, the ratio of both sides of (1.1.a), when both are finite, is an invariant of the isogeny class of E (cf. [49, Thm. 2.1]) – we may further assume:

- E admits an optimal quotient map $\pi : J(X_0(N)) \rightarrow E$ (that is, such that the kernel of π is connected).

7.1. The Birch and Swinnerton-Dyer conjecture

We will eventually deduce both the conjectured upper and lower bounds on $\#\text{III}(E/\mathbb{Q})[p^\infty]$ from corresponding upper and lower bounds for $\#\text{III}(E/\mathcal{K})[p^\infty]$ for suitable imaginary quadratic fields \mathcal{K} . For this reason we find it helpful to recall the general Birch and Swinnerton-Dyer conjecture for an elliptic curve over a number field. As stated by Tate [49, (A) and (B)], this is:

Conjecture 7.1.1 (general Birch and Swinnerton-Dyer Conjecture). *Let F be a number field and let \mathcal{E}/F be an elliptic curve over F .*

- (a) *The Hasse–Weil L -function $L(\mathcal{E}/F, s)$ has an analytic continuation to the entire complex plane and $\text{ord}_{s=1} L(\mathcal{E}/F, s) = \text{rk}_{\mathbb{Z}} \mathcal{E}(F)$;*
- (b) *The Tate–Shafarevich group $\text{III}(\mathcal{E}/F)$ has finite order, and*
(7.1.a)

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

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

$$(7.1.b) \quad \Omega_{\mathcal{E}/F} = N_{F/\mathbb{Q}}(\mathfrak{a}_\omega) \cdot \prod_{\substack{v|\infty \\ v\text{-real}}} \int_{\mathcal{E}(F_v)} |\omega| \cdot \prod_{\substack{v|\infty \\ v\text{-complex}}} \left(2 \cdot \int_{\mathcal{E}(F_v)} \omega \wedge \bar{\omega} \right).$$

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

When $F = \mathbb{Q}$, we generally write $\Omega_{\mathcal{E}}$ for $\Omega_{\mathcal{E}/\mathbb{Q}}$.

7.2. The Birch–Swinnerton-Dyer formula for rank zero elliptic curves

To pass from the expected upper and lower bounds for $\#\text{III}(E/\mathcal{K})[p^\infty]$ for suitable imaginary quadratic fields $\mathcal{K} = \mathbb{Q}(\sqrt{D})$ ($D < 0$) to the expected upper or lower bound for $\#\text{III}(E/\mathbb{Q})[p^\infty]$, we will need to appeal to known results for the BSD formula for the \mathcal{K} -twists⁷ E^D of E . The fields \mathcal{K} will always be chosen so that the groups $E^D(\mathbb{Q})$ have rank 0. We therefore recall the known results about the p -part of the BSD formula for rank 0 curves.

In the theorem below we summarize the already known results on the Birch and Swinnerton-Dyer conjecture for both ordinary and supersingular elliptic curves of analytic rank zero. The inequality of part (i) of the theorem is a consequence of Kato’s groundbreaking work on an Euler system for elliptic curves (see [39, Thm.4.8]). The equality of part (ii) for the ordinary case is proved in [46, Thm.2], [45, Thm.C] as a consequence of the proof Iwasawa main conjecture for GL_2 , and that of part (iii) for the supersingular case is a consequence of the proof of Kobayashi’s main conjecture [54, Cor.4.8].

⁷If E has Weierstrass equation $y^2 = x^3 + Ax + B$, then the \mathcal{K} -twist of E is the curve E^D/\mathbb{Q} having Weierstrass equation $Dy^2 = x^3 + Ax + B$. If f is the newform associated with E , then the newform associated with E^D is just the newform $f_{\mathcal{K}}$ associated with the twist of f by the quadratic character $\chi_{\mathcal{K}}$ of \mathcal{K} .

Theorem 7.2.1. *Let \mathcal{E}/\mathbb{Q} be an elliptic curve with good or multiplicative reduction at the odd prime p and suppose that $\bar{\rho}_{\mathcal{E},p}: \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{Aut}(\mathcal{E}[p])$ is irreducible. Suppose $L(\mathcal{E}, 1) \neq 0$.*

(i) *One has*

$$(7.2.a) \quad \text{ord}_p(\#\text{III}(\mathcal{E}/\mathbb{Q})[p^\infty]) \leq \text{ord}_p\left(\frac{L(\mathcal{E}/\mathbb{Q}, 1)}{\Omega_{\mathcal{E}} \cdot \prod_{\ell} c_{\ell}(\mathcal{E})}\right).$$

(ii) *If \mathcal{E} has good ordinary or multiplicative reduction at p and there exists a prime q of multiplicative reduction for E at which the representation $\bar{\rho}_{\mathcal{E},p}$ is ramified, then*

$$(7.2.b) \quad \text{ord}_p(\#\text{III}(\mathcal{E}/\mathbb{Q})[p^\infty]) = \text{ord}_p\left(\frac{L(\mathcal{E}/\mathbb{Q}, 1)}{\Omega_{\mathcal{E}} \cdot \prod_{\ell} c_{\ell}(\mathcal{E})}\right).$$

(iii) *If \mathcal{E} is semistable or a twist of a semistable elliptic curve by a quadratic character that is unramified at the primes dividing the conductor of the semistable curve and if \mathcal{E} has supersingular reduction at p with $a_p(\mathcal{E}) = 0$, then*

$$(7.2.c) \quad \text{ord}_p(\#\text{III}(\mathcal{E}/\mathbb{Q})[p^\infty]) = \text{ord}_p\left(\frac{L(\mathcal{E}/\mathbb{Q}, 1)}{\Omega_{\mathcal{E}} \cdot \prod_{\ell} c_{\ell}(\mathcal{E})}\right).$$

Remark 7.2.2. Note that the condition that $a_p(\mathcal{E}) = 0$ in part (iii) of this theorem is superfluous if $p \geq 5$.

Remark 7.2.3. Part (iii) of the above theorem is slightly more general than the result cited in [54], where the elliptic curve is assumed to be semistable. However, the same proof extends to the case of the quadratic twist of a semistable curve. The only reason for including the semistable assumption there was to avoid local triple product integrals for supercuspidal representations at split primes in [52], [53], which is excluded under the assumption of the above theorem. The results of Hsieh and Hung on non-vanishing (or non-vanishing modulo p) of L -values and vanishing of μ -invariants are also valid in the more general setting of the quadratic twist.

7.3. Comparison of Tamagawa numbers and periods for quadratic twists

We will derive both upper and lower bounds on $\#\text{III}(E/\mathbb{Q})[p^\infty]$ from corresponding bounds on $\#\text{III}(E/\mathcal{K})[p^\infty]$ for suitable choices of imaginary quadratic fields $\mathcal{K} = \mathbb{Q}(\sqrt{-D})$. In order to derive from this the exact upper and

lower bounds predicted by Conjecture 1.1.1, we recall here the relations between the Tamagawa numbers and periods of E over \mathcal{K} and the Tamagawa numbers and periods of E and its quadratic twist⁸ E^D . These are discussed in detail in [47].

7.3.1. Tamagawa numbers. We recall [47, Cor. 9.2] that

$$(7.3.a) \quad \text{ord}_p \left(\prod_w c_w(E/\mathcal{K}) \right) = \text{ord}_p \left(\prod_\ell c_\ell(E/\mathbb{Q}) \cdot \prod_\ell c_\ell(E^D/\mathbb{Q}) \right).$$

On the left-hand side w is running over finite places of the imaginary quadratic field $\mathcal{K} = \mathbb{Q}(\sqrt{D})$ of discriminant $D < 0$, and on the right-hand side ℓ is running over all primes. Here we have also used that E has good reduction at p and so has Tamagawa number 1 at any place dividing p .

7.3.2. Periods and comparisons. For the elliptic curve E/\mathbb{Q} , one defines its real period to be

$$\Omega_E = \int_{E(\mathbb{R})} |\omega|.$$

Here ω_E is a Néron differential (a \mathbb{Z} -basis of the module of differentials of the Néron model of E over \mathbb{Z}). If $f \in S_2(\Gamma_0(N))$ is the normalized cuspidal eigenform associated with E (that is, satisfying $L(f, s) = L(E, s)$) then, as explained in [47, §9.2], one also defines canonical periods $\Omega_f^+, \Omega_f^- \in \mathbb{C}^\times$; these are defined up to $\mathbb{Z}_{(p)}^\times$ -multiples (this can be refined to \mathbb{Z}^\times -multiples, but we do not need this here). Furthermore, as recalled in [47, §9.3], one also has the congruence (or Hida) period

$$\Omega_f^{\text{cong}} = \frac{\langle f, f \rangle}{\eta_f} \in \overline{\mathbb{Q}}_p^\times,$$

where $\langle f, f \rangle$ is the Petersson norm and η_f is the congruence number of f recalled in *loc. cit.*; to make sense of this definition we use our chosen isomorphism $\overline{\mathbb{Q}}_p \cong \mathbb{C}$. Recall that Ω_f^{cong} is only well-defined up to \mathbb{Z}_p^\times -multiple. We next recall the relations between these various periods.

⁸If E has Weierstrass equation $y^2 = x^3 + Ax + B$, then by E^D we mean the elliptic curve over \mathbb{Q} having Weierstrass equation $-Dy^2 = x^3 + Ax + B$. This is just the \mathcal{K} -twist of E . If f is the newform associated with E , then the newform associated with E^D is just the newform $f_{\mathcal{K}}$ associated with the twist of f by the quadratic character of \mathcal{K} .

Let $f_{\mathcal{K}}$ be the newform associated with the twist of f by the quadratic character of the imaginary quadratic field \mathcal{K} . It is explained in [45, §3.3] (see also [17, Prop. 3.1]) that

$$(7.3.b) \quad \Omega_E = -2\pi i \Omega_f^+ \quad \text{and} \quad \Omega_{E^D} = -2\pi i \Omega_{f_{\mathcal{K}}}^+,$$

up to $\mathbb{Z}_{(p)}^\times$ -multiples. By [47, Lem. 9.5] the congruence period can be chosen to satisfy

$$(7.3.c) \quad \Omega_f^{\text{cong}} = i(2\pi)^2 \Omega_f^+ \Omega_f^-.$$

Under the hypothesis that $\bar{\rho}_{E,p}$ is irreducible, it is shown in [47, Lem. 9.6] that if $p \nmid D$ then

$$(7.3.d) \quad \Omega_f^\pm = \sqrt{-D} \cdot \Omega_{f_{\mathcal{K}}}^\mp,$$

up to a \mathbb{Z}_p^\times -multiple. Note that the statement of *loc. cit.* omits the factor $\sqrt{-D}$ (which equals the Gauss sum $\tau(\chi_{\mathcal{K}})$ up to sign); this is because it is assumed there that p splits in \mathcal{K} (also assumed here) and so $\sqrt{-D} \in \mathbb{Z}_p^\times$. In particular, combining (7.3.b), (7.3.c), and (7.3.d) we find:

$$(7.3.e) \quad \Omega_f^{\text{cong}} = \sqrt{|D|} \cdot \Omega_E \Omega_{E^D}.$$

Remark 7.3.3. The comparison between the periods Ω_E of Ω_{E^D} of the elliptic curves and Ω_f^+ and $\Omega_{f_{\mathcal{K}}}^+$ is often done in terms of what is known as the Manin constants, as explained in [17, §3]. It is known by a result of Mazur that if $p \nmid 2ND$, then p does not divide either of the Manin constants (see, e.g., [26, §1]).

7.4. The final argument

Let $f \in S_2(\Gamma_0(N))$ be the Hecke eigenform associated to E . Then $(V, T, W) = (V_f, T_f, W_f) = (V_p E, T_p E, E[p^\infty])$, $\mathcal{O} = \mathbb{Z}_p$, and $\bar{V} \cong E[p]$. Note that there exists at least one prime $q \mid N$ such that the mod p representation $\bar{\rho}_{E,p}$ is ramified at q . If not, then Ribet’s level lowering theorem [41, Thm.1.1] yields a cusppform g of weight 2 and level 1 with mod p residual representation isomorphic to $\bar{\rho}_{E,p}$ (we apply Ribet’s theorem to remove, one-by-one, the primes dividing N). This is a contradiction as there are no cuspidal eigenforms of weight 2 and level 1. Let $N = q_1 \dots q_r$ with $q_1 = q$.

7.4.1. Lower bounds on $\#\text{III}(E/\mathbb{Q})[p^\infty]$. We first choose an auxiliary imaginary quadratic field $\mathcal{K}' = \mathbb{Q}(\sqrt{D'})$ of discriminant $D' < 0$ such that

- (a) N and \mathcal{K}' satisfy **(gen-H)**;
- (b) q is either inert or ramified in \mathcal{K}' ;
- (c) p splits in \mathcal{K}' ;
- (d) $L(E^{D'}, 1) \neq 0$.

It is easy to find \mathcal{K}' such that (a), (b) and (c) hold. Indeed, if $r \geq 2$ (i.e., N has at least two prime divisors), then we can even guarantee that **(H)** holds by requiring that q be inert in \mathcal{K}' . In the case where $N = q$ is prime, we take $N^- = 1$ and $N^+ = q$, which only satisfies **(gen-H)**. We note that for any \mathcal{K}' for which (a), (b), and (c) hold, the root number $w(E/\mathcal{K}')$ of E/\mathcal{K}' is -1 (cf. **(sign -1)**). As $w(E/\mathbb{Q}) = -1$ by hypothesis (this is a consequence of $\text{ord}_{s=1} L(E, s)$ being odd) and $w(E/\mathcal{K}') = w(E/\mathbb{Q})w(E^{D'}/\mathbb{Q})$, we have $w(E^{D'}) = +1$. As (a), (b), and (c) impose only finitely many congruence conditions on the discriminant of \mathcal{K}' , it then follows from a result of Friedberg and Hoffstein [14, Thm. B] that \mathcal{K}' can be chosen so that (d) also holds. Note that the condition (d) means that $\text{ord}_{s=1} L(E/\mathcal{K}', s) = 1$. In particular, by the work of Gross–Zagier and Kolyvagin we know that $E(\mathcal{K}')$ has rank one and that $\text{III}(E/\mathcal{K}')$ is finite.

To take a first step towards a lower bound on $\#\text{III}(E/\mathcal{K}') [p^\infty]$ we want to appeal to the Proposition 6.2.1. So we first check that the hypotheses of that proposition hold with $\mathcal{K} = \mathcal{K}'$. The conditions **(split)**, **(gen-H)**, **(good)**, and **(□-free)** either follow immediately from our hypotheses on E or from the choice of \mathcal{K}' (recall that in the case when $N = q$, we have used the work of Hsieh [24] in addition to Burungale’s result to include the case when q may not be coprime to the discriminant of \mathcal{K} .) The condition **(irred \mathcal{K})** is an easy consequence of the hypotheses that $\bar{\rho}_{E,p}$ is irreducible and that $\bar{\rho}_{E,p}$ is ramified at the prime $q = q_1 \parallel N$ (see [44, Lem. 2.8.1]). Finally, note that **(corank 1)** and **(sur)** also hold as $\text{rk } E(\mathcal{K}') = 1$ and $\#\text{III}(E/\mathcal{K}') [p^\infty] < \infty$ (cf. Section 3.5).

By Proposition 6.2.1 (with $\mathcal{K} = \mathcal{K}'$) we have

$$(7.4.a) \quad \text{ord}_p(L_p(f, 1)) \leq \text{ord}_p(\#\text{H}_{\mathcal{F}_{ac}}^1(\mathcal{K}', E[p^\infty]) \cdot C(E[p^\infty])).$$

Let $z_{\mathcal{K}'} = z_{\mathcal{K}'}^{N^+, N^-} \in E(\mathcal{K}')$ be the Heegner point defined in Section 4.3. (Note that the hypothesis **(irred \mathcal{K})** ensures that there are many good auxiliary primes ℓ_0 .) As the hypotheses of Proposition 5.1.7 are also clearly satisfied, the left-hand side of (7.4.a) is

$$\text{ord}_p(L_p(f, 1)) = 2 \cdot \text{ord}_p\left(\frac{1 + p - a_p}{p} \log_{\omega_E}(z_{\mathcal{K}'})\right).$$

As $L_p(f, 1) \neq 0$ (also by Proposition 6.2.1), this implies that $z_{\mathcal{K}'}$ has infinite order (of course, this is also a consequence of the general Gross–Zagier formula for $z_{\mathcal{K}'}$). Let

$$m_{\mathcal{K}'} = [E(\mathcal{K}') : \mathbb{Z} \cdot z_{\mathcal{K}'}].$$

This index is finite. The hypotheses of Section 3.5 are also all satisfied, so it follows from (3.5.d) and the definition of $C(E[p^\infty])$ that the right-hand side of (7.4.a) is

$$\begin{aligned} \text{ord}_p(\#\mathbb{H}_{\mathcal{F}_{\text{ac}}}^1(\mathcal{K}', E[p^\infty]) \cdot C(E[p^\infty])) &= \text{ord}_p(\#\text{III}(E/\mathcal{K}')) - 2 \cdot \text{ord}_p(m_{\mathcal{K}'}) \\ &\quad + 2 \cdot \text{ord}_p\left(\frac{1+p-a_p}{p} \log_{\omega_E}(z_{\mathcal{K}'})\right) \\ &\quad + \text{ord}_p\left(\prod_{w|N^+} c_w(E/\mathcal{K}')\right). \end{aligned}$$

We then conclude from all this that

$$(7.4.b) \quad \text{ord}_p(\#\text{III}(E/\mathcal{K}') [p^\infty]) \geq 2 \cdot \text{ord}_p(m_{\mathcal{K}'}) - \text{ord}_p\left(\prod_{w|N^+} c_w(E/\mathcal{K}')\right).$$

To pass from the inequality (7.4.b) to one involving the derivative $L'(E/\mathcal{K}', 1)$ we use the variant of the Gross–Zagier formula for the Heegner point⁹ $z_{\mathcal{K}'}$ [58, p. 245]: up to a unit in \mathbb{Z}_p^\times ,

$$\sqrt{|D'|} \frac{L'(E/\mathcal{K}', 1)}{\Omega_f^{\text{cong}}} = \frac{\delta(N, 1)}{\delta(N^+, N^-)} \frac{\langle z_{\mathcal{K}'}, z_{\mathcal{K}'} \rangle_{NT}}{c_E^2},$$

where $c_E \in \mathbb{Z}$ is the Manin constant of E (so $p \nmid c_E$ in this case; see Remark 7.3.3) and $\delta(N, 1)$, $\delta(N^+, N^-)$ are defined in *loc. cit.* In particular, as explained on the same page of *loc. cit.*,

$$\delta_{N^+, N^-} := \frac{\delta(N, 1)}{\delta(N^+, N^-)} = \prod_{\ell|N^-} c_\ell(E/\mathcal{K}')$$

⁹Though stated in terms of $z_{\mathcal{K}'}$ in [58], the formula in *loc. cit.* is a special case of a formula in [10], which is expressed in terms of a ‘Heegner point’ defined using the map $1/m \cdot \tilde{\iota}_{N^+, N^-}$ from (4.2.e) in place of ι_{N^+, N^-} . However, it is clear from (4.2.f) that replacing this point with $z_{\mathcal{K}'}$ only changes the formula by a p -adic unit.

up to a unit in \mathbb{Z}_p^\times . We can then rewrite the Gross–Zagier formula for $z_{\mathcal{K}'}$ as an equality up to p -adic unit:

$$(7.4.c) \quad \frac{L'(E, 1)}{\Omega_E \cdot \text{Reg}(E/\mathbb{Q})} \cdot \frac{L(E^{D'}, 1)}{\Omega_{E^{D'}}} = m_{\mathcal{K}'}^2 \cdot \prod_{\ell|N^-} c_\ell(E/\mathcal{K}').$$

Here we have used that $\langle z_{\mathcal{K}'}, z_{\mathcal{K}'} \rangle_{NT} = m_{\mathcal{K}'} \text{Reg}(E/\mathcal{K}')$, $\text{Reg}(E/\mathcal{K}') = \text{Reg}(E/\mathbb{Q})$ (as $E^{D'}(\mathbb{Q})$ is finite), $L'(E/\mathcal{K}') = L'(E, 1)L(E^{D'}, 1)$, and the period relation (7.3.e). From (7.4.c) we obtain

$$2 \cdot \text{ord}_p(m_{\mathcal{K}'}) = \text{ord}_p \left(\frac{L'(E, 1)}{\Omega_E \cdot \text{Reg}(E/\mathbb{Q})} \cdot \frac{L(E^{D'}, 1)}{\Omega_{E^{D'}}} \right) - \text{ord}_p \left(\prod_{\ell|N^-} c_\ell(E/\mathcal{K}') \right).$$

Combining this with (7.4.b) and (7.3.a) (with $\mathcal{K} = \mathcal{K}'$) we obtain

$$\begin{aligned} & \text{ord}_p(\#\text{III}(E/\mathcal{K}') [p^\infty]) \\ & \geq \text{ord}_p \left(\frac{L'(E, 1)}{\Omega_E \cdot \text{Reg}(E/\mathbb{Q}) \prod_\ell c_\ell(E/\mathbb{Q})} \cdot \frac{L(E^{D'}, 1)}{\Omega_{E^{D'}} \prod_\ell c_\ell(E^{D'}/\mathbb{Q})} \right). \end{aligned}$$

As $\text{III}(E/\mathcal{K}') [p^\infty] \cong \text{III}(E/\mathbb{Q}) [p^\infty] \oplus \text{III}(E^{D'}/\mathbb{Q}) [p^\infty]$, from the above lower bound on $\text{ord}_p(\#\text{III}(E/\mathcal{K}') [p^\infty])$ and Theorem 7.2.1(i) (really (7.2.a) for $\mathcal{E} = E^{D'}$) we conclude that

$$(7.4.d) \quad \text{ord}_p(\#\text{III}(E/\mathbb{Q}) [p^\infty]) \geq \text{ord}_p \left(\frac{L'(E, 1)}{\Omega_E \cdot \text{Reg}(E/\mathbb{Q}) \prod_\ell c_\ell(E/\mathbb{Q})} \right).$$

That is, we have proved the exact conjectured lower bound on $\#\text{III}(E/\mathbb{Q}) [p^\infty]$.

7.4.2. Upper bounds on $\#\text{III}(E/\mathbb{Q}) [p^\infty]$. Recall that $N = q_1 \cdots q_r$ with $q_1 = q$ such that $p \nmid c_q(E/\mathbb{Q})$. If r is odd, let $N^+ = q_1$ and $N^- = N/q_1$. If r is even, let $N^+ = 1$ and $N^- = N$. We choose a second auxiliary imaginary quadratic field $\mathbb{Q}(\sqrt{D''})$ of discriminant $D'' < 0$ such that

- (a) the primes dividing N^+ split in \mathcal{K}'' ;
- (b) the primes dividing N^- are all inert in \mathcal{K}'' ;
- (c) p splits in \mathcal{K}'' ;
- (d) $L(E^{D''}, 1) \neq 0$.

Note that (H) holds for N and any \mathcal{K}'' satisfying (a), (b), and (c). As with the choice of \mathcal{K}' above, the root number of the quadratic twist $E^{D''}$ is $+1$ and the result of Friedberg and Hoffstein ensures that \mathcal{K}'' can be chosen so that (d) also holds.

Note that by (d) we have $\text{ord}_{s=1} L(E/\mathcal{K}'', s) = 1$. Let $z_{\mathcal{K}''} = z_{\mathcal{K}'', N^+, N^-} \in E(\mathcal{K}'')$ be the Heegner point defined in Section 4.3 and let $m_{\mathcal{K}''} = [E(\mathcal{K}'') : \mathbb{Z} \cdot z_{\mathcal{K}''}]$. From Theorem 4.4.1 we obtain

$$\text{ord}_p(\#\text{III}(E/\mathcal{K}'')[p^\infty]) \leq 2 \cdot \text{ord}_p(m_{\mathcal{K}''}).$$

From the Gross–Zagier formula for $z_{\mathcal{K}''}$ we have, just as we did for $z_{\mathcal{K}'}$, that

$$2 \cdot \text{ord}_p(m_{\mathcal{K}''}) = \text{ord}_p\left(\frac{L'(E, 1)}{\Omega_E \cdot \text{Reg}(E/\mathbb{Q})} \cdot \frac{L(E^{D''}, 1)}{\Omega_{E^{D''}}}\right) - \text{ord}_p\left(\prod_{\ell|N^-} c_\ell(E/\mathcal{K}'')\right).$$

For our choice of \mathcal{K}'' there are no $w \mid N^+$ such that $p \mid c_w(E/\mathcal{K}'')$, and so the product on the right-hand side can be replaced by a product over all w . Combining the above equality with the preceding inequality and appealing to (7.3.a) (for $\mathcal{K} = \mathcal{K}''$) we get

$$\begin{aligned} &\text{ord}_p(\#\text{III}(E/\mathcal{K}'')[p^\infty]) \\ &\leq \text{ord}_p\left(\frac{L'(E, 1)}{\Omega_E \cdot \text{Reg}(E/\mathbb{Q}) \prod_\ell c_\ell(E/\mathbb{Q})} \cdot \frac{L(E^{D''}, 1)}{\Omega_{E^{D''}} \prod_\ell c_\ell(E^{D''}/\mathbb{Q})}\right) \end{aligned}$$

Appealing to part (ii) or (iii) of Theorem 7.2.1 (for $\mathcal{E} = E^{D''}$) then yields

$$(7.4.e) \quad \text{ord}_p(\#\text{III}(E/\mathbb{Q})[p^\infty]) \leq \text{ord}_p\left(\frac{L'(E, 1)}{\Omega_E \cdot \text{Reg}(E/\mathbb{Q}) \prod_\ell c_\ell(E/\mathbb{Q})}\right).$$

That is, we have proved the exact conjectured upper bound on $\#\text{III}(E/\mathbb{Q})[p^\infty]$.

7.4.3. The final step: equality. Combining (7.4.d) and (7.4.e) gives

$$\text{ord}_p(\#\text{III}(E/\mathbb{Q})[p^\infty]) = \text{ord}_p\left(\frac{L'(E, 1)}{\Omega_E \cdot \text{Reg}(E/\mathbb{Q}) \prod_\ell c_\ell(E/\mathbb{Q})}\right),$$

proving Theorem 1.2.1.

7.4.4. Some remarks on the hypotheses in Theorem 1.2.1. We make a few comments on how the various hypotheses on Theorem 1.2.1 intervene in its proof and some remarks on possible generalizations.

- (i) The requirement that N be square-free is made in [7] and so appears as a hypothesis of Proposition 5.1.6. However, this condition can likely be dropped in light of the main results of [32]. The formulas in the latter are not as explicit as the result in [7] but can be made so just as the general Gross–Zagier formula is made explicit in [10].
- (ii) The requirement that N be square-free is also made in [52] and [54], but as we have already indicated (see Remark 7.2.3) this can be replaced with the requirement that the cuspidal automorphic representation $\pi = \otimes_{\ell \leq \infty} \pi_\ell$ associated with E is either a principal series or a Steinberg representation at each $\ell \mid N$. Further relaxing of this conditions requires a better understanding of certain local triple product integrals.
- (iii) If $p = 3$ and E has supersingular reduction at p , then we have required that $a_p(E) = 0$. This is only because the same hypothesis is made in [54], and so the p -part of the BSD formula in the rank 0 case (needed for $L(E^{D''}, 1)$ in the argument deducing the exact upper bound) is only known for supersingular p when $a_p(E) = 0$.
- (iv) As much as possible, we have worked in the context of the Selmer groups of a general newform $f \in S_2(\Gamma_0(N))$ of weight 2 and trivial character. The ultimate restriction to the case of an elliptic curve is made for two reasons: (1) the lack of a precise reference for the upper-bound on $\#\text{III}(A_f/\mathcal{K})[\mathfrak{p}^\infty]$ coming from the Euler system of Heegner points (the generalization of Theorem 4.4.1), and (2) the lack of a general result about the \mathfrak{p} -part of the special value $L(f_{\mathcal{K}}, 1)/2\pi i \Omega_{f_{\mathcal{K}}}^+$ (when $L(f_{\mathcal{K}}, 1) \neq 0$) when f is not ordinary at \mathfrak{p} . We expect that both of these issues will be addressed in forthcoming work.
- (v) The condition that p be a prime of good reduction can likely be relaxed to at least a prime of multiplicative reduction. The rank 0 special value formulas are proved, for example, in [45], and the results of [11] and [32] allow p to be a prime of multiplicative reduction.
- (vi) That p is odd is, of course, an essential hypothesis of many of the results used in the course of our proof.

Acknowledgements

We thank Ernest H. Brooks and Francesc Castella for a careful reading of an earlier draft of this paper and for various helpful discussions. We are grateful to Christophe Cornut for his interest and multiple useful conversations

on the problem. Finally, we are thankful to the anonymous referee for the numerous helpful remarks. The second named author (C.S.) gratefully acknowledges the hospitality of the California Institute of Technology, where part of this work was carried out during an extended visit in 2014.

References

- [1] A. Abbes and E. Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires*, *Compositio Math.* **103** (1996), no. 3, 269–286.
- [2] A. Berti, M. Bertolini, and R. Venerucci, *Congruences between modular forms and the Birch and Swinnerton-Dyer conjecture*, preprint (2015).
- [3] M. Bertolini, H. Darmon, and K. Prasanna, *Generalized Heegner cycles and p -adic Rankin L -series*, *Duke Math. J.* **162** (2013), no. 6, 1033–1148.
- [4] B. J. Birch, *Elliptic curves over \mathbf{Q} : A progress report*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), Amer. Math. Soc., Providence, R.I., 1971, pp. 396–400.
- [5] S. Bloch and K. 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] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990. [MR91i:14034](#)
- [7] H. Brooks, *Shimura curves and special values of p -adic l -functions*, to appear in *Intl. Math. Res. Notices* (2014).
- [8] A. Burungale, *On the non-triviality of generalized Heegner cycles modulo p , II: Shimura curves*, preprint (2014).
- [9] K. Buzzard, *Integral models of certain Shimura curves*, *Duke Math. J.* **87** (1997), no. 3, 591–612.
- [10] L. Cai, J. Shu, and Y. Tian, *Explicit Gross-Zagier and Waldspurger formulae*, *Algebra Number Theory* **8** (2014), no. 10, 2523–2572.
- [11] F. Castella, *On the exceptional specializations of big Heegner points*, preprint (2015).

- [12] C.-L. Chai, B. Conrad, and F. Oort, *Complex multiplication and lifting problems*, Mathematical Surveys and Monographs, vol. 195, American Mathematical Society, Providence, RI, 2014.
- [13] J.-M. Fontaine and B. Mazur, *Geometric Galois representations*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995, pp. 41–78.
- [14] S. Friedberg and J. Hoffstein, *Nonvanishing theorems for automorphic L -functions on $GL(2)$* , Ann. of Math. (2) **142** (1995), no. 2, 385–423.
- [15] R. Greenberg, *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.
- [16] R. Greenberg, *Iwasawa theory for elliptic curves*, Arithmetic theory of elliptic curves (Cetraro, 1997), Lecture Notes in Math., vol. 1716, Springer, Berlin, 1999, pp. 51–144.
- [17] R. Greenberg and V. Vatsal, *On the Iwasawa invariants of elliptic curves*, Invent. Math. **142** (2000), no. 1, 17–63.
- [18] B. Gross and D. Zagier, *Heegner points and derivatives of L -series*, Invent. Math. **84** (1986), no. 2, 225–320.
- [19] B. H. Gross, *Kolyvagin's work on modular elliptic curves, L -functions and arithmetic* (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.
- [20] K. Hashimoto, *Explicit form of quaternion modular embeddings*, Osaka J. Math. **32** (1995), no. 3, 533–546.
- [21] D. Helm, *On maps between modular Jacobians and Jacobians of Shimura curves*, Israel J. Math. **160** (2007), 61–117.
- [22] H. 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.
- [23] B. Howard, *The Heegner point Kolyvagin system*, Compos. Math. **140** (2004), no. 6, 1439–1472.
- [24] M.-L. Hsieh, *Special values of anticyclotomic Rankin-Selberg L -functions*, Doc. Math. **19** (2014), 709–767.
- [25] H. Jacquet and R. P. Langlands, *Automorphic forms on $GL(2)$* , Springer-Verlag, Berlin, 1970, Lecture Notes in Mathematics, Vol. 114.

- [26] D. Jetchev, *Global divisibility of Heegner points and Tamagawa numbers*, Compos. Math. **144** (2008), no. 4, 811–826.
- [27] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Princeton University Press, Princeton, N.J., 1985.
- [28] S. Kobayashi, *The p -adic Gross-Zagier formula for elliptic curves at supersingular primes*, Invent. Math. **191** (2013), no. 3, 527–629.
- [29] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.
- [30] V. A. Kolyvagin, *On the structure of Selmer groups*, Math. Ann. **291** (1991), no. 2, 253–259.
- [31] V. A. Kolyvagin, *On the structure of Shafarevich-Tate groups*, Algebraic geometry (Chicago, IL, 1989), Springer, Berlin, 1991, pp. 94–121.
- [32] Y. Liu, S. Zhang, and W. Zhang, *On p -adic Waldspurger formula*, preprint (2013).
- [33] B. Mazur and K. Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **168** (2004), no. 799, viii+96.
- [34] W. G. McCallum, *On the Shafarevich-Tate group of the Jacobian of a quotient of a Fermat curve*, Invent. Math. **53** (1988), no. 3, 637–666.
- [35] J. S. Milne, *Arithmetic duality theorems*, Academic Press Inc., Boston, Mass., 1986.
- [36] A. Mori, *Power series expansions of modular forms and their interpolation properties*, Int. J. Number Theory **7** (2011), no. 2, 529–577.
- [37] J. Nekovář, *The Euler system method for CM points on Shimura curves, L -functions and Galois representations*, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, pp. 471–547.
- [38] B. Perrin-Riou, *Fonctions L p -adiques, théorie d’Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), no. 4, 399–456.
- [39] Bernadette Perrin-Riou, *Arithmétique des courbes elliptiques à réduction supersingulière en p* , Experiment. Math. **12** (2003), no. 2, 155–186.
- [40] K. Ribet and S. Takahashi, *Parametrizations of elliptic curves by Shimura curves and by classical modular curves*, Proc. Nat. Acad. Sci.

- U.S.A. **94** (1997), no. 21, 11110–11114, Elliptic curves and modular forms (Washington, DC, 1996).
- [41] K. A. Ribet, *On modular representations of $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476.
- [42] K. Rubin, *Euler Systems*, Princeton University Press, Spring 2000, Annals of Mathematics Studies **147**.
- [43] T. Saito, *Modular forms and p -adic Hodge theory*, Invent. Math. **129** (1997), 607–620.
- [44] C. Skinner, *A converse to a theorem of Gross, Zagier, and Kolyvagin*, preprint (2014).
- [45] C. Skinner, *Multiplicative reduction and the cyclotomic main conjecture for \mathbf{GL}_2* , preprint (2014).
- [46] C. Skinner and E. Urban, *The main conjecture for \mathbf{GL}_2* , to appear in Invent. Math. (2013).
- [47] C. Skinner and W. Zhang, *Indivisibility of heegner points in the multiplicative case*, preprint (2014).
- [48] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 288–295. [MR31 #168](#)
- [49] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1965/66, pp. Exp. No. 306, 415–440.
- [50] J. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206. [MR54 #7380](#)
- [51] R. Taylor and T. Yoshida, *Compatibility of local and global Langlands correspondences*, J. Amer. Math. Soc. **20** (2007), no. 2, 467–493.
- [52] X. Wan, *Iwasawa main conjecture for Rankin–Selberg p -adic L -functions*, preprint (2013).
- [53] X. Wan, *Iwasawa main conjecture for Rankin–Selberg p -adic l -functions: non-ordinary case*, preprint (2014).
- [54] X. Wan, *Iwasawa main conjecture for supersingular elliptic curves*, preprint (2014).

- [55] X. Yuan, S.-W. Zhang, and W. Zhang, *The Gross-Zagier formula on Shimura curves*, Annals of Mathematics Studies, vol. 184, Princeton University Press, Princeton, NJ, 2013.
- [56] S. Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2) **153** (2001), no. 1, 27–147.
- [57] S. W. Zhang, *Gross-Zagier formula for GL_2* , Asian J. Math. **5** (2001), no. 2, 183–290.
- [58] W. Zhang, *Selmer groups and divisibility of Heegner points*, Cambridge J. Math. **2** (2014), no. 2, 191–253.

DIMITAR JETCHEV
ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE
FSB MATHGEOM GR-JET
BÂTIMENT MA C3 605
CH-1015 LAUSANNE
SWITZERLAND
E-mail address: dimitar.jetchev@epfl.ch

CHRISTOPHER SKINNER
DEPARTMENT OF MATHEMATICS
PRINCETON UNIVERSITY
FINE HALL, WASHINGTON ROAD
PRINCETON, NJ 08544-1000
USA
E-mail address: cmcls@princeton.edu

XIN WAN
MORNINGSIDE CENTER OF MATHEMATICS
ACADEMY OF MATHEMATICS AND SYSTEMS SCIENCE
CHINESE ACADEMY OF SCIENCE
BEIJING, 100190
CHINA
E-mail address: xw2295@math.columbia.edu

RECEIVED APRIL 24, 2017