Congruences for critical values of higher derivatives of twisted Hasse-Weil L-functions, III

Werner Bley and Daniel Macias Castillo

Abstract. Let A be an abelian variety defined over a number field k, let p be an odd prime number and let F/k be a cyclic extension of p-power degree. Under not-too-stringent hypotheses we give an interpretation of the p-component of the relevant case of the equivariant Tamagawa number conjecture in terms of integral congruence relations involving the evaluation on appropriate points of A of the $\mathrm{Gal}(F/k)$-valued height pairing of Mazur and Tate. We then discuss the numerical computation of this pairing, and in particular obtain the first numerical verifications of this conjecture in situations in which the p-completion of the Mordell-Weil group of A over F is not a projective Galois module.

1. Introduction

Let A be an abelian variety defined over a number field k. The Birch and Swinnerton-Dyer conjecture for A over k (as extended to this setting by Tate) predicts a remarkable equality between the leading term $L^*(A,1)$ at $z=1$ of the Hasse-Weil L-series $L(A,z)$ of A over k (assuming that this function has a suitable meromorphic continuation) and the key algebraic invariants of A over k.

Nevertheless, there are various natural contexts in which it seems likely that this equality does not encompass the full extent of the interplay between the leading terms $L^*(A,\psi,1)$ at $z=1$ of the twisted Hasse-Weil L-series $L(A,\psi,z)$, associated to A and to finite dimensional complex characters ψ of the absolute Galois group of k, and the algebraic invariants of A. For instance, building on a conjecture due to Deligne and Gross concerning the order of vanishing at $z=1$ of such functions one may, for a fixed character ψ, predict that a suitable normalisation of $L^*(A,\psi,1)$ is algebraic and generates an explicit fractional ideal inside any large enough number field. See [10, Prop. 7.3] for such explicit predictions.

However, even such conjectural formulas would not themselves account for any connections that might exist between the numbers $L^*(A,\psi,1)$ as ψ ranges over characters that are not necessarily in the same Galois orbit. In this direction, Mazur and Tate [24] have, in certain concrete settings and by building on the theory of modular symbols, predicted explicit congruence relations between the *values* $L(A,\psi,1)$ at $z=1$ of the functions $L(A,\psi,z)$. In addition, Darmon [17] has subsequently used the theory of Heegner points to formulate analogous predictions for the values $L'(A,\psi,1)$ at $z=1$ of the *first derivatives* $L'(A,\psi,z)$ of the functions $L(A,\psi,z)$.

Let F be a finite Galois extension of k. Then, in all cases, the congruence relations discussed in the previous paragraph, as ψ ranges over complex irreducible characters of $\mathrm{Gal}(F/k)$, involve the evaluation at suitable points of $A(k)$ of the canonical $\mathrm{Gal}(F/k)$-valued height pairings that had been previously constructed by Mazur and Tate [23] by using the geometrical theory of biextensions.

In recent work [10] of Burns and the second author, a completely general framework for the conjectural theory of integral congruence relations between the leading terms $L^*(A,\psi,1)$ has been developed, thereby extending and refining the aforementioned conjectures of Mazur and Tate and of Darmon. This framework relies on the formulation of a completely general 'refined conjecture of Birch and Swinnerton-Dyer type' (or 'refined BSD conjecture' in the sequel) for A and F/k, which is then shown to encode general families of integral congruence relations involving the Mazur-Tate pairing.

Fix F as above and set $G := \mathrm{Gal}(F/k)$. We let A_F denote the base change of A through F/k and consider $M_F := h^1(A_F)(1)$ as a motive over k with a natural action of the semisimple $\mathbb{Q}$-algebra $\mathbb{Q}[G]$.

It is then also shown in [10] that the refined BSD conjecture is equivalent to the equivariant Tamagawa number conjecture (or 'eTNC' in the sequel) for the pair $(M_F,\mathbb{Z}[G])$, as formulated by Burns and Flach [7]. In addition, both of these conjectures decompose naturally into 'p-components', one for each rational prime number p, and each such component is itself of interest.

For example, if A has good ordinary reduction at p, then the compatibility results proved by Burns and Venjakob [12] show that this p-component is (under certain hypotheses) a consequence of the main conjecture of non-commutative Iwasawa theory for A, as formulated by Coates et al. [16].

Assume now that p is a fixed odd prime and F/k a cyclic p-extension of degree p^n for some natural number n. In this note we will continue the study of the p-component of the eTNC that we begun in [6]. We recall that the main result of loc.cit. was the computation of an equivariant regulator under certain not-too-stringent conditions. Through this computation it was then possible to give a reformulation of this p-component which both was of theoretical interest and also made it amenable to providing partial numerical evidence.

For simplicity of the exposition, let us in the rest of this introduction assume that A is an elliptic curve. The computation of the equivariant regulator in [6] relied on the fact that, under suitable hypotheses, a representation-theoretic result due to Yakovlev [31] implies that the p-completion $A(F)_p := \mathbb{Z}_p \otimes_{\mathbb{Z}} A(F)$ of the Mordell-Weil group of A over F is a permutation $\mathbb{Z}_p[G]$-module. Explicitly speaking, this fact means that one may find points $P_{(H,j)} \in A(F^H)$, where H runs over all subgroups of G, with the

property that $\mathbb{Z}_p[G/H] \cdot P_{(H,j)}$ is a free $\mathbb{Z}_p[G/H]$-module of rank one and also that

$$A(F)_p = \bigoplus_{H \leq G} \bigoplus_{j=1}^{m_H} \mathbb{Z}_p[G/H] \cdot P_{(H,j)}$$

(for some set of non-negative integers $\{m_H : H \leq G\}$).

However, our formula for the equivariant regulator involved a choice of an integral matrix Φ, with entries in $\mathbb{Z}_p[G]$, which depended upon a canonical extension class in the Yoneda 2-extension group $\mathrm{Ext}^2_{\mathbb{Z}_p[G]}(\mathrm{Hom}_{\mathbb{Z}_p}(A(F)_p, \mathbb{Z}_p), A(F)_p)$ and was therefore not computable in any examples unless this group vanished. Given the above direct sum decomposition of $A(F)_p$, the vanishing of this group holds if and only if m_H is equal to zero for each subgroup $H \neq 1$, or equivalently, if and only if $A(F)_p$ is a free $\mathbb{Z}_p[G]$-module of the form $\bigoplus_{j=1}^{m_1} \mathbb{Z}_p[G] \cdot P_{(1,j)}$.

This limitation of our previous methods is consistent with those occurring in all existing verifications of p-components of the eTNC for any elliptic curves. Indeed, in the settings of the theoretical verifications obtained by the first author in [5], by Burns, Wuthrich and the second author in [11], or of the recent extensions of these results by Burns and the second author in [10], as well as of the numerical verifications carried out in [11, 3, 4] and in our previous article [6], a full verification of this conjecture was only ever achieved in situations which forced the $\mathbb{Z}_p[G]$-module $A(F)_p$ to be projective. On the other hand, even for $n = 1$ (meaning that the extension F/k has degree p), the result [10, Thm. 9.11] shows that the p-component of the eTNC (or refined BSD conjecture) encodes a family of congruence relations between the leading terms $L^*(A, \psi, 1)$ and certain 'Mazur-Tate regulators' (coming from the evaluation of Mazur-Tate height pairings) which are non-trivial unless $A(F)_p$ is projective.

This observation is consistent with our previously encountered difficulties and also justifies why, from the point of view of our approach, it is only interesting to consider components of the general conjectures at primes which divide the degree of the extension.

In this note we use a result of Burns and the second author [10, Thm. 10.3] to obtain an alternative computation of the equivariant regulator which is much better suited for the purpose of verifying 'non-projective' instances of the refined BSD conjecture.

To be a little more precise we note that, under our hypotheses, and for any subgroup H of G, the Mazur-Tate pairing for A considered over the sub-extension F/F^H of F/k gives a well defined pairing

$$\langle\, , \rangle^{\mathrm{MT}}_{F/F^H} : A(F^H)_p \otimes_{\mathbb{Z}_p} A(F^H)_p \to H \cong I_p(H)/I_p(H)^2.$$

Here $I_p(H)$ denotes the augmentation ideal in the group ring $\mathbb{Z}_p[H]$ and the isomorphism maps $g \in H$ to the class of $g - 1$.

Fix any choice of points as above and any generator σ of G. For any double-indices (H, j) and (J, i) with $H, J \neq 1$ and $H \leq J$, we let $\Psi_{(H,j),(J,i)}$ be any element of $\mathbb{Z}_p[G]$ which, in the group

$$\mathbb{Z}_p[G/H] \otimes_{\mathbb{Z}_p} I_p(H)/I_p(H)^2,$$

satisfies the equality

$$\Psi_{(H,j),(J,i)} \otimes (\sigma^{|G/H|} - 1) = \sum_{\gamma \in G/H} \big(\gamma \otimes \langle P_{(J,i)}, \gamma P_{(H,j)} \rangle^{\mathrm{MT}}_{F/F^H}\big).$$

For double-indices with $J < H$ we will let $\Psi_{(H,j),(J,i)}$ be any element of $\mathbb{Z}_p[G]$ which satisfies a straightforward variant of this equality. See (6) and Remark 2.3 below for more details.
We then show that any matrix Ψ obtained in this manner (by ordering all double-indices $(H,j),(J,i)$ lexicographically) is, independently of all of the above choices, a suitable replacement for the essentially inexplicit matrix Φ that occurred in the computation of the equivariant regulator in [6].
In the main result of this note, Theorem 2.1, we thus give a reformulation for the p-component of the refined BSD conjecture in terms of Mazur-Tate regulators obtained from considering natural components of the matrix Ψ. This is in particular a suitable extension to general n of the result [10, Thm. 9.11] of Burns and the second author.
As an application we are now able to obtain the first numerical verifications of the p-component of the refined BSD conjecture in situations in which the p-completed Mordell-Weil group $A(F)_p$ is not a projective $\mathbb{Z}_p[G]$-module. We emphasise again that there exists no other theoretical or numerical verification for this conjecture in such situations.
We shall give a detailed description, which we feel may be of some independent interest, of the methods that are appropriate to the numerical computation of Mazur-Tate pairings. We comment upon the results of our computations in Section 4.4. Here we also give a list of pairs $(A, F/k)$ for which we have numerically verified the conjecture, although this list is not exhaustive. See also the webpage of the first author for more details and the MAGMA implementation.

1.1. **General Notation.** For a finite abelian group Γ we set $\mathrm{Tr}_\Gamma := \sum_{\gamma\in\Gamma}\gamma \in \mathbb{Z}[\Gamma]$ and also $\widehat{\Gamma} := \mathrm{Hom}_{\mathbb{Z}}(\Gamma, \mathbb{C}^\times)$. We write $\check{\psi}$ for the contragrediant character of each $\psi \in \hat{\Gamma}$ and also write

$$e_\psi = \frac{1}{|\Gamma|}\sum_{\gamma\in\Gamma}\psi(\gamma)\gamma^{-1}$$

for the associated idempotent.
For any abelian group M we let M_{tor} denote its torsion subgroup. We also set $M_p := \mathbb{Z}_p \otimes_{\mathbb{Z}} M$. If M is finitely generated, then for a field extension E of $\mathbb{Q}$ we shall sometimes abbreviate $E\otimes_{\mathbb{Z}} M$ to $E\cdot M$. Finally, for any integer n we write $M[n]$ for the subgroup of n-torsion points of M.
For any $\mathbb{Z}_p[\Gamma]$-Module M we write M^* for the linear dual $\mathrm{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p)$, endowed with the natural contragredient action of Γ. Explicitly, for a homomorphism f and elements $m \in M$ and $\gamma \in \Gamma$, one has $(\gamma f)(m) = f(\gamma^{-1}m)$. If Δ is a subgroup of Γ, we write M_Δ for the module of Δ-coinvariants of M.
For any Galois extension of fields we abbreviate $\mathrm{Gal}(L/K)$ to $G_{L/K}$. We fix an algebraic closure K^c of K and abbreviate $G_{K^c/K}$ to G_K.
If A is an abelian variety defined over a number field k and L/k a finite extension, we write $A(L)$ for the Mordell-Weil group, $Ш(A_L)$ for the Tate-Shafarevich group of A over L and $Ш_p(A_L)$ for its p-primary part.

2. STATEMENT OF THE MAIN RESULT

In this section we state our standing hypotheses and, after defining all the relevant objects, state the main result of this article.

2.1. **The hypotheses.** Let A be an abelian variety of dimension d, defined over a number field k. Let p be an odd prime number and let F/k be a cyclic field extension of degree p^n, for some natural number n. We write A^t for the dual abelian variety.
As in [6, Sec. 2], we will assume the validity of the following list of hypotheses.

(a) $p \nmid |A(k)_{\mathrm{tor}}| \cdot |A^t(k)_{\mathrm{tor}}|$;
(b) p does not divide the Tamagawa number of A at any place of k at which it has bad reduction;
(c) A has good reduction at all p-adic places of k;
(d) p is unramified in $F/\mathbb{Q}$;
(e) no place of bad reduction of A is ramified in F/k;
(f) if a place v of k ramifies in F/k then no point of order p of the reduction of A is defined over the residue field of v;
(g) $Ш(A_F)$ is finite;
(h) $Ш_p(A_{F^H})$ vanishes for all non-trivial subgroups H of G;
(i) The group $H^1(\mathrm{Gal}(k(A[p^n])/k), A[p^n])$ vanishes.

Remark 2.1. The hypotheses (a)-(h) recover those in place throughout [6]. The full list of hypotheses also recovers those that are in place in [10, Thm. 9.9, Thm.9.11]. We refer the reader to [6, Rem. 2.1] or [10, Rem. 6.1] for a further discussion of these hypotheses.
The hypothesis (i) recovers Hypothesis 10.1 from [10] in our setting and will hence allow us to apply Theorem 10.3 of loc. cit.. We recall that it is widely satisfied. For instance, it holds whenever multiplication-by-'-1' belongs to the image of the canonical Galois representation $G_k \to \mathrm{Aut}_{\mathbb{F}_p}(A[p])$. In particular, if A is an elliptic curve then this hypothesis excludes only finitely many primes, by a result of Serre. Moreover, if A is an elliptic curve and k does not contain any p-th roots of unity, Lawson and Wuthrich have recently shown that hypothesis (i) is valid in all but certain exceptional cases that, in particular, all have $p \leq 11$ (see [21, Thm. 2, §6]).

Remark 2.2. It is possible, using computations in [10], to obtain a generalisation of our main result under a significantly weaker version of hypotheses (d) (that still ensures the surjectivity of the appropriate norm maps on Mordell-Weil groups).

Our main result will concern an 'equivariant regulator' $\mathrm{Reg}_{A,F/k,j}$ in $\mathbb{C}_p[G]^\times/\mathbb{Z}_p[G]^\times$ for each isomorphism $j : \mathbb{C} \cong \mathbb{C}_p$, which we now proceed to define. Throughout the construction of this element, we will always use j to implicitly identify $\widehat{G}$ with $\mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{C}_p^\times)$.

2.2. **Néron-Tate regulators.** For $0 \leq r \leq n$ we denote by J_r the subgroup of G of order p^{n-r} and set $F_r := F^{J_r}$ and $\Gamma_r := G/J_r$. Clearly, $[F_r : k] = |\Gamma_r| = p^r$.
Our hypotheses allow us to apply a result of Yakovlev [31] in order to restrict the Galois structure of the Mordell-Weil groups $A(F)_p$ and $A^t(F)_p$ as follows. For any natural number m we write $[m]$ for the set $\{1, \dots, m\}$.

By [6, Prop. 2.2 and (2.1)] we may and will fix a set of non-negative integers $\{m_r : 0 \leq r \leq n\}$ and subsets

$$\begin{aligned} \mathcal{P}_{(r)} &= \{P_{(r,j)} : j \in [m_r]\} \subseteq A(F_r), \\ \mathcal{P}^t_{(r)} &= \{P^t_{(r,j)} : j \in [m_r]\} \subseteq A^t(F_r) \end{aligned}$$

such that the $\mathbb{Z}_p[\Gamma_r]$-modules generated by each of the points $P_{(r,j)}$ and $P^t_{(r,j)}$ are free of rank one and there are direct sum decompositions of $\mathbb{Z}_p[G]$-modules

$$A(F)_p = \bigoplus_{r=0}^{n} \bigoplus_{j=1}^{m_r} \mathbb{Z}_p[\Gamma_r] \cdot P_{(r,j)} \quad \text{and} \quad A^t(F)_p = \bigoplus_{r=0}^{n} \bigoplus_{j=1}^{m_r} \mathbb{Z}_p[\Gamma_r] \cdot P^t_{(r,j)}. \tag{1}$$

We set

$$\mathcal{P} := \bigcup_{r=0}^{n} \mathcal{P}_{(r)}, \quad \mathcal{P}^t := \bigcup_{r=0}^{n} \mathcal{P}^t_{(r)}.$$

By ordering our fixed choice of points $\mathcal{P}$ and $\mathcal{P}^t$ lexicographically, we obtain a 'regulator matrix'

$$R^{\mathrm{NT}}_{A,F/k}(\mathcal{P}, \mathcal{P}^t) := \left(\sum_{g \in G} \langle g P^t_{(r,j)}, P_{(s,i)} \rangle_{A_F} \cdot g^{-1} \right)_{(r,j),(s,i)} \in M_N(\mathbb{R}[G])$$

with $N := \sum_{r=0}^{n} m_r$, and where $\langle -, - \rangle_{A_F}$ denotes the Néron-Tate height pairing for A over F.

For any matrix $X = (x_{(r,j),(s,i)})$ where the indices $\{(r,j) : 0 \leq r \leq n, j \in [m_r]\}$ are ordered lexicographically and for any $0 \leq t \leq n$, we set

$$X_t := (x_{(r,j),(s,i)})_{r,s \geq t}$$

and, given any matrix Y with entries in $\mathbb{C}[G]$, resp. $\mathbb{C}_p[G]$, and any $\psi \in \widehat{G}$, we write $\psi(Y)$ for the matrix with entries in $\mathbb{C}$, resp. $\mathbb{C}_p$, obtained after extending ψ to a function on $\mathbb{C}[G]$, resp. $\mathbb{C}_p[G]$, by linearity and then evaluating ψ at each entry of Y. For any $\psi \in \widehat{G}$ we define an integer t_ψ between 0 and n by the equality $\ker(\psi) = J_{t_\psi}$ and then set

$$\varepsilon_\psi(Y) := \det\left(\psi(Y)_{t_\psi}\right). \tag{2}$$

We now put

$$m_\psi := \sum_{r=t_\psi}^{n} (n-r) m_r$$

and define the ψ-component of the equivariant Néron-Tate regulator by

$$\mathrm{Reg}^{\mathrm{NT}}_\psi(\mathcal{P}, \mathcal{P}^t) := p^{-2m_\psi} \cdot \varepsilon_\psi\big(R^{\mathrm{NT}}_{A,F/k}(\mathcal{P}, \mathcal{P}^t)\big). \tag{3}$$

Each regulator term $\mathrm{Reg}^{\mathrm{NT}}_\psi(\mathcal{P}, \mathcal{P}^t)$ coincides with the element $\lambda_\psi(\mathcal{P}, \mathcal{P}^t)$ defined in [6, Def. 2.4].

We finally fix a generator σ of G and then define a non-zero complex number

$$\delta_\psi := \prod_{r=0}^{t_\psi - 1} \left(\psi(\sigma)^{p^r} - 1\right)^{m_r}. \tag{4}$$

2.3. **Mazur-Tate regulators.** For any $0 \leq r \leq n$ we recall that, under our given hypotheses, [10, Prop. 6.3(ii)] implies that every element of $A^t(F_r)_p$ and $A(F_r)_p$ is 'locally-normed'. Indeed, from this result one knows that for every finite prime w of F, the G-modules $\mathbb{Z}_p \otimes_{\mathbb{Z}} A^t(F_w)$ and $\mathbb{Z}_p \otimes_{\mathbb{Z}} A(F_w)$ are cohomologically-trivial and from this it follows easily that the p-completions of the subgroups of locally-normed elements in $A^t(F_r)$ and in $A(F_r)$ are equal to the full p-completions $A^t(F_r)_p$ and $A(F_r)_p$, respectively.
In particular, the construction of Mazur and Tate using the theory of biextensions gives well defined canonical height pairings

$$\langle\, , \rangle^{\mathrm{MT}}_{F/F_r} : A^t(F_r)_p \otimes_{\mathbb{Z}_p} A(F_r)_p \to J_r \cong I_p(J_r)/I_p(J_r)^2. \tag{5}$$

Here $I_p(J_r)$ denotes the augmentation ideal in the group ring $\mathbb{Z}_p[J_r]$ and the isomorphism maps $g \in J_r$ to the class of $g-1$.
In the sequel we also write ρ_r for the canonical projection $\mathbb{Z}_p[G] \to \mathbb{Z}_p[\Gamma_r]$. For any indices $0 \leq r, s \leq n-1$, any $j \in [m_r]$ and any $i \in [m_s]$, we set $\ell := \max(r,s)$ and then fix any elements $\Psi_{(r,j),(s,i)}$ of $\mathbb{Z}_p[G]$ which satisfy the equality

$$\rho_r(\Psi_{(r,j),(s,i)}) \otimes (\sigma^{p^\ell} - 1) = \sum_{\gamma \in \Gamma_r} \left(\gamma \otimes \langle P^t_{(s,i)}, \gamma P_{(r,j)} \rangle^{\mathrm{MT}}_{F/F_\ell} \right) \tag{6}$$

in

$$\mathbb{Z}_p[\Gamma_r] \otimes_{\mathbb{Z}_p} I_p(J_\ell)/I_p(J_\ell)^2.$$

It will be clear from Proposition 3.2 below that such elements always exist.

Remark 2.3. Let $\mathcal{I}_p(J_r)$ denote the ideal of $\mathbb{Z}_p[G]$ generated by $I_p(J_r)$. Then the inclusion $I_p(J_\ell) \subset I_p(J_r)$ induces a canonical inclusion

$$\mathbb{Z}_p[\Gamma_r] \otimes_{\mathbb{Z}_p} I_p(J_\ell)/I_p(J_\ell)^2 \hookrightarrow \mathbb{Z}_p[\Gamma_r] \otimes_{\mathbb{Z}_p} I_p(J_r)/I_p(J_r)^2 \cong \mathcal{I}_p(J_r)/\mathcal{I}_p(J_r)^2. \tag{7}$$

Here the isomorphism is canonical (see [8, Prop. 4.9]). It is then clear that the left-hand side of the equality (6) coincides with the class of $\Psi_{(r,j),(s,i)} \cdot (\sigma^{p^\ell} - 1)$ in the quotient $\mathcal{I}_p(J_r)/\mathcal{I}_p(J_r)^2$.

Using these choices we construct a matrix

$$\Psi(\mathcal{P}, \mathcal{P}^t) := \left(\begin{array}{c|c} \left(\Psi_{(r,j),(s,i)}\right)_{r,s<n} & \begin{array}{c} 0 \\ \vdots \\ 0 \end{array} \\ \hline 0 \quad \dots \quad 0 & I_{m_n} \end{array} \right) \tag{8}$$

with entries in $\mathbb{Z}_p[G]$. Here I_{m_n} denotes the identity $m_n \times m_n$ matrix.
For any $\psi \in \widehat{G}$, Lemma 3.4 below will show that the element

$$\sum_{\psi \in \widehat{G}} \varepsilon_\psi(\Psi(\mathcal{P}, \mathcal{P}^t)) \cdot e_\psi \tag{9}$$

of $\mathbb{C}_p[G]$ belongs to $\mathbb{C}_p[G]^\times$ (so in particular each term $\varepsilon_\psi(\Psi(\mathcal{P}, \mathcal{P}^t))$ is non-zero) and is independent, up to multiplication by an element of $\mathbb{Z}_p[G]^\times$, of the choices made in (6).

2.4. **The equivariant regulator.** We may now define our equivariant regulator. We again set $N := \sum_{r=0}^{n} m_r$.

Definition 2.4. For a fixed isomorphism $j\colon \mathbb{C} \to \mathbb{C}_p$, the class of

$$\mathrm{Reg}_{A,F/k,j} := (-1)^{N-m_n} \cdot \sum_{\psi \in \widehat{G}} \frac{j(\mathrm{Reg}_{\psi}^{\mathrm{NT}}(\mathcal{P},\mathcal{P}^t)\cdot \delta_{\psi})}{\varepsilon_{\psi}(\Psi(\mathcal{P},\mathcal{P}^t))} \cdot e_{\psi} \tag{10}$$

in $\mathbb{C}_p[G]^{\times}/\mathbb{Z}_p[G]^{\times}$ is the (p-primary) equivariant regulator associated to A and F/k.

The claims made in Section 2.3 imply that $\mathrm{Reg}_{A,F/k,j}$ is independent of the choices of $\mathcal{P}, \mathcal{P}^t, \sigma$ and the matrix $\Psi(\mathcal{P},\mathcal{P}^t)$. By abuse of terminology we will often refer to any choice of $\mathrm{Reg}_{A,F/k,j}$ in $\mathbb{C}_p[G]^{\times}$ itself as the equivariant regulator.

Remark 2.5. The results of Proposition 3.2 and Lemma 3.4 below combine to show that $\mathrm{Reg}_{A,F/k,j}$ is precisely the element

$$\sum_{\psi \in \hat{G}} \lambda_{\psi}(\mathcal{P},\mathcal{P}^t)\cdot \varepsilon_{\psi}(\Phi)\cdot \delta_{\psi}\cdot e_{\psi} \quad (\bmod \mathbb{Z}_p[G]^{\times})$$

which occurs in [6, Th. 2.9]. The main new insight is that the elements $\varepsilon_{\psi}(\Phi) \in \mathbb{C}_p^{\times}$ which depended upon an essentially unknown matrix $\Phi \in M_N(\mathbb{Z}_p[G])$ can be explicitly determined by (6).

2.5. **Statement of the result.** The refined Birch and Swinnerton-Dyer conjecture is an equality between analytic and algebraic invariants associated with A/k and F/k. We now briefly describe the analytic part refering the reader to [6, Sec. 2] or [10] for further details.
For each $\psi \in \widehat{G}$ we set

$$\mathcal{L}_{\psi}^{*} = \mathcal{L}_{A,F/k,\psi}^{*} := \frac{L_{S_{\mathrm{r}}}^{*}(A,\check{\psi},1)\cdot \tau^{*}(\mathbb{Q},\mathrm{ind}_{k}^{\mathbb{Q}}(\psi))^{d}}{\Omega_{A}^{\psi}\cdot w_{\psi}^{d}} \in \mathbb{C}^{\times},$$

where

- $L_{S_r}^{*}(A,\psi,1)$ is the leading term in the Taylor expansion at $z=1$ of the ψ-twisted Hasse-Weil L-function $L_{S_r}(A,\psi,z)$ of A, truncated by removing the Euler factors corresponding to the set S_{r} of primes of k which ramify in F/k;
- $\tau^{*}(\mathbb{Q},\mathrm{ind}_{k}^{\mathbb{Q}}(\psi))$ is a suitably modified global Galois-Gauss sum;
- $\Omega_{A}^{\psi}\cdot w_{\psi}^{d}$ is a (suitably normalised) product of periods.

We finally set

$$\mathcal{L}^{*} = \mathcal{L}_{A,F/k}^{*} := \sum_{\psi \in \widehat{G}} \mathcal{L}_{A,F/k,\psi}^{*} e_{\psi} \in \mathbb{C}[G]^{\times}$$

and note that the element $\mathcal{L}^{*}$ defined immediately above [10, Th. 6.5] specialises precisely to our definition.
Without any further mention we will always assume that the functions $L_{S_r}(A,\psi,z)$ have analytic continuation to $z=1$, so that the above term is well-defined. We also recall that Deligne and Gross have then predicted that these functions should vanish at $z=1$ exactly to order equal to the multiplicity with which the character ψ occurs in the representation $\mathbb{C}\otimes_{\mathbb{Z}} A^{t}(F)$ of G.

We now formulate the main result of this manuscript. For any $j : \mathbb{C} \cong \mathbb{C}_p$ we write j_* for the associated map $\mathbb{C}[G]^\times \to \mathbb{C}_p[G]^\times$.

Theorem 2.1. *Assume that the hypotheses (a)-(i) are valid. Let $\mathcal{P}$ and $\mathcal{P}^t$ be any choice of points such that (1) holds. Assume also that $Ш_p(A_F) = 0$.*
Then the p-component of the refined Birch and Swinnerton-Dyer conjecture is valid if and only if, for any $j : \mathbb{C} \cong \mathbb{C}_p$, the element

$$\frac{j_*\left(\mathcal{L}^*_{A,F/k}\right)}{\mathrm{Reg}_{A,F/k,j}} \tag{11}$$

belongs to $\mathbb{Z}_p[G]^\times$.

Remark 2.6. One may rephrase the condition that the element (11) belongs to $\mathbb{Z}_p[G]^\times$ in terms of explicit congruence relations in the augmentation filtration, as occurring in [22, Conj. 3.11].

The proof of Theorem 2.1 will occupy the next section.

3. The proof of Theorem 2.1

Under our listed hypotheses, Theorem 6.5 and Remark 6.6 in [10] reformulate the p-component of the refined BSD conjecture (denoted by $\mathrm{BSD}_p(A_{F/k})$ throughout loc. cit.) as an equality of the form

$$\delta_{G,p}\left(j_*\left(\mathcal{L}^*_{A,F/k}\right)\right) = \chi_{G,p}\left(\mathrm{SC}_p(A_{F/k}), h^j_{A,F}\right)$$

in the relative algebraic K-group $K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$. Here

$$\delta_{G,p} : \mathbb{C}_p[G]^\times \to K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$$

is the canonical 'extended boundary homomorphism' considered by Burns and Flach in [7, Sec. 4.2] while the right-hand side is the refined Euler characteristic of the pair $(\mathrm{SC}_p(A_{F/k}), h^j_{A,F})$. We thus also recall that $\mathrm{SC}_p(A_{F/k})$ is the 'classical p-adic Selmer complex' for A and F/k, as defined in Definition 2.3 of [10], while $h^j_{A,F}$ is the canonical trivialisation of this complex that is induced by the Néron-Tate height (see below).
At the outset we set $C := \mathrm{SC}_p(A_{F/k})$ and note that, under the hypotheses of Theorem 2.1, it is proved in [10, Prop. 6.3] that C is a perfect complex of $\mathbb{Z}_p[G]$-modules. In addition, there are canonical identifications

$$r_i : H^i(C) \cong \begin{cases} A^t(F)_p, & i = 1; \\ A(F)^*_p, & i = 2; \\ 0, & i \neq 1, 2. \end{cases} \tag{12}$$

The trivialisation

$$h^j_{A,F} : \mathbb{C}_p \otimes_{\mathbb{Z}_p} H^1(C) \cong \mathbb{C}_p \otimes_{\mathbb{Z}_p} H^2(C)$$

is then the canonical isomorphism induced by the Néron-Tate height pairing via (12) and j.
We now rephrase the validity of the p-component of the refined BSD conjecture as the vanishing of the element

$$\xi := \delta_{G,p}\left(j_*\left(\mathcal{L}^*_{A,F/k}\right)\right) - \chi_{G,p}(C, h^j_{A,F})$$

of $K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$.

Remark 3.1. For an abelian group G and a field E with $\mathbb{Q}_p \subseteq E \subseteq \mathbb{C}_p$ the relative algebraic K-group $K_0(\mathbb{Z}_p[G], E[G])$ is naturally isomorphic to $E[G]^\times/\mathbb{Z}_p[G]^\times$. Moreover, these isomorphisms are induced by $\delta_{G,p}$.

The first key step is to explicitly compute the second term that occurs in the definition of ξ and to do this we use the canonical identifications (12) to identify the complex C with a unique element $\delta_{A,F,p} = \delta_{C,r_1,r_2}$ of the Yoneda Ext-group $\mathrm{Ext}^2_{\mathbb{Z}_p[G]}(A(F)^*_p, A^t(F)_p)$.
For each pair (r,j) we define a dual element $P^*_{(r,j)}$ of $A(F)^*_p$ by setting, for any pair (s,i) and $\tau \in G$,

$$P^*_{(r,j)}(\tau P_{(s,i)}) := \begin{cases} 1, & \text{if } r = s, j = i \text{ and } \tau \in J_r; \\ 0, & \text{otherwise .} \end{cases} \tag{13}$$

By [6, Lem. 4.1] one then has

$$A(F)^*_p = \bigoplus_{(r,j)} \mathbb{Z}_p[\Gamma_r] P^*_{(r,j)}$$

with each summand isomorphic to $\mathbb{Z}_p[\Gamma_r]$. We fix a free $\mathbb{Z}_p[G]$-module

$$X := \bigoplus_{(r,j)} \mathbb{Z}_p[G] b_{(r,j)}$$

of rank $N = \sum_r m_r$ and consider the exact sequence

$$0 \to A^t(F)_p \xrightarrow{\iota} X \xrightarrow{\Theta} X \xrightarrow{\pi} A(F)^*_p \to 0, \tag{14}$$

where we set

$$\pi(b_{(r,j)}) := P^*_{(r,j)}, \quad \Theta(b_{(r,j)}) := (\sigma^{p^r} - 1) b_{(r,j)} \text{ and } \iota(P^t_{(r,j)}) := \mathrm{Tr}_{J_r}\, b_{(r,j)}.$$

This sequence defines a canonical isomorphism

$$\mathrm{Ext}^2_{\mathbb{Z}_p[G]}(A(F)^*_p, A^t(F)_p) \cong \mathrm{End}_{\mathbb{Z}_p[G]}(A^t(F)_p)/\iota_*(\mathrm{Hom}_{\mathbb{Z}_p[G]}(X, A^t(F)_p)) \tag{15}$$

where ι_* denotes composition with ι. Before proceeding to describe the map (15) let us note that it is bijective by the general result [20, Thm. IV.9.1].
For a given $\phi \in \mathrm{End}_{\mathbb{Z}_p[G]}(A^t(F)_p)$ we consider the push-out commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^t(F)_p & \xrightarrow{\iota} & X & \xrightarrow{\Theta} & X & \xrightarrow{\pi} & A(F)^*_p & \longrightarrow & 0 \\ & & {\scriptstyle\phi}\downarrow & & \downarrow & & \| & & \| & & \\ 0 & \longrightarrow & A^t(F)_p & \longrightarrow & X(\phi) & \longrightarrow & X & \xrightarrow{\pi} & A(F)^*_p & \longrightarrow & 0. \end{array} \tag{16}$$

In this diagram $X(\phi)$ is defined as the push-out of ι and ϕ and all the unlabeled arrows are the canonical maps induced by the push-out construction. Then the pre-image of ϕ under (15) is represented by the bottom row of this diagram.
Then, since C belongs to $D^{\mathrm{perf}}(\mathbb{Z}_p[G])$, the results of [6, Lem. 4.2 and Lem. 4.3] imply that there exists an automorphism ϕ of the $\mathbb{Z}_p[G]$-module $A^t(F)_p$ that represents the image of $\delta_{A,F,p}$ under (15) and also fixes the element $P^t_{(n,j)}$ for every j in $[m_n]$.

It follows that the exact sequence

$$0 \to A^t(F)_p \overset{\iota\circ\phi^{-1}}{\to} X \overset{\Theta}{\to} X \overset{\pi}{\to} A(F)_p^* \to 0 \tag{17}$$

is a representative of the extension class $\delta_{A,F,p}$.
In particular, for any choice of $\mathbb{C}_p[G]$-equivariant splittings

$$s_1 : \mathbb{C}_p \cdot X \to \mathbb{C}_p \cdot A^t(F)_p \oplus \mathbb{C}_p \cdot \mathrm{im}(\Theta) \tag{18}$$

and

$$s_2 : \mathbb{C}_p \cdot X \to \mathbb{C}_p \cdot A(F)_p^* \oplus \mathbb{C}_p \cdot \mathrm{im}(\Theta) \tag{19}$$

of the scalar extensions of the canonical exact sequences

$$0 \to A^t(F)_p \overset{\iota}{\to} X \overset{\Theta}{\to} \mathrm{im}(\Theta) \to 0$$

and

$$0 \to \mathrm{im}(\Theta) \to X \overset{\pi}{\to} A(F)_p^* \to 0,$$

an explicit computation of the refined Euler characteristic occurring in the definition of ξ implies that

(20)

$$\begin{aligned}
&-\chi_{G,p}(C, h^j_{A,F}) \\
&= -\delta_{G,p}(\det_{\mathbb{C}_p[G]}(s_2^{-1}\circ(h^j_{A,F}\oplus \mathrm{id}_{\mathbb{C}_p\cdot\mathrm{im}(\Theta)})\circ((\mathbb{C}_p\cdot\phi)\oplus \mathrm{id}_{\mathbb{C}_p\cdot\mathrm{im}(\Theta)})\circ s_1)) \\
&= -\delta_{G,p}(\det_{\mathbb{C}_p[G]}(s_2^{-1}\circ(h^j_{A,F}\oplus \mathrm{id}_{\mathbb{C}_p\cdot\mathrm{im}(\Theta)})\circ s_1\circ s_1^{-1}\circ((\mathbb{C}_p\cdot\phi)\oplus \mathrm{id}_{\mathbb{C}_p\cdot\mathrm{im}(\Theta)})\circ s_1)) \\
&= \delta_{G,p}(\det_{\mathbb{C}_p[G]}(s_1^{-1}\circ((h^j_{A,F})^{-1}\oplus \mathrm{id}_{\mathbb{C}_p\cdot\mathrm{im}(\Theta)})\circ s_2)) \\
&\qquad + \delta_{G,p}(\det_{\mathbb{C}_p[G]}(s_1^{-1}\circ((\mathbb{C}_p\cdot\phi^{-1})\oplus \mathrm{id}_{\mathbb{C}_p\cdot\mathrm{im}(\Theta)})\circ s_1)) \\
&= \delta_{G,p}(\det_{\mathbb{C}_p[G]}(s_1^{-1}\circ((h^j_{A,F})^{-1}\oplus \mathrm{id}_{\mathbb{C}_p\cdot\mathrm{im}(\Theta)})\circ s_2)) \\
&\qquad + \delta_{G,p}(\det_{\mathbb{Q}_p[G]}((\mathbb{Q}_p\cdot\phi^{-1})\oplus \mathrm{id}_{\mathbb{Q}_p\cdot\mathrm{im}(\Theta)})).
\end{aligned}$$

In addition, specialising the explicit computation of [6, Prop. 4.4] to the case $\Phi = \mathrm{id}_{A^t(F)_p}$ shows that

(21)

$$\det_{\mathbb{C}_p[G]}(s_1^{-1}\circ((h^j_{A,F})^{-1}\oplus \mathrm{id}_{\mathbb{C}_p\cdot\mathrm{im}(\Theta)})\circ s_2) = \left(\sum_{\psi\in\widehat{G}} j(\mathrm{Reg}_\psi^{\mathrm{NT}}(\mathcal{P},\mathcal{P}^t)\cdot\delta_\psi)\cdot e_\psi\right)^{-1}.$$

To compute the second term that occurs in the final equality of (20) we may and will fix any elements $\Lambda_{(r,j),(s,i)}$ of $\mathbb{Z}_p[G]$ with the property that

$$\phi^{-1}(P^t_{(s,i)}) = \sum_{(r,j)} \Lambda_{(r,j),(s,i)} P^t_{(r,j)}. \tag{22}$$

We thus obtain an invertible matrix

$$\Lambda = \Lambda(\mathcal{P},\mathcal{P}^t) := \left(\Lambda_{(r,j),(s,i)}\right)_{(r,j),(s,i)}$$

with entries $\Lambda_{(r,j),(s,i)}$ in $\mathbb{Z}_p[G]$ uniquely determined modulo the kernel of the canonical projection $\rho_r : \mathbb{Z}_p[G] \to \mathbb{Z}_p[\Gamma_r]$, which also has the form (8).

Recall the definition of $\varepsilon_\psi(\Lambda)$ in (2). The chosen properties of the representative ϕ of $\delta_{A,F,p}$ fixed above then imply that

$$\det_{\mathbb{Q}_p[G]}((\mathbb{Q}_p \cdot \phi^{-1}) \oplus \mathrm{id}_{\mathbb{Q}_p \cdot \mathrm{im}(\Theta)}) = \sum_{\psi \in \widehat{G}} \varepsilon_\psi(\Lambda) \cdot e_\psi. \tag{23}$$

The equalities (20), (21) and (23) now combine with the definition of ξ to imply that $\xi = \delta_{G,p}(\mathcal{L})$ with

$$\mathcal{L} := j_*(\mathcal{L}^*_{A,F/k}) \cdot \left(\sum_{\psi \in \widehat{G}} j(\mathrm{Reg}^{\mathrm{NT}}_\psi(\mathcal{P}, \mathcal{P}^t) \cdot \delta_\psi) \cdot e_\psi \right)^{-1} \cdot \left(\sum_{\psi \in \widehat{G}} \varepsilon_\psi(\Lambda) \cdot e_\psi \right).$$

By Remark 3.1 it thus follows that ξ vanishes if and only if $\mathcal{L}$ belongs to $\mathbb{Z}_p[G]^\times$ and hence the proof of Theorem 2.1 is completed by the proposition below.

Proposition 3.2. *For any $0 \leq r, s \leq n-1$ we set $\ell := \max(r,s)$. Then for any $j \in [m_r]$, any $i \in [m_s]$ and any elements $\Lambda_{(r,j),(s,i)}$ of $\mathbb{Z}_p[G]$ satisfying (22) one has*

$$\rho_r(\Lambda_{(r,j),(s,i)}) \otimes (\sigma^{p^\ell} - 1) = - \sum_{\gamma \in \Gamma_r} \left(\gamma \otimes \langle P^t_{(s,i)}, \gamma(P_{(r,j)}) \rangle^{\mathrm{MT}}_{F/F_\ell} \right)$$

in $\mathbb{Z}_p[\Gamma_r] \otimes_{\mathbb{Z}_p} I_p(J_\ell)/I_p(J_\ell)^2$.

Proof. We refer the reader to [10, App. B.2] for the construction of algebraic height pairings via Bockstein homomorphisms. It is proved in [10, Thm. 8.3] that

$$\langle\, , \rangle^{\mathrm{MT}}_{F/F_\ell} \colon A^t(F_\ell)_p \otimes_{\mathbb{Z}_p} A(F_\ell)_p \to I_p(J_\ell)/I_p(J_\ell)^2$$

coincides with the inverse of the pairing induced by

$$\beta_{A,F/F_\ell,p} \colon A^t(F_\ell)_p \to I_p(J_\ell)/I_p(J_\ell)^2 \otimes_{\mathbb{Z}_p} (A(F)^*_p)_{J_\ell} \to I_p(J_\ell)/I_p(J_\ell)^2 \otimes_{\mathbb{Z}_p} A(F_\ell)^*_p,$$

where the first arrow is the Bockstein homomorphism associated to the complex of $\mathbb{Z}_p[J_\ell]$-modules $\mathrm{SC}_p(A_{F/F_\ell})$ together with the canonical identifications (12), and the second arrow is induced by restriction to $A(F_\ell)_p$.
Now, it is immediately clear from their definitions in [10, Def. 2.3] that the complexes $\mathrm{SC}_p(A_{F/F_\ell})$ and $\mathrm{SC}_p(A_{F/k})$ are canonically isomorphic in $D(\mathbb{Z}_p[J_\ell])$ and furthermore that this isomorphism is compatible with the identifications (12). The complex $\mathrm{SC}_p(A_{F/F_\ell})$ may therefore be represented by the (restriction of scalars of) the exact sequence (17).
Now $\beta_{A,F/F_\ell,p}$ may be computed, through the representative (17), as the connecting homomorphism which arises when applying the snake lemma to the following commutative diagram (in which both rows and the third column are exact and the first

column is a complex)

$$\begin{array}{ccccccccc}
 & & & & & & & & A^t(F_\ell)_p \\
 & & & & & & & & \downarrow{\scriptstyle (\iota\circ\phi^{-1})^{J_\ell}} \\
0 & \longrightarrow & & I_p(J_\ell)\otimes_{\mathbb{Z}_p[J_\ell]} X & & \xrightarrow{\subseteq} & X & \xrightarrow{\mathrm{Tr}_{J_\ell}} & X^{J_\ell} & \longrightarrow & 0 \\
 & & & \downarrow{\scriptstyle \mathrm{id}\otimes_{\mathbb{Z}_p[J_\ell]}\Theta} & & & \downarrow{\scriptstyle \Theta} & & \downarrow{\scriptstyle \Theta^{J_\ell}} & & \\
0 & \longrightarrow & & I_p(J_\ell)\otimes_{\mathbb{Z}_p[J_\ell]} X & & \xrightarrow{\subseteq} & X & \xrightarrow{\mathrm{Tr}_{J_\ell}} & X^{J_\ell} & \longrightarrow & 0 \\
 & & & \downarrow{\scriptstyle (\mathrm{id}\otimes_{\mathbb{Z}_p[J_\ell]}\pi)_{J_\ell}} & & & & & & & \\
 & & & I_p(J_\ell)/I_p(J_\ell)^2\otimes_{\mathbb{Z}_p}(A(F)^*_p)_{J_\ell}. & & & & & & &
\end{array}$$

From (22) and the definition of ι we immediately derive

$$\iota(\phi^{-1}(P^t_{(s,i)})) = \iota\left(\sum_{(u,h)}\Lambda_{(u,h),(s,i)}P^t_{(u,h)}\right) = \sum_{(u,h)}\Lambda_{(u,h),(s,i)}\,\mathrm{Tr}_{J_u}(b_{(u,h)}).$$

By its definition in (13) one has $P^*_{(u,h)}(\gamma P_{(r,j)}) = 0$ whenever the pair (u,h) is different from (r,j). We thus find for any $\gamma\in\Gamma_r$ that

$$\begin{aligned}
-\langle P^t_{(s,i)},\gamma P_{(r,j)}\rangle^{\mathrm{MT}}_{F/F_\ell} &= \left((\mathrm{id}\otimes_{\mathbb{Z}_p[J_\ell]}\pi)_{J_\ell}\left(\Theta\left(\mathrm{Tr}_{J_r/J_\ell}(\Lambda_{(r,j),(s,i)}b_{(r,j)})\right)\right)\right)(\gamma P_{(r,j)}) \\
&= \left((\mathrm{id}\otimes_{\mathbb{Z}_p[J_\ell]}\pi)_{J_\ell}\left((\sigma^{p^r}-1)\,\mathrm{Tr}_{J_r/J_\ell}(\Lambda_{(r,j),(s,i)}b_{(r,j)})\right)\right)(\gamma P_{(r,j)}) \\
&= \left((\mathrm{id}\otimes_{\mathbb{Z}_p[J_\ell]}\pi)_{J_\ell}\left((\sigma^{p^\ell}-1)(\Lambda_{(r,j),(s,i)}b_{(r,j)})\right)\right)(\gamma P_{(r,j)}) \\
&= \left(\left((\sigma^{p^\ell}-1)+I_p(J_\ell)^2\right)\otimes(\Lambda_{(r,j),(s,i)}P^*_{(r,j)})\right)(\gamma P_{(r,j)}) \\
&= (\sigma^{p^\ell}-1)((\Lambda_{(r,j),(s,i)}P^*_{(r,j)})(\gamma P_{(r,j)})) + I_p(J_\ell)^2.
\end{aligned}$$

Here the first equality uses the fact that

$$\mathrm{Tr}_{J_r}(\Lambda_{(r,j),(s,i)}b_{(r,j)}) = \mathrm{Tr}_{J_\ell}(\mathrm{Tr}_{J_r/J_\ell}(\Lambda_{(r,j),(s,i)}b_{(r,j)})).$$

Now, if we write $\rho_r(\Lambda_{(r,j),(s,i)}) = \sum_{\gamma\in\Gamma_r}a_\gamma\gamma$ in $\mathbb{Z}_p[\Gamma_r]$, then the definition (13) of P^* implies

$$(\Lambda_{(r,j),(s,i)}P^*_{(r,j)})(\gamma P_{(r,j)}) = a_\gamma.$$

It therefore follows that the right-hand side of the claimed equality is equal to

$$\sum_{\gamma\in\Gamma_r}(\gamma\otimes(a_\gamma(\sigma^{p^\ell}-1))) = \sum_{\gamma\in\Gamma_r}((a_\gamma\gamma)\otimes(\sigma^{p^\ell}-1)) = \rho_r(\Lambda_{(r,j),(s,i)})\otimes(\sigma^{p^\ell}-1),$$

as required.

□

For the proof that all of our constructions are independent of any choices we made we will need the following general result which is straightforward to prove.

Lemma 3.3. *For any indices $0 \leq r \leq \ell \leq n$ and any elements λ and λ' of $\mathbb{Z}_p[G]$, one has that*

$$\rho_r(\lambda) \otimes (\sigma^{p^\ell} - 1) = \rho_r(\lambda') \otimes (\sigma^{p^\ell} - 1)$$

in $\mathbb{Z}_p[\Gamma_r] \otimes_{\mathbb{Z}_p} I_p(J_\ell)/I_p(J_\ell)^2$ if and only if $p^{\ell-r}(\lambda - \lambda')$ belongs to the ideal

$$(\sigma^{p^r} - 1) \cdot \mathbb{Z}_p[G] + \mathrm{Tr}_{J_r} \cdot \mathbb{Z}_p[G]$$

of $\mathbb{Z}_p[G]$.

We finally justify that all assertions in the statement of our main result were indeed well-defined.

Lemma 3.4. *For any elements $\Psi_{(r,j),(s,i)}$ of $\mathbb{Z}_p[G]$ satisfying the equalities (6), the sum (9) belongs to $\mathbb{C}_p[G]^\times$ and is independent, up to multiplication by an element of $\mathbb{Z}_p[G]^\times$, of the choices made.*

Proof. By Proposition 3.2, any collection of elements $-\Lambda_{(r,j),(s,i)}$ (for $r, s < n$) satisfying (22) also constitutes an appropriate choice satisfying the equalities (6). In addition, the sum

$$\sum_{\psi \in \widehat{G}} \varepsilon_\psi(-\Lambda) \cdot e_\psi$$

clearly belongs to $\mathbb{C}_p[G]^\times$. (In fact, by the argument of [6, Lem. 4.8], it also belongs to $\mathcal{M}^\times$, where $\mathcal{M}$ denotes the (unique) maximal $\mathbb{Z}_p$-order in $\mathbb{Q}_p[G]$.)
It is therefore enough to set $\Psi' := -\Lambda$, fix any collection of elements $\Psi_{(r,j),(s,i)}$ satisfying the equalities (6), and prove that the sum

$$\sum_{\psi \in \widehat{G}} \frac{\varepsilon_\psi(\Psi)}{\varepsilon_\psi(\Psi')} \cdot e_\psi$$

belongs to $\mathbb{Z}_p[G]^\times$.
The main step involved in proving this assertion is given by the following intermediate result.

Lemma 3.5. *The endomorphism ψ of $A^t(F)_p$ which maps a point $P^t_{(s,i)}$ to the sum*

$$\sum_{(r,j)} (\Psi_{(r,j),(s,i)} - \Psi'_{(r,j),(s,i)}) \cdot P^t_{(r,j)}$$

factors through the map $\iota : A^t(F)_p \to X$ occurring in the exact sequence (14).
In addition, if we define an endomorphism γ of $A^t(F)_p$ by setting

$$\gamma(P^t_{(s,i)}) := \sum_{(r,j)} \Psi_{(r,j),(s,i)} P^t_{(r,j)},$$

then γ is bijective.

Proof. By Lemma 3.3, for each pair $(r,j),(s,i)$ with $r, s < n$, there exist elements $\lambda_{(r,j),(s,i)}$ and $\mu_{(r,j),(s,i)}$ in $\mathbb{Z}_p[G]$ with the property that
(24)

$$\Psi_{(r,j),(s,i)} - \Psi'_{(r,j),(s,i)} = \begin{cases} (\sigma^{p^r} - 1) \cdot \lambda_{(r,j),(s,i)} + \mathrm{Tr}_{J_r} \cdot \mu_{(r,j),(s,i)}, & \text{if } r \geq s; \\ \big((\sigma^{p^r} - 1) \cdot \lambda_{(r,j),(s,i)} + \mathrm{Tr}_{J_r} \cdot \mu_{(r,j),(s,i)}\big) p^{r-s}, & \text{if } r < s. \end{cases}$$

For $r = n$ or $s = n$ we may simply take $\lambda_{(r,j),(s,i)}$ and $\mu_{(r,j),(s,i)}$ to be equal to 0 and still have these equalities.
Now since σ^{p^r} acts trivially on $P^t_{(r,j)}$ one thus has

$$\begin{aligned}\psi(P^t_{(s,i)}) &= \sum_{r\geq s} \mathrm{Tr}_{J_r}\cdot\mu_{(r,j),(s,i)}\cdot P^t_{(r,j)} + \sum_{r<s} p^{r-s}\,\mathrm{Tr}_{J_r}\cdot\mu_{(r,j),(s,i)}\cdot P^t_{(r,j)}\\ &= \sum_{r\geq s} \mathrm{Tr}_{J_r}\cdot\mu_{(r,j),(s,i)}\cdot P^t_{(r,j)} + \sum_{r<s} \mathrm{Tr}_{J_s}\cdot\mu_{(r,j),(s,i)}\cdot P^t_{(r,j)}. \qquad (25)\end{aligned}$$

In addition, J_s acts trivially both on $P^t_{(s,i)}$ and on the second summand of the above expression and therefore it must also act trivially on each term $\mathrm{Tr}_{J_r}\cdot\mu_{(r,j),(s,i)}\cdot P^t_{(r,j)}$ with $r \geq s$. Now, since $\mathbb{Z}_p[G]\cdot P^t_{(r,j)} = \mathbb{Z}_p[G/J_r]\cdot P^t_{(r,j)}$ is a free $\mathbb{Z}_p[G/J_r]$-module of rank one, this condition necessarily implies that Tr_{J_s/J_r} divides $\mu_{(r,j),(s,i)}$. We may therefore, for every indices with $r \geq s$, write $\mu_{(r,j),(s,i)} = \mathrm{Tr}_{J_s/J_r}\cdot\tilde{\mu}_{(r,j),(s,i)}$ for some element $\tilde{\mu}_{(r,j),(s,i)}$ of $\mathbb{Z}_p[G]$.
We now define a homomorphism $\alpha : X \to A^t(F)_p$ by setting

$$\alpha(b_{(s,i)}) := \sum_{r\geq s} \tilde{\mu}_{(r,j),(s,i)}\cdot P^t_{(r,j)} + \sum_{r<s} \mu_{(r,j),(s,i)}\cdot P^t_{(r,j)}$$

and claim that $\psi = \alpha\circ\iota$, as required to prove the first claim of the lemma.
Indeed, one has

$$\begin{aligned}(\alpha\circ\iota)(P_{(s,i)}) =& \alpha(\mathrm{Tr}_{J_s}\cdot P_{(s,i)}) = \mathrm{Tr}_{J_s}\cdot\alpha(P_{(s,i)})\\ &= \sum_{r\geq s} \mathrm{Tr}_{J_s}\cdot\tilde{\mu}_{(r,j),(s,i)}\cdot P^t_{(r,j)} + \sum_{r<s} \mathrm{Tr}_{J_s}\cdot\mu_{(r,j),(s,i)}\cdot P^t_{(r,j)}\\ &= \sum_{r\geq s} \mathrm{Tr}_{J_r}\cdot\mu_{(r,j),(s,i)}\cdot P^t_{(r,j)} + \sum_{r<s} \mathrm{Tr}_{J_s}\cdot\mu_{(r,j),(s,i)}\cdot P^t_{(r,j)},\end{aligned}$$

which is equal to $\psi(P_{(s,i)})$ by (25).
To prove the second claim we write $\epsilon : \mathbb{Z}_p[G] \to \mathbb{Z}_p$ for the canonical augmentation map and define a canonical ring homomorphism $\epsilon_{\mathbb{F}_p}$ as the composition

$$\mathbb{Z}_p[G] \xrightarrow{\epsilon} \mathbb{Z}_p \to \mathbb{F}_p.$$

Now, the equalities (24) imply that

$$\epsilon(\Psi'_{(r,j),(s,i)}) = \begin{cases}\epsilon(\Psi_{(r,j),(s,i)}) - p^{n-r}\epsilon(\mu_{(r,j),(s,i)}), & \text{if } r \geq s;\\ \epsilon(\Psi_{(r,j),(s,i)}) - p^{n-s}\epsilon(\mu_{(r,j),(s,i)}), & \text{if } r < s,\end{cases}$$

and hence also that if $r, s < n$ then $\epsilon_{\mathbb{F}_p}(\Psi'_{(r,j),(s,i)}) = \epsilon_{\mathbb{F}_p}(\Psi_{(r,j),(s,i)})$ (this equality is trivial for $r = n$ or $s = n$).
The ring $\mathbb{Z}_p[G]$ is local with maximal ideal equal to $\ker(\epsilon_{\mathbb{F}_p})$. In particular an element x of $\mathbb{Z}_p[G]$ is a unit if and only if $\epsilon_{\mathbb{F}_p}(x) \neq 0$.
One then knows that $\epsilon_{\mathbb{F}_p}(\det(\Psi)) = \det(\epsilon_{\mathbb{F}_p}(\Psi)) = \det(\epsilon_{\mathbb{F}_p}(\Psi')) = \epsilon_{\mathbb{F}_p}(\det(\Psi')) \neq 0$.
It thus follows that $\det(\Psi) \in \mathbb{Z}_p[G]^\times$ and therefore that γ is bijective, as required. □

Now, if we denote by $[f]$ the pre-image in $\mathrm{Ext}^2_{\mathbb{Z}_p[G]}(A(F)^*_p, A^t(F)_p)$ under the isomorphism (15) of the class of an endomorphism f of $A^t(F)_p$, then Lemma 3.5 implies that $[\gamma] - [-\phi^{-1}] = [\psi] = 0$ and hence also that $[\gamma] = [-\phi^{-1}]$.

In addition, since both γ and $-\phi^{-1}$ are bijective, this class in $\mathrm{Ext}^2_{\mathbb{Z}_p[G]}(A(F)_p^*, A^t(F)_p)$ may be represented by both of the exact sequences obtained by replacing ϕ^{-1} by γ^{-1} or by $-\phi$ in the exact sequence (17).
By the general result [9, Lem. 4.7] there exist automorphisms κ^1 and κ^2 of X with the property that the (exact) diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^t(F)_p & \xrightarrow{\iota\circ\gamma^{-1}} & X & \xrightarrow{\Theta} & X & \xrightarrow{\pi} & A(F)_p^* & \longrightarrow & 0 \\ & & \| & & \kappa^1\downarrow & & \kappa^2\downarrow & & \| & & \\ 0 & \longrightarrow & A^t(F)_p & \xrightarrow{\iota\circ(-\phi)} & X & \xrightarrow{\Theta} & X & \xrightarrow{\pi} & A(F)_p^* & \longrightarrow & 0 \end{array} \tag{26}$$

is commutative.
Now, one may compute (for instance, by the argument of [6, Prop. 4.4]) the desired sum as

$$\sum_{\psi\in\widehat{G}} \frac{\varepsilon_\psi(\Psi)}{\varepsilon_\psi(\Psi')}\cdot e_\psi = \frac{\det_{\mathbb{Q}_p[G]}(\langle\gamma,\Theta,s_1,s_2\rangle)}{\det_{\mathbb{Q}_p[G]}(\langle-\phi^{-1},\Theta,s_1,s_2\rangle)}$$

where, for any ($\mathbb{Q}_p[G]$-equivariant) splittings s_1 and s_2 as in (18) and (19), and any endomorphism β of $A^t(F)_p$, we have written $\langle\beta,\Theta,s_1,s_2\rangle$ for the composite isomorphism

$$\begin{aligned}\mathbb{Q}_p\cdot X \xrightarrow{s_1} \mathbb{Q}_p\cdot A^t(F)_p \oplus \mathbb{Q}_p\cdot \mathrm{im}(\Theta) \xrightarrow{\beta\oplus\mathrm{id}} \mathbb{Q}_p\cdot A^t(F)_p \oplus \mathbb{Q}_p\cdot \mathrm{im}(\Theta)\\ \to \mathbb{Q}_p\cdot A(F)_p^* \oplus \mathbb{Q}_p\cdot \mathrm{im}(\Theta) \xrightarrow{s_2^{-1}} \mathbb{Q}_p\cdot X,\end{aligned}$$

with the unlabeled arrow simply mapping a point $P^t_{(s,i)}$ to $P^*_{(s,i)}$.
It is then straightforward to deduce from the commutativity of the diagram (26) that

$$\sum_{\psi\in\widehat{G}} \frac{\varepsilon_\psi(\Psi)}{\varepsilon_\psi(\Psi')}\cdot e_\psi = \det_{\mathbb{Z}_p[G]}(\kappa_1)\cdot\det_{\mathbb{Z}_p[G]}(\kappa_2)^{-1}$$

and, since both of the determinants on the right hand side are by construction elements of $\mathbb{Z}_p[G]^\times$, this concludes the proof of Lemma 3.4. □

4. Computation of the Mazur-Tate pairing

In this section we explain how one may numerically compute the Mazur-Tate pairing (5). The computation can be reduced to the computation of local Tate duality pairings which, in turn, may in simple situations be computed by the evaluation of Hilbert symbols thanks to recent results of Fisher and Newton [18] or of Visse [30].
Our approach is based crucially on the ability to compute certain generalised Selmer groups, for whose calculation we will apply a method of Schaefer and Stoll [26]. In this regard we also wish to mention subsequent work of Cremona, Fisher, O'Neil, Simon and Stoll [13, 14, 15] where they develop algorithms for computing n-Selmer groups by representing their elements as curves of degree n in $\mathbb{P}^{n-1}$. However, we have not so far required using their methods.

4.1. **The general strategy.** We continue to assume the hypotheses of Section 2.1. In particular,as explained in Section 2.3, the result [10, Prop. 6.3(ii)] implies that every element of $A^t(k)_p$ and $A(k)_p$ is 'locally-normed'. Under this condition, Bertolini and Darmon have defined in [1, §3.4.1] and [2, §2.2] a pairing

$$\langle\ ,\ \rangle_1 \colon A^t(k)_p \otimes_{\mathbb{Z}_p} A(k)_p \longrightarrow G \simeq I_p(G)/I_p(G)^2.$$

Although the definition of this pairing is only given in the case that A is an elliptic curve, it extends naturally to our more general setting (see also [10, §10]).
The results of Bertolini and Darmon in [2, Thm. 2.8 and Rem. 2.10] and of Tan in [29, Prop. 3.1] combine to directly show that the pairing $\langle\ ,\ \rangle_1$ coincides with the Mazur-Tate pairing $\langle\ ,\ \rangle_{F/k}^{\mathrm{MT}}$. We are therefore left with the task to describe the explicit computation of $\langle\ ,\ \rangle_1$.
Let B be either A or its dual A^t. For a finite set S of non-archimedean places of k we define the generalised Selmer group

$$\mathrm{Sel}_S^{(p^n)}(B/F) \leq H^1(F, B[p^n])$$

to be the kernel of the localisation map

$$H^1(F, B[p^n]) \longrightarrow \prod_{w \notin S(F)} H^1(F_w, B),$$

with the product running over all non-archimedean places of F that do not belong to the set $S(F)$ of places that lie above a place in S. We recall that this group is also often referred to as a 'relaxed Selmer group'.
By Kummer theory we then have

$$\begin{aligned} & \mathrm{Sel}_S^{(p^n)}(B/F) \\ = \ & \{\xi \in H^1(F, B[p^n]) \mid \mathrm{res}_w(\xi) \in \delta_w(B(F_w)/p^n B(F_w)) \text{ for all } w \notin S(F)\}. \end{aligned}$$

Here $\mathrm{res}_w : H^1(F, B[p^n]) \to H^1(F_w, B[p^n])$ denotes the canonical localisation map and $\delta_w : B(F_w)/p^n B(F_w) \to H^1(F_w, B[p^n])$ is the canonical Kummer map. In particular, when S is taken to be the empty set, one recovers the usual Selmer group $\mathrm{Sel}^{(p^n)}(B/F)$ associated with multiplication by p^n.
In the following we will employ the notation from [10, Sec. 10.2.1]. We set $Z := \mathbb{Z}/p^n\mathbb{Z}$ and $R := Z[G]$ and define additional R-modules

$$B_S(\mathbb{A}_F)/p^n := \prod_{w \in S(F)} B(F_w)/p^n B(F_w)$$

and

$$H^1_S(\mathbb{A}_F, B[p^n]) := \prod_{w \in S(F)} H^1(F_w, B[p^n]).$$

In order to define $\langle\ ,\ \rangle_1$, we first recall the construction of a canonical (local duality) perfect pairing

$$\langle\ ,\ \rangle \colon H^1_S(\mathbb{A}_F, A^t[p^n]) \times H^1_S(\mathbb{A}_F, A[p^n]) \longrightarrow R. \tag{27}$$

If A is defined over an ℓ-adic field L (for some prime ℓ), then we write $\langle\ ,\ \rangle_{L,p^n}$ for the local Tate duality pairing obtained by combining the cup product, the Weil pairing

and the invariant map as follows:

$$\begin{aligned} H^1(L,A^t[p^n])\times H^1(L,A[p^n]) &\xrightarrow{\cup} H^2(L,A^t[p^n]\otimes_{\mathbb{Z}_p}A[p^n]) \\ &\longrightarrow H^2(L,\mu_{p^n}) \\ &\xrightarrow{\mathrm{inv}_L} \mathbb{Q}_p/\mathbb{Z}_p. \end{aligned} \tag{28}$$

Then, for $x=(x_w)_{w\in S(F)}\in H^1_S(\mathbb{A}_F,A^t[p^n])$ and $y=(y_w)_{w\in S(F)}\in H^1_S(\mathbb{A}_F,A[p^n])$ we set

$$\langle x,y\rangle_S := \sum_{w\in S(F)}\langle x_w,y_w\rangle_{F_w,p^n}.$$

All values $\langle x,y\rangle_S$ in fact belong to $\frac{1}{p^n}\mathbb{Z}_p/\mathbb{Z}_p$, which we henceforth identify with $Z=\mathbb{Z}/p^n\mathbb{Z}$. We may thus define the pairing (27) by the explicit formula

$$\langle x,y\rangle := \sum_{g\in G}\langle x^g,y\rangle_S g^{-1}. \tag{29}$$

We now recall the explicit definition of $\langle P,Q\rangle_1$ for $P\in A^t(k)$ and $Q\in A(k)$. Let Σ be an admissible set of primes as in [1, Def. 2.22], [2, Def. 1.5] or [10, Lem. 10.5]. A crucial consequence of the definition of admissibility is that the canonical (diagonal) localisation map

$$A(F)/p^nA(F)\longrightarrow A_\Sigma(\mathbb{A}_F)/p^n \tag{30}$$

is injective.

We write δ for the canonical global Kummer map and let $\tilde{x}\in \mathrm{Sel}_\Sigma^{(p^n)}(A^t/F)^G$ denote the image of P under the canonical composition

$$A^t(k)\longrightarrow (A^t(F)/p^nA^t(F))^G \xrightarrow{\delta^G} \mathrm{Sel}_\Sigma^{(p^n)}(A^t/F)^G.$$

We also let $\tilde{y}\in (A_\Sigma(\mathbb{A}_F)/p^n)^G$ be the image of Q under the canonical (diagonal) localisation map

$$A(k)\longrightarrow (A(F)/p^nA(F))^G\longrightarrow (A_\Sigma(\mathbb{A}_F)/p^n)^G.$$

By [1, §3.1] the R-modules $\mathrm{Sel}_\Sigma^{(p^n)}(A^t/F)$ and $A_\Sigma(\mathbb{A}_F)/p^n$ are G-cohomologically trivial. We therefore find elements $x\in \mathrm{Sel}_\Sigma^{(p^n)}(A^t/F)$ and $y=(y_w)_{w\in\Sigma(F)}\in A_\Sigma(\mathbb{A}_F)/p^n$ such that

$$\mathrm{Tr}_G(x)=\tilde{x},\quad \mathrm{Tr}_G(y)=\tilde{y}.$$

We next consider the canonical (diagonal) localisation map

$$\lambda_\Sigma\colon \mathrm{Sel}_\Sigma^{(p^n)}(A^t/F)\subseteq H^1(F,A^t[p^n])\xrightarrow{\oplus \mathrm{res}_w} H^1_\Sigma(\mathbb{A}_F,A^t[p^n])$$

and the product of local Kummer maps

$$\delta_\Sigma\colon A_\Sigma(\mathbb{A}_F)/p^n\xrightarrow{\oplus\delta_w} H^1_\Sigma(\mathbb{A}_F,A[p^n]).$$

Then, by the definition of $\langle\ ,\ \rangle_1$ given in [2, §2.2], we obtain

$$\langle P,Q\rangle_1\equiv\langle\lambda_\Sigma(x),\delta_\Sigma(y)\rangle \pmod{I_p(G)^2},$$

with $\langle\ ,\ \rangle$ as in (27). Noting the sign involved in the definition (10) of the equivariant regulator, we are in fact interested in computing the inverse $-\langle P,Q\rangle_1$. From the definition (29) of $\langle\ ,\ \rangle$, we easily derive the explicit expression

$$-\langle P,Q\rangle_1 \equiv \sum_{g\in G}\left(\sum_{w\in\Sigma(F)}\langle \mathrm{res}_w(x^g),\delta_w(y_w)\rangle_{F_w,p^n}\right)g \pmod{I_p(G)^2}, \tag{31}$$

which is convenient for the explicit evaluations which we will describe in the next subsection.

4.2. **Algorithmic evaluation of the pairing.** In this subsection we describe how we numerically evaluate the right hand side of (31). From an algorithmic point of view we are mainly interested in the case of elliptic curves and, for this reason, we henceforth assume that $E := A = A^t$ is an elliptic curve defined over k. Furthermore, we assume that F/k is cyclic of degree p where as before p is an odd prime such that E, F/k and p satisfy the hypotheses of Section 2.1.
The central computational problem in the numerical evaluation of the Mazur-Tate pairing, using the approach of Bertolini and Darmon as described in the previous section, is first of all the computation of the generalised Selmer group $\mathrm{Sel}_\Sigma^{(p)}(E/F)$. We will closely follow the method of Schaefer and Stoll [26] to compute this group.
We fix a finite set V of places of F containing the p-adic places and all places w such that the Tamagawa number c_w of E at w is divisible by p. We also fix an admisible set Σ of places of k as in Section 4.1. We then write $H^1(F,E[p];V\cup\Sigma(F))$ for the group of cohomology classes in $H^1(F,E[p])$ that are unramified outside $V\cup\Sigma(F)$. Now the result of [26, Prop. 3.2] shows that $\mathrm{Sel}^{(p)}(E/F)$ is given by

$$\{\xi\in H^1(F,E[p];V\cup\Sigma(F)) \mid \mathrm{res}_w(\xi)\in\delta_w(E(F_w)/pE(F_w)) \text{ for all } w\in V\cup\Sigma(F)\},$$

whereas a slight generalization of the above mentioned result implies that the generalised Selmer group $\mathrm{Sel}_\Sigma^{(p)}(E/F)$ is equal to

$$\{\xi\in H^1(F,E[p];V\cup\Sigma(F)) \mid \mathrm{res}_w(\xi)\in\delta_w(E(F_w)/pE(F_w)) \text{ for all } w\in V\setminus\Sigma(F)\}. \tag{32}$$

We fix an algebraic closure F^c of F and let $W\subseteq E[p]\setminus\{0\}$ be a G_F-invariant spanning set for $E[p]$. Thus W is a union of G_F-orbits containing an $\mathbb{F}_p$-basis of $E[p]$. Note that in the generic case G_F acts transitively on $E[p]\setminus\{0\}$, so that in such cases we are forced to use $W=E[p]\setminus\{0\}$.
We write $A^c := \mathrm{Map}(W,F^c)$ for the set of maps from W to F^c. Then the Galois group G_F acts on A^c by conjugation, i.e., for $\sigma\in G_F$, $a\in A^c$ and $P\in W$ one has $(\sigma a)(P)=\sigma(a(\sigma^{-1}(P)))$.
We denote by $A=\mathrm{Map}_{G_F}(W,F^c):=\mathrm{Map}(W,F^c)^{G_F}$ the set of G_F-invariant maps in A^c. Then A is a finite dimensional étale F-algebra. Explicitly, let $P_1,\dots,P_s\in W$ be a set of G_F-orbit representatives of W and set

$$H_i := \{\sigma\in G_F \mid \sigma(P_i)=P_i\}$$

and $L_i := (F^c)^{H_i}$. Then each L_i/F is a finite separable field extension and we have a canonical isomorphism

$$A \longrightarrow \prod_{i=1}^{s} L_i, \quad a \mapsto (a(P_i))_{1\leq i\leq s}\,.$$

The Weil pairing $e_p\colon E[p]\times E[p] \longrightarrow \mu_p(F^c)$ defines a map

$$\omega\colon E[p] \longrightarrow \mu_p(A^c) := \mathrm{Map}(W, \mu_p(F^c)), \quad P \mapsto e_p(P, \_\,).$$

This map induces a homomorphism in cohomology

$$\bar{\omega}\colon H^1(F, E[p]) \longrightarrow H^1(F, \mu_p(A^c)) \tag{33}$$

which, by [26, Prop. 4.3], is known to be injective if $p\nmid |\mathrm{Gal}(F(E[p])/F)|$ or $p\nmid |W|$. In addition, by an immediate generalization of Hilbert's Theorem 90, we have a Kummer isomorphism

$$\kappa\colon H^1(F, \mu_p(A^c)) \longrightarrow A^\times/A^{\times p} \tag{34}$$

which combined with $\bar{\omega}$ defines an embedding (assuming, for example, that $p\nmid |W|$)

$$H^1(F, E[p]) \hookrightarrow A^\times/A^{\times p}.$$

Roughly speaking, the algorithm of Schaefer and Stoll [26], in a first step, computes $H^1(F, E[p]; V\cup\Sigma(F))$ as a subset of $A^\times/A^{\times p}$ via the embedding $\kappa\circ\bar{\omega}$ and then, in a second step, checks the local conditions occurring in (32).

To describe the first step we let L/F be a finite extension. For a finite place t of L we write $\mathrm{ord}_t\colon L^\times \longrightarrow \mathbb{Z}$ for the associated normalised valuation. If T is a finite set of finite places of F, we set

$$L(T,p) := \{a\in L^\times/L^{\times p} \mid \mathrm{ord}_t(a)\in p\mathbb{Z} \text{ for all } t\notin T(L)\},$$

and more generally, if $A\simeq\prod_{i=1}^s L_i$ is an étale F-algebra as above, we define

$$A(T,p) := \prod_{i=1}^{s} L_i(T,p).$$

Then, using the embedding $H^1(F, E[p])\hookrightarrow A^\times/A^{\times p}$ given by $\kappa\circ\bar{\omega}$, the result of [26, Cor. 5.9] shows the equality

$$H^1(F, E[p]; V\cup\Sigma(F)) = H^1(F, E[p])\cap A(V\cup\Sigma(F), p).$$

The work of Schaefer and Stoll now describes how to compute the group $H^1(F, E[p])$ inside $A^\times/A^{\times p}$ and then, by intersecting with the finite group $A(V\cup\Sigma(F),p)$, we obtain $H^1(F, E[p]; V\cup\Sigma(F))$ as a subgroup of $A^\times/A^{\times p}$. For further details we refer the reader to [26].

Testing the local conditions in the second step (see again [26] for details) we finally obtain both $\mathrm{Sel}^{(p)}(E/F)$ and $\mathrm{Sel}^{(p)}_\Sigma(E/F)$ as subgroups of $A^\times/A^{\times p}$, or even better, as subgroups of the finite group $A(V\cup\Sigma(F),p)$. Note, however, that the computation of $A(V\cup\Sigma(F),p)$ requires the computation of ideal class groups and units in all of the fields L_i, $i=1,..,s$.

In this context we recall that in the generic case we have to use $W = E[p]\setminus\{0\}$. In any such cases we will fix $S_0\in W$ and set $L := F(S_0)$, so that $[L:F] = p^2-1$ and $A\simeq L$.

For any place w in $\Sigma(F)$ we fix an embedding $\iota_w : F \to F_w$ and set $A_w^c := F_w^c \otimes_F A$ and $A_w := F_w \otimes_F A$. Note that there is a canonical isomorphism

$$A_w \xrightarrow{\simeq} \mathrm{Map}_{G_{F_w}}(W, F_w^c), \quad z \otimes a \mapsto (S \mapsto z\iota_w(a(S)))\,.$$

We then consider the following commutative diagram

$$\begin{array}{ccccccc} E(F)/pE(F) & \xrightarrow{\delta} & H^1(F, E[p]) & \xrightarrow{\bar{\omega}} & H^1(F, \mu_p(A^c)) & \xrightarrow{\kappa} & A^\times/A^{\times p} \\ \downarrow{\scriptstyle \iota_w} & & \downarrow{\scriptstyle \mathrm{res}_w} & & \downarrow{\scriptstyle \mathrm{res}_w} & & \downarrow{\scriptstyle \iota_{w,*}} \\ E(F_w)/pE(F_w) & \xrightarrow{\delta_w} & H^1(F_w, E[p]) & \xrightarrow{\bar{\omega}_w} & H^1(F_w, \mu_p(A_w^c)) & \xrightarrow{\kappa_w} & A_w^\times/A_w^{\times p}, \end{array} \tag{35}$$

where $\iota_{w,*}$ is induced by composition with ι_w while the maps $\bar{\omega}_w$ and κ_w are the local analogues of (33) and (34), respectively, and res_w is the localisation map.
The local Tate pairing

$$\langle\ ,\ \rangle_{F_w,p} \colon H^1(F_w, E[p]) \times H^1(F_w, E[p]) \longrightarrow \mathbb{Q}_p/\mathbb{Z}_p$$

of (28) induces a pairing $\langle\ ,\ \rangle_{A_w}$ on the image of $\kappa_w \circ \bar{\omega}_w$. In what follows we will describe the computation of $\langle\ ,\ \rangle_{A_w}$.
We write q_{A_w} for the unique quadratic form such that, for all

$$a, b \in (\kappa_w \circ \bar{\omega}_w)\left(H^1(F_w, E[p])\right),$$

one has

$$\langle a, b\rangle_{A_w} = q_{A_w}(ab) - q_{A_w}(a) - q_{A_w}(b).$$

Let

$$\{\ ,\ \}_{F_w,p} \colon F_w^\times/F_w^{\times p} \times F_w^\times/F_w^{\times p} \longrightarrow \mu_p$$

denote the Hilbert symbol. We henceforth assume that $E[p]$ is contained in $E(F_w)$ (which is always the case for places $w \in \Sigma(F)$ for an admissible set Σ of places of k). In this particular case one can shift the problem of computing the local Tate pairing to the computation of Hilbert symbols which is easy for places w which are prime to p by [25, Ch. V, Prop. 3.4].
We fix generators $S, T \in E(F_w)$ of $E[p]$. Then $e_p(T, S)$ generates μ_p and we define a map

$$\xi_{S,T} \colon \mu_p \longrightarrow \mathbb{Z}/p\mathbb{Z}$$

by $\xi_{S,T}(e_p(T, S)) = 1 + p\mathbb{Z}$. For $\bar{a} \in A_w^\times/A_w^{\times p}$ with $a \in A_w \simeq \mathrm{Map}_{G_w}(W, \bar{F}_w)$ we obtain a well defined map $\bar{a} \colon W \longrightarrow F_w^\times/F_w^{\times p}$.
Fisher and Newton in [18] have given an explicit description of the local Tate pairing associated with the p-torsion of an elliptic curve in the special case $p = 3$. Their formulas have subsequently been generalised by Visse in [30] to any odd prime p. In particular, from [30, Th. 3.7 and 3.11] we obtain, for arbitrary odd p, an equality

$$q_{A_w}(\bar{a}) = \xi_{S,T}\left(\{\bar{a}(S), \bar{a}(T)\}_{F_w,p}\right)$$

for all $\bar{a} \in (\kappa_w \circ \bar{\omega}_w)\left(H^1(F_w, E[p])\right)$. As a consequence we obtain

$$\langle \bar{a}, \bar{b}\rangle_{A_w} = \xi_{S,T}\left(\frac{\{\bar{a}(S), \bar{b}(T)\}_{F_w,p}}{\{\bar{a}(T), \bar{b}(S)\}_{F_w,p}}\right). \tag{36}$$

We are now in a position to describe the explicit computation of $-\langle P,Q\rangle_1$ using the formula in (31). Let $\tilde{y}$ denote the image of Q in $E_\Sigma(\mathbb{A}_F)/p$ as in Section 4.1. Assuming that the point Q is not divisible by p ensures that $\tilde{y} \neq 0$ because of the injectivity of the map (30).
For each $v \in \Sigma$ we fix a place $\hat{v}$ of F lying over v. For each $w \in \Sigma(F)$ we define

$$y_w := \begin{cases} \tilde{y}_{\hat{v}}, & \text{if } w \mid v \text{ and } w = \hat{v}, \\ 0, & \text{otherwise .} \end{cases}$$

Since $\tilde{y}$ is fixed by G it is easy to see that $y := (y_w)_{w\in\Sigma(F)} \in E_\Sigma(\mathbb{A}_F)/p$ satisfies $\mathrm{Tr}_G(y) = \tilde{y}$. Hence the formula in (31) simplifies to

$$-\langle P,Q\rangle_1 \equiv \sum_{g\in G}\left(\sum_{v\in\Sigma}\langle \mathrm{res}_{\hat{v}}(x^g), \delta_{\hat{v}}(y_{\hat{v}})\rangle_{F_{\hat{v}},p}\right) g \pmod{I_p(G)^2}. \tag{37}$$

Next we explain how to compute $x \in \mathrm{Sel}_\Sigma^{(p)}(E/F)$ with $\mathrm{Tr}_G(x) = \tilde{x}$. The generalised Selmer group $\mathrm{Sel}_\Sigma^{(p)}(E/F)$ is computed as a subgroup of $A^\times/A^{\times p}$ which carries an action of G induced by conjugation. Explicitly, for all $\sigma \in G$, $a \in A$ and $S \in W$ we choose an arbitrary lift $\hat{\sigma} \in G_k$ of σ and set

$$(\sigma a)(S) = \hat{\sigma}(a(\hat{\sigma}^{-1}(S))). \tag{38}$$

As sketched in Section 4.3 below this action is explicitly computable. We can therefore compute the $\mathbb{F}_p$-representation of G induced by $\mathrm{Sel}_\Sigma^{(p)}(E/F)$ and then represent Tr_G as a linear map $\mathrm{Sel}_\Sigma^{(p)}(E/F) \longrightarrow \mathrm{Sel}_\Sigma^{(p)}(E/F)$ and thus compute a preimage x of $\tilde{x}$.
In the same way we can compute the elements x^g occuring in (37). Note that as an element of $A^\times/A^{\times p}$ the element $\tilde{x}$ is given by $(\kappa\circ\bar{\omega}\circ\delta)(P)$. The computation of the map

$$H := \kappa\circ\bar{\omega}\circ\delta$$

is quite non-trivial and explained in [27, 28, Ch. 2] and [26, Ch. 3], as well as the computation of the local analogue

$$H_w := \kappa_w\circ\bar{\omega}_w\circ\delta_w.$$

For each $v \in \Sigma$ we now compute the completion $F_{\hat{v}}$ together with an embedding $\iota_v\colon F \longrightarrow F_{\hat{v}}$ and define $a_{P,g,\hat{v}} := \mathrm{res}_{\hat{v}}(x^g) = \iota_v \circ x^g$.
In order to compute $\delta_{\hat{v}}(y_{\hat{v}})$ we use the commutativity of diagram (35) and define

$$a_{Q,\hat{v}} := \kappa_{\hat{v}}(\bar{\omega}_{\hat{v}}(\delta_{\hat{v}}(\iota_{\hat{v}}(Q)))) = \iota_{\hat{v}} \circ (\kappa(\bar{\omega}(\delta(Q))) = \iota_{\hat{v}} \circ H(Q)$$

and finally obtain

$$\langle \mathrm{res}_{\hat{v}}(x^g), \delta_{\hat{v}}(y_{\hat{v}})\rangle_{F_{\hat{v}},p} = \xi_{S,T}\left(\frac{\{a_{P,g,\hat{v}}(S), a_{Q,\hat{v}}(T)\}_{F_w,p}}{\{a_{P,g,\hat{v}}(T), a_{Q,\hat{v}}(S)\}_{F_w,p}}\right).$$

4.3. **Comments on the implementation.** In this subsection we discuss the restrictions on our MAGMA implementation, where we must always assume that G_F acts transitively on $E[p]\setminus\{0\}$. Hence, for the rest of this subsection, we set $W = E[p]\setminus\{0\}$ and fix a point $S_0 \in W$. As before, F/k is a cyclic extension of degree p where p is an odd prime.

We choose $\lambda \in \mathbb{Q}$ such that the elements

$$w_S := y_S + \lambda x_S, \quad S = (x_S, y_S) \in W,$$

are pairwise distinct. Since G_F acts transitively on W the polynomial

$$f(x) := \prod_{S \in W} (x - w_S) \in F[x]$$

is irreducible. It is easily seen that $F(S_0) = F(w_{S_0})$. We therefore may and will use $L := F(w_{S_0})$.
This has the following useful consequence for the computation of $a_w := \iota_w \circ a$, where a is an element of $A = \mathrm{Map}_{G_F}(W, F^c)$ and ι_w an embedding of F into F_w. Namely, if we assume that $a \in A$ corresponds to $\bar{h} \in F[x]/(f(x))$ under the composite map

$$A \xrightarrow{\alpha} L \xrightarrow{\beta^{-1}} F[x]/(f(x)), \quad \alpha(a) := a(S_0), \quad \beta(\bar{h}) := h(w_{S_0}),$$

then we have $a(S_0) = h(w_{S_0})$. Assume further that $\tilde{S} \in E(F_w)[p]$ and let $S \in W$ be such that $\iota_w(S) = \tilde{S}$. Then a straightforward computation shows that $a_w(\tilde{S}) = (\iota_w h)(w_{\tilde{S}})$.
A further useful consequence is a particularly simple description of the action of G on A. Recall that $\sigma \in G$ acts on A by conjugation as in (38). If $\bar{h} \in F[x]/(f(x))$ corresponds to $a \in A$, then we claim that σa corresponds to $\overline{\sigma h}$. Indeed, if $\tau(S_0) = \hat{\sigma}^{-1}(S_0)$ with $\tau \in G_F$, then

$$(\sigma a)(S_0) = \hat{\sigma}(a(\hat{\sigma}^{-1}(S_0))) = \hat{\sigma}(\tau(h(w_{S_0}))) = \hat{\sigma}(h(\tau(w_{S_0}))) = (\sigma h)(w_{S_0}).$$

In our implementation we additionally assume $k = \mathbb{Q}$ and $p = 3$. In this case explicit formulae for the computation of the generalised Selmer group based on the work of Schaefer and Stoll in [26] are given in [19, Sec. 7]. These are used throughout in our implementation.
We summarise the above discussion in the following remark.

Remark 4.1. Our MAGMA implementation is restricted to handle the case $k = \mathbb{Q}$, $p = 3$ and $\mathrm{rk}(E(F)) = \mathrm{rk}(E(\mathbb{Q})) = r$ with $r > 0$. Assuming the validity of the classical Birch and Swinnerton-Dyer conjecture for E/F the implementation will check the hypotheses (a) - (i) of Section 2.1 as well as triviality of $Ш_p(E_F)$ and then numerically verify the rationality part of the eTNC up to the precision of the computation. We then rigorously prove the condition from Theorem 2.1 (by rewriting it in terms of congruence relations in the manner suggested in Remark 2.6).

4.4. **Computations.** Our MAGMA implementation can be used to numerically verify the validity of the refined Birch and Swinnerton-Dyer conjecture for pairs $(E, F/k)$ where

- $k = \mathbb{Q}$ and $E/\mathbb{Q}$ is an elliptic curve with global minimal Weierstrass equation,
- F is the unique subfield of degree $p = 3$ in $\mathbb{Q}(\zeta_\ell)/\mathbb{Q}$ for primes $\ell \equiv 1 \pmod 3$,
- $\mathrm{rk}(E(F)) = \mathrm{rk}(E(\mathbb{Q})) = r$ for some $r > 0$,
- E and F satisfy the hypotheses (a) - (i) of Section 2.1.

Note that the condition $\mathrm{rk}(E(F)) = \mathrm{rk}(E(\mathbb{Q})) = r$ ensures that $E(F)_p \simeq \mathbb{Z}_p^r$ is not projective as a $\mathbb{Z}_p[G]$-module.

Here is the list of examples for $r = 1$, $\ell < 50$ and conductor less than 100. We specify elliptic curves by their Cremona reference.

- E is $37a1$ and $\ell \in \{13, 19\}$.
- E is $43a1$ and $\ell \in \{7, 13, 37\}$.
- E is $53a1$ and $\ell \in \{13, 19, 31, 43\}$.
- E is $58a1$ and $\ell \in \{7, 13, 19, 31, 43\}$.
- E is $61a1$ and $\ell \in \{7, 13, 43\}$.
- E is $65a2$ and $\ell \in \{19, 37, 43\}$.
- E is $77a1$ and $\ell \in \{19, 37\}$.
- E is $79a1$ and $\ell \in \{13, 19, 37\}$.
- E is $82a1$ and $\ell \in \{13, 19, 43\}$.
- E is $82a2$ and $\ell \in \{13, 19, 43\}$.
- E is $83a1$ and $\ell \in \{7, 13, 37\}$.
- E is $88a1$ and $\ell \in \{7, 43\}$.
- E is $89a1$ and $\ell \in \{19, 31, 37\}$.
- E is $91a1$ and $\ell \in \{31\}$.
- E is $389a1$ and $\ell \in \{7, 13, 43\}$.
- E is $433a1$ and $\ell \in \{7, 13, 31, 37\}$.
- E is $446d1$ and $\ell \in \{19\}$.

For $r = 2$, $\ell < 50$ and conductor less than 500 we computed the following examples.

- E is $389a1$ and $\ell \in \{7, 13, 43\}$.
- E is $433a1$ and $\ell \in \{7, 13, 31, 37\}$.
- E is $446d1$ and $\ell \in \{19\}$.

Acknowledgements. The authors are very grateful to David Burns for many interesting discussions and much encouragement, as well as to Christian Wuthrich for his constant interest in our work and many related discussions. We also wish to thank the referee for their careful reading of the manuscript. In particular, their comments and suggestions on Section 4 significantly helped to improve the presentation of this part of the manuscript.

The first author wants to thank Chris Geishauser who in the context of his master thesis [19] provided many MAGMA routines used in the computation of our numerical examples.

The second author is grateful to Stefano Vigni for some pertinent discussions. He also acknowledges financial support from the Spanish Ministry of Science and Innovation, through the 'Severo Ochoa Programme for Centres of Excellence in R&D' [SEV-2015-0554] and [CEX-2019-000904-S] as well as through projects [MTM2016-79400-P] and [PID2019-108936GB-C21].

REFERENCES

[1] M. Bertolini, H. Darmon, Derived heights and generalized Mazur-Tate regulators, Duke Math Journal **76** No. 1 (1994) pp. 75-111.

[2] M. Bertolini, H. Darmon, Derived p-adic heights, American Journal of Math **117** (1995) pp. 1517-1554.

[3] W. Bley, Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture, Exp. Math. **20** (2011), 426-456.

[4] W. Bley, Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture (part II), Math. Comp. **81** (2012), 1681-1705.
[5] W. Bley, The equivariant Tamagawa number conjecture and modular symbols, Math. Ann. **356** (2013), 179-190.
[6] W. Bley, D. Macias Castillo, Congruences for critical values of higher derivatives of twisted Hasse-Weil L-functions, J. reine u. angew. Math. **722** (2017) 105-136.
[7] D. Burns, M. Flach, Tamagawa numbers for motives with (non-commutative) coefficients, Doc. Math. **6** (2001) 501-570.
[8] D. Burns, M. Kurihara, T. Sano, On zeta elements for $\mathbb{G}_m$, Documenta Math. **21** (2016) 555-626.
[9] D. Burns, D. Macias Castillo, Organising matrices for arithmetic complexes, Int. Math. Res. Notices **2014** 10 (2014) 2814-2883.
[10] D. Burns, D. Macias Castillo, On refined conjectures of Birch and Swinnerton-Dyer type for Artin-Hasse-Weil L-series, submitted for publication.
[11] D. Burns, D. Macias Castillo, C. Wuthrich, On Mordell-Weil groups and congruences between derivatives of twisted Hasse-Weil L-functions, J. reine angew. Math. **734** (2017) 187-228.
[12] D. Burns, O. Venjakob, On descent theory and main conjectures in non-commutative Iwasawa theory, J. Inst. Math. Jussieu **10** (2011) 59-118.
[13] J.E. Cremona, T.A.Fisher, C. O'Neil, D. Simon, M. Stoll, Explicit n-decent on elliptic curves, I. Algebra, J.reine angew. Math **615** (2008) 121-155.
[14] J.E. Cremona, T.A.Fisher, C. O'Neil, D. Simon, M. Stoll, Explicit n-decent on elliptic curves, I. Geometry, J.reine angew. Math **632** (2009) 63-84.
[15] J.E. Cremona, T.A.Fisher, C. O'Neil, D. Simon, M. Stoll, Explicit n-decent on elliptic curves, I. Algorithms, Mathematics of Computation **84**, Vol.292, (2014) 895-922.
[16] J. Coates, T. Fukaya, K. Kato, R. Sujatha, O. Venjakob, The GL_2-main conjecture for elliptic curves without complex multiplication, Publ. IHES **101** (2005) 163-208.
[17] H. Darmon, A refined conjecture of Mazur-Tate type for Heegner points, Invent. Math. **110** (1992) 123-146.
[18] T. Fisher, R. Newton, Computing the Cassels-Tate pairing on the 3-Selmer group of an elliptic curve, Int. J. Number Theory **10** (2014), no. 7, 1881-1907.
[19] C. Geishauser, Computation of 2-extensions of dual Selmer groups, Master thesis, LMU 2018.
[20] P. J. Hilton, U. Stammbach, A course in Homological Algebra, Springer-Verlag, New York, 1970.
[21] T. Lawson, C. Wuthrich, Vanishing of some Galois cohomology groups for elliptic curves, in: Elliptic Curves, Modular Forms and Iwasawa Theory (ed. D. Loeffler and S. L. Zerbes), Springer Proc. in Math. and Stat., **188** (2017) 373-399.
[22] D. Macias Castillo, Congruences for critical values of higher derivatives of twisted Hasse-Weil L-functions, II, Acta Arith. **195** (2020), no. 7, 327-365.
[23] B. Mazur, J. Tate, Canonical height pairings via biextensions, In: 'Arithmetic and Geometry' vol. 1, Prog. Math. **35** (1983) 195-237.
[24] B. Mazur, J. Tate, Refined Conjectures of the Birch and Swinnerton-Dyer Type, Duke Math. J. **54** (1987) 711-750.
[25] J. Neukirch, Algebraic Number Theory, Springer-Verlag, 1999.
[26] E.F. Schaefer, M. Stoll, How to do a p-descent on an ellitpic curve, Transactions of the AMS, **356** (2003) 1209-1231.
[27] E.F. Schaefer, Computing a Selmer group of a Jacobian using functions on the curve, Mathematische Annalen, **310** (1998) 447-471.
[28] E.F. Schaefer, Computing a Selmer group of a Jacobian using functions on the curve, ArXiv e-prints, July 2015.
[29] K.-S. Tan, p-adic pairings, Contemp. Math. **165** (1994) 111-121.
[30] E. Visse, Calculating the Tate local pairing for any odd prime number, ArXiv e-prints, October 2016.
[31] A. V. Yakovlev, Homological definability of p-adic representations of groups with cyclic Sylow p-subgroup, An. St. Univ. Ovidius Constanţa **4** (1996) 206-221.

Werner Bley,
Ludwig-Maximilians-Universität München,
Theresienstr. 39,
D-80333 München,
Germany,
bley@math.lmu.de

Daniel Macias Castillo,
Departamento de Matemáticas,
Universidad Autónoma de Madrid, 28049 Madrid (Spain);
and Instituto de Ciencias Matemáticas, 28049 Madrid (Spain).
daniel.macias@uam.es