

**ON MORDELL-WEIL GROUPS  
AND CONGRUENCES BETWEEN DERIVATIVES  
OF TWISTED HASSE-WEIL  $L$ -FUNCTIONS**

DAVID BURNS, DANIEL MACIAS CASTILLO AND CHRISTIAN WUTHRICH

ABSTRACT. Let  $A$  be an abelian variety defined over a number field  $k$  and let  $F$  be a finite Galois extension of  $k$ . Let  $p$  be a prime number. Then under certain not-too-stringent conditions on  $A$  and  $F$  we compute explicitly the algebraic part of the equivariant Tamagawa number of the pair  $(h^1(A/F)(1), \mathbb{Z}[\mathrm{Gal}(F/k)])$ . By comparing the result of this computation with the theorem of Gross and Zagier we are able to give the first verification of the  $p$ -component of the equivariant Tamagawa number conjecture for an abelian variety in the technically most demanding case in which the relevant Mordell-Weil group has strictly positive rank and the relevant field extension is both non-abelian and of degree divisible by  $p$ . More generally, our approach leads us to the formulation of certain precise families of conjectural  $p$ -adic congruences between the values at  $s = 1$  of derivatives of the Hasse-Weil  $L$ -functions associated to twists of  $A$ , normalised by a product of explicit equivariant regulators and periods, and to explicit predictions concerning the Galois structure of Tate-Shafarevich groups. In several interesting cases we provide theoretical and numerical evidence in support of these more general predictions.

1. INTRODUCTION

Let  $A$  be an abelian variety defined over a number field  $k$ . Then for any finite Galois extension  $F$  of  $k$  with group  $G$  the equivariant Tamagawa number conjecture for the pair  $(h^1(A/F)(1), \mathbb{Z}[G])$  is formulated in [16, Conjecture 4(iv)] as an equality in a relative algebraic  $K$ -group. This conjectural equality is rather technical to state and very inexplicit in nature but is known to constitute a strong and simultaneous refinement of the Birch and Swinnerton-Dyer conjecture for  $A$  over each of the intermediate fields of  $F/k$ .

The refined conjecture also naturally decomposes into ‘components’, one for each rational prime  $p$ , in a way that will be made precise in §5.1 below, and each such  $p$ -component (which for convenience we refer to as ‘eTNC $_p$ ’ in the remainder of this introduction) is itself of some interest. We recall, for example, that if  $A$  has good ordinary reduction at  $p$ , then the compatibility result proved by Venjakob and the first named author in [19, Theorem 8.4] shows that eTNC $_p$  is very closely related to the main conjecture of non-commutative Iwasawa theory for  $A$  with respect to any compact  $p$ -adic Lie extension of  $k$  that contains  $F$ .

If  $p$  does not divide the order of  $G$ , then, without any hypothesis on the reduction of  $A$  at  $p$ , it is straightforward to use the techniques developed in [15, §1.7] to give an explicit interpretation of eTNC $_p$  (although, of course, obtaining a full proof in this case still remains a very difficult problem). However, if  $p$  divides the order of  $G$ , then even obtaining an explicit interpretation of eTNC $_p$  has hitherto seemed to be a very difficult problem - see, for example, the considerable efforts made by Bley [3, 4] in this direction.

One of the main goals of the present article is therefore to develop a general approach which can be used to obtain (both theoretical and numerical) verifications of eTNC $_p$  in the technically most demanding case in which the abelian variety  $A$  has strictly positive rank over  $F$  and the Galois group  $G$  is both non-abelian and of order divisible by  $p$ .

To give a concrete example of the results we shall obtain in this way, we note that in §6.1 our techniques will be combined with the theorem of Gross and Zagier to prove the following result (and to help put this result into context see Remarks 1.2 and 1.3 below).

**Theorem 1.1.** *Let  $p$  be an odd prime,  $K$  an imaginary quadratic field in which  $p$  is unramified and  $F$  its Hilbert  $p$ -classfield. Write  $G$  for the generalised dihedral group  $\text{Gal}(F/\mathbb{Q})$ .*

*Let  $A$  be an elliptic curve over  $\mathbb{Q}$  which satisfies, with respect to the field  $K$ , the hypotheses (a), (b), (c), (e) and (f) that are listed in §3 and for which the Tate-Shafarevich group  $\text{III}(A_F)$  is finite.*

*Assume in addition that each of the following four hypotheses is satisfied.*

- (i) *all primes of bad reduction for  $A$  split in  $K/\mathbb{Q}$ ;*
- (ii) *the Galois group of  $K(A[p])/K$  is isomorphic to  $\text{GL}_2(\mathbb{F}_p)$ ;*
- (iii) *the Hasse-Weil  $L$ -function  $L(A/K, s)$  has a simple zero at  $s = 1$ ;*
- (iv) *the trace to  $A(K)$  of the Heegner point is not divisible by  $p$ .*

*Then the  $p$ -component of the equivariant Tamagawa number conjecture is valid for the pair  $(h^1(A/F)(1), \mathbb{Z}[G])$ .*

*Remark 1.2.* For a fixed elliptic curve  $A$  over  $\mathbb{Q}$  and imaginary quadratic field  $K$ , it will be clear that the hypotheses (a), (b) and (c) that occur in the statement of Theorem 1.1 are satisfied by all but finitely many primes  $p$ . In addition, it will be clear that for a fixed  $A$  and  $p$  the hypotheses (e) and (f) only constitute a mild restriction on the ramification of the extension  $K/\mathbb{Q}$ . Finally we recall that, by a famous result of Serre [46], the hypothesis (ii) holds for almost all  $p$  if  $A$  does not have complex multiplication.

*Remark 1.3.* In the context of Theorem 1.1 we also note that for any natural number  $n$  there are infinitely many imaginary quadratic fields  $K$  in which  $p$  does not ramify and for which the group  $\text{Gal}(F/K)$  has exponent divisible by  $p^n$ . (For details of an explicit, and infinite, family of such fields see for example Louboutin [36].) In this context it therefore seems worth noting that the only previous verification of  $\text{eTNC}_p$  for an abelian variety  $A$  and a Galois extension of degree divisible by  $p$  is given by Bley in [5, Corollary 1.4 and Remark 4.1] where it is assumed, amongst other things, that  $A$  is an elliptic curve,  $F$  is an abelian extension of  $\mathbb{Q}$  of exponent  $p$  and, critically, that the rank of  $A$  over  $F$  is equal to zero.

In addition to the proof of Theorem 1.1, in §6 we will also provide further explicit examples in which our approach leads to a proof of  $\text{eTNC}_p$  in cases for which  $p$  divides the degree of the relevant extension. More precisely, we show that for certain elliptic curves  $A$  the validity of  $\text{eTNC}_p$  with  $p = 3$  follows from that of the relevant cases of the Birch and Swinnerton-Dyer conjecture for a family of  $S_3$ -extensions of number fields (see Corollary 6.2) and provide examples (with  $p = 5$  and  $p = 7$ ) in which our approach allows  $\text{eTNC}_p$  to be verified by numerical computations (see §6.3).

In order to prove the above results we must first establish several intermediate results which are both more general and also we feel of some independent interest. To briefly discuss these results, we fix an abelian variety  $A$  over a number field  $k$ , a finite Galois extension  $F$  of  $k$  with Galois group  $G$  and an odd prime  $p$ .

In §4 we shall first compute, under some not-too-stringent conditions on  $A$  and  $F$ , the ‘algebraic part’ of the  $p$ -component of the equivariant Tamagawa number of the pair  $(h^1(A/F)(1), \mathbb{Z}[G])$ . This computation requires a close analysis of certain refined Euler characteristics (in the sense reviewed in §4.1) that are constructed by combining the finite support cohomology complex of Bloch and Kato for the base change through  $F/k$  of the  $p$ -adic Tate module of the dual  $A^t$  of  $A$  together with the Néron-Tate height of  $A$  relative to the field  $F$ . We note that the main result of this analysis constitutes a natural equivariant refinement and/or generalisation of several earlier computations in

this area including those that are made by Venjakob in [50, §3.1], by Bley in [3], by Kings in [35, Lecture 3] and by the first named author in [14, §12].

The detailed computation made in §4 then allows us in §5 to interpret the relevant case of  $e\text{TNC}_p$  as a family of  $p$ -adic congruence relations between the values at  $s = 1$  of higher derivatives of the Hasse-Weil  $L$ -functions of twists of  $A$  by irreducible complex characters of  $G$ , suitably normalised by a product of explicit equivariant regulators and periods.

We next describe several interesting (conjectural) consequences of this reinterpretation of  $e\text{TNC}_p$ , including the predicted annihilation as a Galois module of the  $p$ -primary Tate-Shafarevich of  $A^t$  over  $F$  by elements which interpolate the (suitably normalised) values at  $s = 1$  of higher derivatives of twisted Hasse-Weil  $L$ -functions (see Proposition 5.2 and Proposition 5.6).

By using results on the explicit Galois structure of Selmer groups that are obtained in [18], we then show that for generalised dihedral groups  $G$  the necessary  $p$ -adic congruence relations can be made very explicit even in the case that  $A$  has strictly positive rank over  $F$  (see Theorem 5.8).

The latter explicit interpretation is then used as a key step in the proof of Theorem 1.1.

We note finally that there are several ways in which it seems reasonable to expect that some of the explicit computations made in §4 could (with perhaps considerably more effort) be extended and our overall approach thereby generalised and that we hope such possibilities will be further explored in subsequent articles.

**1.1. Acknowledgements.** The authors are very grateful to Werner Bley and Stefano Vigni for helpful discussions and correspondence and to the anonymous referee for making several useful suggestions.

## 2. NOTATIONS AND SETTING

For any finite group  $\Gamma$  we use the following notation. We write  $\text{Ir}(\Gamma)$  for the set of irreducible  $E$ -valued characters of  $\Gamma$ , where  $E$  denotes either  $\mathbb{C}$  or  $\mathbb{C}_p$  (and the intended meaning will always be clear from the context). We also write  $\mathbf{1}_\Gamma$  for the trivial character of  $\Gamma$  and  $\check{\psi}$  for the contragredient of each  $\psi$  in  $\text{Ir}(\Gamma)$ . For each  $\psi$  in  $\text{Ir}(\Gamma)$  we write

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

for the primitive idempotent of the centre  $\zeta(E[\Gamma])$  of the group ring  $E[\Gamma]$ . For each  $E$ -valued character  $\psi$  we also fix an  $E[\Gamma]$ -module  $V_\psi$  of character  $\psi$ .

For any abelian group  $M$  we write  $M_{\text{tor}}$  for its torsion subgroup and  $M_{\text{tf}}$  for the quotient  $M/M_{\text{tor}}$ , which we often regard as a subgroup of  $\mathbb{Q} \otimes_{\mathbb{Z}} M$ . For any prime  $p$  we write  $M[p]$  for the subgroup  $\{m \in M : pm = 0\}$  of the Sylow  $p$ -subgroup  $M[p^\infty]$  of  $M_{\text{tor}}$ . We also set  $M_p := \mathbb{Z}_p \otimes_{\mathbb{Z}} M$  and write  $M_p^\wedge$  for the pro- $p$ -completion  $\varprojlim_n M/p^n M$ . If  $M$  is finitely generated, then we set  $\text{rk}(M) := \dim_{\mathbb{Q}}(\mathbb{Q} \otimes_{\mathbb{Z}} M)$ .

For any  $\mathbb{Z}_p[\Gamma]$ -module  $M$  we write  $M^\vee$  for the Pontryagin dual  $\text{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$  and  $M^*$  for the linear dual  $\text{Hom}_{\mathbb{Z}_p}(M, \mathbb{Z}_p)$ , each endowed with the natural contragredient action of  $\Gamma$ . If  $M$  is finitely generated, then for any field extension  $F$  of  $\mathbb{Q}_p$  we set  $F \cdot M := F \otimes_{\mathbb{Z}_p} M$ .

For any Galois extension of fields  $L/K$  we write  $G_{L/K}$  in place of  $\text{Gal}(L/K)$ . We also fix an algebraic closure  $K^c$  of  $K$  and abbreviate  $G_{K^c/K}$  to  $G_K$ . For each non-archimedean place  $v$  of a number field we write  $\kappa_v$  for its residue field.

Throughout this paper, we will consider the following situation. We have a fixed odd prime  $p$  and a Galois extension  $F/k$  of number fields with Galois group  $G = G_{F/k}$ . We choose a  $p$ -Sylow subgroup  $P$  in  $G$  and set  $K := F^P$ . We give ourselves an abelian variety  $A$  of dimension  $d$  defined over  $k$ . We write  $A^t$  for the dual abelian variety of  $A$ .

For each intermediate field  $L$  of  $F/k$  we write  $S_p^L$ ,  $S_r^L$  and  $S_b^L$  for the set of non-archimedean places of  $L$  that are  $p$ -adic, which ramify in  $F/L$  and at which  $A/L$  has bad reduction respectively. Similarly, we write  $S_\infty^L$ ,  $S_\mathbb{R}^L$  and  $S_\mathbb{C}^L$  for the set of archimedean, real and complex places of  $L$  respectively. The notation  $S_?$  will stand for  $S_?^k$  when “?” is  $b, r, p, \infty, \mathbb{R}$  or  $\mathbb{C}$ .

For each such field  $L$  we also set  $\text{rk}(A_L) := \text{rk}(A(L))$  and write  $\text{III}_p(A_L)$  and  $\text{Sel}_p(A_L)$  for the  $p$ -primary Tate-Shafarevich and Selmer groups of  $A/L$ . We recall that there exists a canonical exact sequence of the form

$$(1) \quad 0 \longrightarrow \text{III}_p(A_L)^\vee \longrightarrow \text{Sel}_p(A_L)^\vee \longrightarrow A(L)_p^* \longrightarrow 0.$$

### 3. THE HYPOTHESES

Fix an odd prime  $p$ , number fields  $k, F$  and  $K = F^P$  and an abelian variety  $A$  as described above. Then throughout this article we will find it convenient to assume that this data satisfies the following hypotheses:

- (a)  $A(K)[p] = 0$  and  $A^t(K)[p] = 0$ ;
- (b) The Tamagawa number of  $A/K$  at each place in  $S_b^K$  is not divisible by  $p$ ;
- (c)  $A/K$  has good reduction at all  $p$ -adic places;
- (d) For all  $p$ -adic places  $v$  that ramify in  $F/K$ , the reduction is ordinary and  $A(\kappa_v)[p] = 0$ ;
- (e) No place of bad reduction for  $A/k$  is ramified in  $F/k$ , i.e.  $S_b \cap S_r = \emptyset$ .
- (f) For any place  $v$  in  $K$  such that the primes above it in  $F$  are ramified in  $F/k$ , we have  $A(\kappa_v)[p] = 0$ ;
- (g) The Tate-Shafarevich group  $\text{III}(A_F)$  is finite.

*Remark 3.1.* For a fixed abelian variety  $A$  over  $k$  and extension  $K/k$  the hypotheses (a), (b) and (c) are clearly satisfied by all but finitely many primes  $p$  (which do not divide the degree of  $K/k$ ), the hypotheses (e) and (f) constitute a mild restriction on the ramification of  $F/k$  and the hypothesis (g) is famously conjectured to be true in all cases. However, the hypothesis (d) excludes the case that is called ‘anomalous’ by Mazur in [38] and, for a given  $A$ , there may be infinitely many primes  $p$  for which there are  $p$ -adic places  $v$  at which  $A$  has good ordinary reduction but  $A(\kappa_v)[p]$  does not vanish. Nevertheless, it is straightforward to describe examples of abelian varieties  $A$  for which there are only finitely many such anomalous places – see, for example, the result of Mazur and Rubin in [39, Lemma A.5].

*Remark 3.2.* In the analysis of finite support cohomology complexes that is given in Lemma 4.1 below we find it convenient to adopt the convention of considering the  $p$ -adic Tate module of  $A^t$  rather than that of  $A$  itself. Applications of the hypotheses (b)–(f) in this article will therefore often take place with  $A$  replaced by  $A^t$ . In this regard, we note that the validity of each of these hypotheses as currently formulated is equivalent to the validity of the corresponding hypothesis with  $A$  replaced by  $A^t$  and we will henceforth use this fact without further explicit comment.

### 4. CANONICAL EULER CHARACTERISTICS

In most of this section we assume that the fixed data  $p, k, F, K$  and  $A$  satisfy all of the hypotheses (a)–(g) that are listed in §3.

Our main aim is to compute explicitly the natural (refined) Euler characteristic that is associated to the pair comprising the Bloch-Kato finite support cohomology complex of the base-change through  $F/k$  of the  $p$ -adic Tate module of the dual abelian variety  $A^t$  of  $A$  and the Néron-Tate height of  $A$  relative to the field  $F$ .

**4.1. Euler characteristics.** We first quickly review the definition of refined Euler characteristics that will play an essential role in the sequel. For convenience, we shall only give an explicit construction in the relevant special case rather than discussing the general approach (which is given in [13])

For any finite group  $\Gamma$  we write  $D(\mathbb{Z}_p[\Gamma])$  for the derived category of complexes of (left)  $\mathbb{Z}_p[\Gamma]$ -modules. We also write  $D^{\text{p}}(\mathbb{Z}_p[\Gamma])$  for the full triangulated subcategory of  $D(\mathbb{Z}_p[\Gamma])$  comprising complexes that are ‘perfect’ (that is, isomorphic in  $D(\mathbb{Z}_p[\Gamma])$  to a bounded complex of finitely generated projective  $\mathbb{Z}_p[\Gamma]$ -modules).

We assume to be given a complex  $C$  in  $D^{\text{p}}(\mathbb{Z}_p[G])$  which is acyclic outside degrees  $a$  and  $a+1$  for any given integer  $a$  and such that  $H^a(C)$  is  $\mathbb{Z}_p$ -free. We also assume to be given an isomorphism of  $\mathbb{C}_p[G]$ -modules  $\lambda : \mathbb{C}_p \otimes_{\mathbb{Z}_p} H^a(C) \cong \mathbb{C}_p \otimes_{\mathbb{Z}_p} H^{a+1}(C)$ . Then, under these hypotheses, it can be shown that there exists an isomorphism  $\iota : P^\bullet \cong C$  in  $D^{\text{p}}(\mathbb{Z}_p[G])$  where  $P^\bullet$  is a complex of  $\mathbb{Z}_p[G]$ -modules of the form  $P \xrightarrow{d} P$  where  $P$  is finitely generated and projective and the first term occurs in degree  $a$ . We then consider the following auxiliary composite isomorphism of  $\mathbb{C}_p[G]$ -modules

$$\begin{aligned} \lambda_{P^\bullet} : \mathbb{C}_p \otimes_{\mathbb{Z}_p} P &\cong (\mathbb{C}_p \otimes_{\mathbb{Z}_p} H^a(P^\bullet)) \oplus (\mathbb{C}_p \otimes_{\mathbb{Z}_p} \text{im}(d)) \\ &\cong (\mathbb{C}_p \otimes_{\mathbb{Z}_p} H^{a+1}(P^\bullet)) \oplus (\mathbb{C}_p \otimes_{\mathbb{Z}_p} \text{im}(d)) \cong \mathbb{C}_p \otimes_{\mathbb{Z}_p} P \end{aligned}$$

where the first and third maps are obtained by choosing  $\mathbb{C}_p[G]$ -equivariant splittings of the tautological surjections  $\mathbb{C}_p \otimes_{\mathbb{Z}_p} P \rightarrow \mathbb{C}_p \otimes_{\mathbb{Z}_p} \text{im}(d)$  and  $\mathbb{C}_p \otimes_{\mathbb{Z}_p} P \rightarrow \mathbb{C}_p \otimes_{\mathbb{Z}_p} H^{a+1}(P^\bullet)$  respectively and the second is  $((\mathbb{C}_p \otimes_{\mathbb{Z}_p} H^{a+1}(\iota))^{-1} \circ \lambda \circ (\mathbb{C}_p \otimes_{\mathbb{Z}_p} H^a(\iota)), \text{id})$ .

We now write  $K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$  for the relative algebraic  $K$ -group of the inclusion  $\mathbb{Z}_p[G] \subset \mathbb{C}_p[G]$  and recall that this group is generated by elements of the form  $[Q, \mu, Q']$  where  $Q$  and  $Q'$  are finitely generated projective  $\mathbb{Z}_p[G]$ -modules and  $\mu$  is an isomorphism of  $\mathbb{C}_p[G]$ -modules  $\mathbb{C}_p \otimes_{\mathbb{Z}_p} Q \cong \mathbb{C}_p \otimes_{\mathbb{Z}_p} Q'$ .

In particular, in terms of this description, it can be shown that the element of  $K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$  obtained by setting

$$\chi_{G,p}(C, \lambda) := (-1)^a [P, \lambda_{P^\bullet}, P]$$

is independent of the choice of isomorphism  $\iota$  (and hence of the module  $P$ ) and of the splittings made when defining the isomorphism  $\lambda_{P^\bullet}$ . This element will be referred to as the ‘refined Euler characteristic’ of the pair  $(C, \lambda)$  in the sequel.

**4.2. Cohomology with finite support.** We now turn to consider the finite support cohomology complex of the  $p$ -adic Tate module  $T_p(A)$  of  $A^t$ .

To do this we write  $\Sigma_k(F)$  for the set of  $k$ -embeddings  $F \rightarrow k^c$  and  $Y_{F/k,p}$  for the module  $\prod_{\Sigma_k(F)} \mathbb{Z}_p$ , endowed with the obvious action of  $G \times G_k$ .

Then the  $p$ -adic Tate module of the base change of  $A^t$  through  $F/k$  is equal to

$$T_{p,F}(A) := Y_{F/k,p} \otimes_{\mathbb{Z}_p} T_p(A),$$

where  $G$  acts naturally on the first factor and  $G_k$  acts diagonally. We set  $V_{p,F}(A) := \mathbb{Q}_p T_{p,F}(A)$ .

For each place  $v$  of  $k$  we set  $G_v := G_{k_v}$  and write  $I_v$  for the inertia subgroup of  $G_v$ . We also fix a place  $w$  of  $F$  above  $v$  and a corresponding embedding  $F \rightarrow k_v^c$  and write  $\bar{G}_v$  and  $\bar{I}_v$  for the images of  $G_v$  and  $I_v$  under the induced homomorphism  $G_v \rightarrow G$ .

For each non-archimedean place  $v$  we then define a complex of  $\mathbb{Z}_p[G]$ -modules by setting

$$R\Gamma_f(k_v, T_{p,F}(A)) := \begin{cases} T_{p,F}(A)^{I_v} \xrightarrow{1 - \text{Fr}_v^{-1}} T_{p,F}(A)^{I_v}, & \text{if } v \nmid p \\ H_f^1(k_v, T_{p,F}(A))[-1], & \text{if } v \mid p \end{cases}$$

where, if  $v \nmid p$ , the first occurrence of  $T_{p,F}(A)^{I_v}$  is placed in degree zero and  $\text{Fr}_v$  is the natural Frobenius in  $G_v/I_v$  and, if  $v \mid p$ , then  $H_f^1(k_v, T_{p,F}(A))$  denotes the full pre-image in  $H^1(k_v, T_{p,F}(A))$  of the ‘finite part’ subspace  $H_f^1(k_v, V_{p,F}(A))$  of  $H^1(k_v, V_{p,F}(A))$  that is defined by Bloch and Kato in [8, (3.7.2)].

We next define  $R\Gamma_{/f}(k_v, T_{p,F}(A))$  to be a complex of  $\mathbb{Z}_p[G]$ -modules which lies in an exact triangle in  $D(\mathbb{Z}_p[G])$  of the form

$$(2) \quad R\Gamma_f(k_v, T_{p,F}(A)) \xrightarrow{\varpi_v} R\Gamma(k_v, T_{p,F}(A)) \xrightarrow{\varpi'_v} R\Gamma_{/f}(k_v, T_{p,F}(A)) \longrightarrow$$

where  $\varpi_v$  is the natural inflation morphism if  $v \nmid p$ , and is induced by the inclusion  $H_f^1(k_v, T_{p,F}(A)) \subseteq H^1(k_v, T_{p,F}(A))$  and the fact that  $R\Gamma(k_v, T_{p,F}(A))$  is acyclic in degrees less than one, if  $v \mid p$ . We finally set  $S := S_r \cup S_b$ , write  $\mathcal{O}_{k,S}$  for the subring of  $k$  comprising elements that are integral at all non-archimedean places outside  $S$  and define the complex  $R\Gamma_f(k, T_{p,F}(A))$  so that it lies in an exact triangle in  $D(\mathbb{Z}_p[G])$  of the form

$$(3) \quad R\Gamma_f(k, T_{p,F}(A)) \longrightarrow R\Gamma\left(\mathcal{O}_{k,S}\left[\frac{1}{p}\right], T_{p,F}(A)\right) \xrightarrow{\varpi'} \bigoplus_{v \in S \cup S_p} R\Gamma_{/f}(k_v, T_{p,F}(A)) \longrightarrow .$$

Here each  $v$ -component of  $\varpi'$  is equal to the composite of the natural localisation morphism  $R\Gamma(\mathcal{O}_{k,S}[\frac{1}{p}], T_{p,F}(A)) \rightarrow R\Gamma(k_v, T_{p,F}(A))$  in étale cohomology and the morphism  $\varpi'_v$ .

In the sequel we also set

$$H_f^i(k, T_{p,F}(A)) := H^i(R\Gamma_f(k, T_{p,F}(A)))$$

in each degree  $i$ .

**Lemma 4.1.**

- (i) *Assume that  $A$  and  $F$  satisfy the hypotheses (c)–(f). Then  $R\Gamma_f(k, T_{p,F}(A))$  belongs to  $D^p(\mathbb{Z}_p[G])$ . In addition, for any non-archimedean place  $v$  of  $k$  which ramifies in  $F/k$  and does not divide  $p$ , the complex  $R\Gamma_f(k_v, T_{p,F}(A))$  is acyclic.*
- (ii) *Assume that  $A$  and  $F$  satisfy the hypotheses (a), (b), (e) and (g). Then the complex  $R\Gamma_f(k, T_{p,F}(A))$  is acyclic outside degrees one and two and there are canonical identifications of  $H_f^1(k, T_{p,F}(A))$  and  $H_f^2(k, T_{p,F}(A))$  with  $A^\dagger(F)_p$  and  $\text{Sel}_p(A_F)^\vee$  respectively.*

*Proof.* First, since  $p$  is odd and  $T_{p,F}(A)$  is a (finitely generated) free  $\mathbb{Z}_p[G]$ -module the complexes  $R\Gamma(\mathcal{O}_{k,S}[\frac{1}{p}], T_{p,F}(A))$  and  $R\Gamma(k_v, T_{p,F}(A))$  for each place  $v$  of  $k$  belong to  $D^p(\mathbb{Z}_p[G])$ . In view of the exact triangles (2) and (3), claim (i) will therefore follow if we can show that for each  $v$  in  $S \cup S_p$  the complex  $R\Gamma_f(k_v, T_{p,F}(A))$  belongs to  $D^p(\mathbb{Z}_p[G])$ , or equivalently (as  $P$  is a Sylow  $p$ -subgroup) that it belongs to  $D^p(\mathbb{Z}_p[P])$ .

We first consider the case  $v \nmid p$ . In this case  $R\Gamma_f(k_v, T_{p,F}(A))$  is isomorphic in  $D(\mathbb{Z}_p[P])$  to  $R\Gamma_f(K_{w'}, T_p)$  where we write  $w'$  for a place in  $K$  below  $w$  and set  $T_p := \mathbb{Z}_p[P] \otimes_{\mathbb{Z}_p} T_p(A/K)$ .

In particular, even without assuming our hypotheses, if the ramification index of  $v$  in  $F/k$  is not divisible by  $p$ , then  $w'$  is unramified in  $F/K$  so  $T_p^{I_{w'}} \cong \mathbb{Z}_p[P] \otimes_{\mathbb{Z}_p} T_p(A)^{I_{w'}}$  is a free  $\mathbb{Z}_p[P]$ -module and so  $R\Gamma_f(K_{w'}, T_p)$  belongs to  $D^p(\mathbb{Z}_p[P])$ .

Next we show that hypotheses (e) and (f) imply that if  $w'$  ramifies in  $F/k$  and  $v \nmid p$ , then  $R\Gamma_f(K_{w'}, T_p)$  (and therefore also  $R\Gamma_f(k_v, T_{p,F}(A))$ ) is acyclic. We write  $d^0$  for the differential in degree 0 of  $R\Gamma_f(K_{w'}, T_p)$ . Then it is clear that  $\ker(d^0) = T_p^{G_{w'}}$  vanishes and so it suffices to prove  $\text{cok}(d^0)$  vanishes or equivalently, since  $P$  and  $\text{cok}(d^0)$  are finite  $p$ -groups, that  $\text{cok}(d^0)_P$  vanishes.



vanishes as a consequence of (b) and the fact that  $H^0\left(K_{w'}, H^1(I_{w'}, T_p(A))_{\text{tor}}\right)$  has cardinality equal to the maximal power of  $p$  that divides the Tamagawa number of  $A_{/K}^t$  at  $w'$ . Since  $\overline{G}_{w'}$  is a  $p$ -group, this implies that  $H^0(F_w, H^1(I_w, T_p(A))_{\text{tor}})$  vanishes, as required to complete the proof of claim (ii).  $\square$

In the sequel we assume that  $A$ ,  $F$  and  $p$  satisfy the hypotheses (a)–(g). Then Lemma 4.1 implies that the complex

$$C_{A,F}^{f,\bullet} := R\Gamma_f(k, T_{p,F}(A))$$

belongs to  $DP(\mathbb{Z}_p[G])$ , is acyclic outside degrees one and two and is such that for each isomorphism of fields  $j : \mathbb{C} \cong \mathbb{C}_p$  there exists a canonical composite isomorphism of  $\mathbb{C}_p[G]$ -modules of the form

$$\begin{aligned} \lambda_{A,F}^{\text{NT},j} : \mathbb{C}_p \otimes_{\mathbb{Z}_p} H^1(C_{A,F}^{f,\bullet}) &\cong \mathbb{C}_p \otimes_{\mathbb{Z}_p} A^t(F)_p \\ &\cong \mathbb{C}_p \otimes_{\mathbb{C},j} (\mathbb{C} \otimes_{\mathbb{Z}} A^t(F)) \cong \mathbb{C}_p \otimes_{\mathbb{C},j} \text{Hom}_{\mathbb{C}}(\mathbb{C} \otimes_{\mathbb{Z}} A(F), \mathbb{C}) \\ &\cong \mathbb{C}_p \otimes_{\mathbb{Z}_p} \text{Hom}_{\mathbb{Z}_p}(A(F)_p, \mathbb{Z}_p) \cong \mathbb{C}_p \otimes_{\mathbb{Z}_p} H^2(C_{A,F}^{f,\bullet}) \end{aligned}$$

in which the central isomorphism is induced by the  $\mathbb{C}$ -linear extension to  $\mathbb{C} \otimes_{\mathbb{Z}} A(F)$  of the Néron-Tate height of  $A$  relative to the field  $F$ .

Hypothesis (a) implies that the  $p$ -group  $P$  acts on  $A(F)[p]$  with a single fixed point and hence that the module  $A^t(F)_p \cong H^1(C_{A,F}^{f,\bullet})$  is  $\mathbb{Z}_p$ -free and so the above observations imply that the construction in §4.1 applies to the pair  $(C_{A,F}^{f,\bullet}, \lambda_{A,F}^{\text{NT},j})$  to give a canonical Euler characteristic

$$\chi_j(A, F/k) := -\chi_{G,p}(C_{A,F}^{f,\bullet}, \lambda_{A,F}^{\text{NT},j})$$

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

This element  $\chi_j(A, F/k)$  encodes detailed information about a range of aspects of the arithmetic of  $A/F$  and in the remainder of §4 we shall explicitly relate it to the equivariant Tamagawa numbers that are defined in [16]. In §5 this comparison result plays a key role in the formulation of a precise conjectural description of a pre-image of  $\chi_j(A, F/k)$  under the boundary homomorphism  $K_1(\mathbb{C}_p[G]) \rightarrow K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$ .

**4.3. The element  $R\Omega_j(h^1(A/F)(1), \mathbb{Z}[G])$ .** For each isomorphism  $j : \mathbb{C} \cong \mathbb{C}_p$  as above there is an induced composite homomorphism of abelian groups

$$(4) \quad j_{G,*} : K_0(\mathbb{Z}[G], \mathbb{R}[G]) \rightarrow K_0(\mathbb{Z}[G], \mathbb{C}[G]) \cong K_0(\mathbb{Z}[G], \mathbb{C}_p[G]) \rightarrow K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$$

(where the first and third arrows are induced by the inclusions  $\mathbb{R}[G] \subset \mathbb{C}[G]$  and  $\mathbb{Z}[G] \subset \mathbb{Z}_p[G]$  respectively).

For each such  $j$  we set

$$R\Omega_j(h^1(A/F)(1), \mathbb{Z}[G]) := j_{G,*}\left(R\Omega(h^1(A/F)(1), \mathbb{Z}[G])\right)$$

where  $R\Omega(h^1(A/F)(1), \mathbb{Z}[G])$  is the ‘algebraic part’ of the equivariant Tamagawa number for the pair  $(h^1(A/F)(1), \mathbb{Z}[G])$ , as defined (unconditionally under the assumed validity of hypothesis (g)) in [16, §3.4].

In order to relate this element to the Euler characteristic  $\chi_j(A, F/k)$  defined above we must first introduce an auxiliary element of  $K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$ .

To do this we define a complex

$$C_{A,F}^{\text{loc},\bullet} := \bigoplus_{v \in S_\infty} R\Gamma(k_v, T_{p,F}(A)) \oplus \bigoplus_{v \in S \cup S_p} R\Gamma_f(k_v, T_{p,F}(A)),$$

where, as before,  $S$  denotes  $S_{\text{r}} \cup S_{\text{b}}$ . It is then clear that  $C_{A,F}^{\text{loc},\bullet}$  is acyclic outside degrees zero and one, that  $H^0(C_{A,F}^{\text{loc},\bullet}) = \bigoplus_{v \in S_{\infty}} H^0(k_v, T_{p,F}(A))$  and that there is a canonical identification of  $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1(C_{A,F}^{\text{loc},\bullet})$  with  $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} A^t(F_p)_p^{\wedge}$ , where we set  $F_p := F \otimes_{\mathbb{Q}} \mathbb{Q}_p$ .

We next use this description of the cohomology of  $C_{A,F}^{\text{loc},\bullet}$  to define a canonical isomorphism of  $\mathbb{C}_p[G]$ -modules

$$\lambda_{A,F}^{\text{exp},j} : \mathbb{C}_p \otimes_{\mathbb{Z}_p} H^0(C_{A,F}^{\text{loc},\bullet}) \cong \mathbb{C}_p \otimes_{\mathbb{Z}_p} H^1(C_{A,F}^{\text{loc},\bullet}).$$

For this we write  $\Sigma(k)$  for the set of embeddings  $k \rightarrow \mathbb{C}$  and  $\Sigma_{\sigma}(F)$ , for each  $\sigma$  in  $\Sigma(k)$ , for the set of embeddings  $F \rightarrow \mathbb{C}$  that extend  $\sigma$ . For  $v$  in  $S_{\infty}$  we fix a corresponding element  $\sigma_v$  of  $\Sigma(k)$  and consider the  $\mathbb{C}$ -linear map

$$\begin{aligned} \pi_v : \mathbb{C} \otimes_{\mathbb{Z}} H_1(\sigma_v(A^t)(\mathbb{C}), \mathbb{Z}) \\ \longrightarrow \text{Hom}_{\mathbb{C}}\left(\mathbb{C} \otimes_{k, \sigma_v} H^0(A^t, \Omega_{A^t}^1), \mathbb{C}\right) = \mathbb{C} \otimes_{k, \sigma_v} \text{Hom}_k(H^0(A^t, \Omega_{A^t}^1), k) \end{aligned}$$

that sends the image  $\gamma$  in  $H_1(\sigma_v(A^t)(\mathbb{C}), \mathbb{Z})$  of a cycle  $\hat{\gamma}$  to the map induced by sending a differential  $\omega$  to  $\int_{\hat{\gamma}} \omega := \int_{\hat{\gamma}} \omega$ .

For each place  $v$  in  $S_{\infty}$  we also write  $Y_{v,F}$  for the module  $\prod_{\Sigma_{\sigma_v}(F)} \mathbb{Z}$ , endowed with its natural action of the direct product  $G \times G_v$ , and then define  $\lambda_{A,F}^{\text{exp},j}$  to be the following composite isomorphism of  $\mathbb{C}_p[G]$ -modules

$$\begin{aligned} \mathbb{C}_p \otimes_{\mathbb{Z}_p} H^0(C_{A,F}^{\text{loc},\bullet}) &= \mathbb{C}_p \otimes_{\mathbb{Z}_p} \bigoplus_{v \in S_{\infty}} H^0(k_v, T_{p,F}(A)) \\ &\cong \mathbb{C}_p \otimes_{\mathbb{Z}} \bigoplus_{v \in S_{\infty}} H^0\left(k_v, Y_{v,F} \otimes_{\mathbb{Z}} H_1(\sigma_v(A^t)(\mathbb{C}), \mathbb{Z})\right) \\ &\cong \mathbb{C}_p \otimes_{\mathbb{Q}} \left(F \otimes_k \text{Hom}_k(H^0(A^t, \Omega_{A^t}^1), k)\right) \\ &\cong \mathbb{C}_p \otimes_{\mathbb{Z}_p} A^t(F_p)_p^{\wedge} \\ &= \mathbb{C}_p \otimes_{\mathbb{Z}_p} H^1(C_{A,F}^{\text{loc},\bullet}). \end{aligned}$$

Here the first isomorphism is induced by the canonical comparison isomorphisms

$$(5) \quad T_{p,F}(A) = Y_{F/k,p} \otimes_{\mathbb{Z}_p} T_p(A) \cong Y_{v,F,p} \otimes_{\mathbb{Z}_p} H_1(\sigma_v(A^t)(\mathbb{C}), \mathbb{Z})_p,$$

the second by the maps  $\mathbb{C}_p \otimes_{\mathbb{C},j} \pi_v$  and the canonical decomposition

$$\begin{aligned} (6) \quad \mathbb{R} \otimes_{\mathbb{Q}} \left(F \otimes_k \text{Hom}_k(H^0(A^t, \Omega_{A^t}^1), k)\right) \\ \cong \bigoplus_{v \in S_{\infty}} H^0\left(k_v, (\mathbb{C} \otimes_{k, \sigma} F) \otimes_{\mathbb{C}} (\mathbb{C} \otimes_{k, \sigma} \text{Hom}_k(H^0(A^t, \Omega_{A^t}^1), k))\right) \\ \cong \bigoplus_{v \in S_{\infty}} H^0\left(k_v, \mathbb{C} Y_{v,F} \otimes_{\mathbb{C}} (\mathbb{C} \otimes_{k, \sigma} \text{Hom}_k(H^0(A^t, \Omega_{A^t}^1), k))\right), \end{aligned}$$

and the third by the sum over places  $v$  in  $S_p$  of the classical exponential map

$$(7) \quad F_v \otimes_k \text{Hom}_k(H^0(A^t, \Omega_{A^t}^1), k) \cong \text{Hom}_{F_v}(H^0(A^t_{/F_v}, \Omega_{A^t_{/F_v}}^1), F_v) \cong \mathbb{Q}_p A^t(F_v)_p^{\wedge}$$

where we set  $F_v := F \otimes_k k_v$ .

Under our stated hypotheses the complex  $C_{A,F}^{\text{loc},\bullet}$  belongs to  $D^{\text{p}}(\mathbb{Z}_p[G])$ . It is also acyclic outside degrees zero and one and such that  $H^0(C_{A,F}^{\text{loc},\bullet})$  is  $\mathbb{Z}_p$ -free and so we may use the construction of §4.1

to define an element of  $K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$  by setting

$$\chi_j^{\text{loc}}(A, F/k) := \chi_{G,p} \left( C_{A,F}^{\text{loc}, \bullet}, \lambda_{A,F}^{\text{exp}, j} \right).$$

We are now ready to state the main result of this section. In this result, and the sequel, we shall use the composite homomorphism

$$\delta_{G,p} : \zeta(\mathbb{C}_p[G])^\times \rightarrow K_1(\mathbb{C}_p[G]) \rightarrow K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$$

where the first arrow is the inverse of the (bijective) reduced norm homomorphism  $\text{Nrd}_{\mathbb{C}_p[G]}$  and the second is the standard boundary homomorphism  $\partial_{G,p}$ .

**Proposition 4.2.** *Assume that  $A$  and  $F$  satisfy the hypotheses (a)–(g). Then in  $K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$  one has*

$$R\Omega_j(h^1(A/F)(1), \mathbb{Z}[G]) = -\chi_j(A, F/k) - \chi_j^{\text{loc}}(A, F/k) + \sum_{v \in S \cup S_p} \delta_{G,p}(L_v(A, F/k)).$$

Here for each place  $v$  in  $S \cup S_p$  we set

$$L_v(A, F/k) := \begin{cases} \text{Nrd}_{\mathbb{Q}_p[G]}(1 - \text{Fr}_v^{-1} \mid V_{p,F}(A)^{I_v}), & \text{if } v \nmid p \\ \text{Nrd}_{\mathbb{Q}_p[G]}(1 - \varphi_v \mid D_{\text{cr},v}(V_{p,F}(A))), & \text{if } v \mid p, \end{cases}$$

where  $\varphi_v$  is the crystalline Frobenius at  $v$ .

*Proof.* To discuss  $R\Omega_j(h^1(A/F)(1), \mathbb{Z}[G])$  we first recall relevant facts concerning the formalism of virtual objects introduced by Deligne in [24] (for more details see [16, §2]).

With  $R$  denoting either  $\mathbb{Z}_p[G]$  or  $\mathbb{C}_p[G]$  we write  $V(R)$  for the category of virtual objects over  $R$  and  $[C]_R$  for the object of  $V(R)$  associated to each  $C$  in  $D^p(R)$ . Then  $V(R)$  is a Picard category with  $\pi_1(V(R))$  naturally isomorphic to  $K_1(R)$  (see [16, (2)]) and we write  $(X, Y) \mapsto X \cdot Y$  for its product and  $\mathbf{1}_R$  for the unit object  $[0]_R$ . Writing  $\mathcal{P}_0$  for the Picard category with unique object  $\mathbf{1}_{\mathcal{P}_0}$  and  $\text{Aut}_{\mathcal{P}_0}(\mathbf{1}_{\mathcal{P}_0}) = 0$  we use the isomorphism of abelian groups

$$(8) \quad \pi_0 \left( V(\mathbb{Z}_p[G]) \times_{V(\mathbb{C}_p[G])} \mathcal{P}_0 \right) \cong K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$$

that is described in [16, Proposition 2.5]. In particular, via this isomorphism, each pair comprising an object  $X$  of  $V(\mathbb{Z}_p[G])$  and a morphism  $\iota : \mathbb{C}_p[G] \otimes_{\mathbb{Z}_p[G]} X \rightarrow \mathbf{1}_{\mathbb{C}_p[G]}$  gives rise to a canonical element  $[X, \iota]$  of  $K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$ .

Now if  $C$  belongs to  $D^p(\mathbb{Z}_p[G])$  and is acyclic outside degrees  $a$  and  $a+1$  (for any integer  $a$ ), then any isomorphism  $\lambda : H^a(\mathbb{C}_p \otimes_{\mathbb{Z}_p} C) \cong H^{a+1}(\mathbb{C}_p \otimes_{\mathbb{Z}_p} C)$  of  $\mathbb{C}_p[G]$ -modules gives a canonical morphism  $\lambda_{\text{Triv}} : [\mathbb{C}_p \otimes_{\mathbb{Z}_p} C]_{\mathbb{C}_p[G]} \rightarrow \mathbf{1}_{\mathbb{C}_p[G]}$  in  $V(\mathbb{C}_p[G])$ . The associated element  $[[C]_{\mathbb{Z}_p[G]}, \lambda_{\text{Triv}}]$  of  $K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$  coincides with the Euler characteristic  $\chi_{\mathbb{Z}_p[G], \mathbb{C}_p[G]}(C, \lambda^{(-1)^a})$  defined in [11, Definition 5.5]. In particular, from Proposition 5.6(3) in loc. cit. it follows that  $[[C[-1]]_{\mathbb{Z}_p[G]}, \lambda_{\text{Triv}}] = -[[C]_{\mathbb{Z}_p[G]}, \lambda_{\text{Triv}}]$ , whilst Theorem 6.2 and Lemma 6.3 in loc. cit. combine to imply that if  $H^a(C)$  is  $\mathbb{Z}_p$ -free, then

$$(9) \quad [[C]_{\mathbb{Z}_p[G]}, \lambda_{\text{Triv}}] = \chi_{G,p}(C, \lambda) + \delta_{G,p} \left( \prod_{i \equiv 1, 2 \pmod{4}} \text{Nrd}_{\mathbb{Q}_p[G]}(-\text{id} \mid \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^i(C))^{(-1)^i} \right),$$

where  $\chi_{G,p}(-, -)$  is the explicit Euler characteristic discussed in §4.1.

We now set

$$C_{A,F}^{c, \bullet} := R\Gamma_c(\mathcal{O}_{k,S}[\frac{1}{p}], T_{p,F}(A)),$$

which is the complex of the compactly supported étale cohomology of  $T_{p,F}(A)$  on  $\text{Spec}(\mathcal{O}_{k,S}[\frac{1}{p}])$ , regarded as a complex of  $\mathbb{Z}_p[G]$ -modules in the natural way.

Then a direct comparison of the definitions of  $C_{A,F}^{c,\bullet}$  and  $C_{A,F}^{f,\bullet}$  shows that there is a canonical exact triangle in  $D^p(\mathbb{Z}_p[G])$

$$(10) \quad C_{A,F}^{\text{loc},\bullet}[-1] \longrightarrow C_{A,F}^{c,\bullet} \longrightarrow C_{A,F}^{f,\bullet} \longrightarrow C_{A,F}^{\text{loc},\bullet}.$$

We consider the following diagram in  $V(\mathbb{C}_p[G])$

$$(11) \quad \begin{array}{ccc} [\mathbb{C}_p \otimes_{\mathbb{Z}_p} C_{A,F}^{c,\bullet}]_{\mathbb{C}_p[G]} & \xrightarrow{\Delta} & [\mathbb{C}_p \otimes_{\mathbb{Z}_p} C_{A,F}^{\text{loc},\bullet}[-1]]_{\mathbb{C}_p[G]} \cdot [\mathbb{C}_p \otimes_{\mathbb{Z}_p} C_{A,F}^{f,\bullet}]_{\mathbb{C}_p[G]} \\ \alpha \downarrow & & \downarrow [(\lambda_{A,F}^{\text{exp},j})_{\text{Triv}}]_{\mathbb{C}_p[G]} \cdot [(\lambda_{A,F}^{\text{NT},j})_{\text{Triv}}]_{\mathbb{C}_p[G]} \\ \mathbf{1}_{\mathbb{C}_p[G]} & \xrightarrow{\iota} & \mathbf{1}_{\mathbb{C}_p[G]} \cdot \mathbf{1}_{\mathbb{C}_p[G]} \\ \alpha' \downarrow & & \downarrow (\prod_{v \in S \cup S_p} L_v(A, F/k)) \cdot \text{id} \\ \mathbf{1}_{\mathbb{C}_p[G]} & \xrightarrow{\iota} & \mathbf{1}_{\mathbb{C}_p[G]} \cdot \mathbf{1}_{\mathbb{C}_p[G]}. \end{array}$$

Here  $\Delta$  is the morphism induced by the scalar extension of (10),  $\iota$  denotes the canonical identification and the morphisms  $\alpha$  and  $\alpha'$  are defined by the condition that the two squares commute.

We claim that this definition of  $\alpha$  and  $\alpha'$  implies that

$$(12) \quad \alpha' \circ \alpha = (\mathbb{C}_p \otimes_{\mathbb{R},j} \vartheta_\infty) \circ (\mathbb{C}_p \otimes_{\mathbb{Q}_p} \vartheta_p)^{-1}$$

where the morphisms  $\vartheta_\infty$  and  $\vartheta_p$  are as constructed in [16, §3.4]. To verify this we note that the scalar extension of (10) is naturally isomorphic to the exact triangle in  $D^p(\mathbb{C}_p[G])$  induced by the central column of the diagram [16, (26)] and then simply compare the explicit definitions of the morphisms  $\lambda_{A,F}^{\text{exp},j}$  and  $\vartheta_p$  and of  $\lambda_{A,F}^{\text{NT},j}$  and  $\vartheta_\infty$ . After this it only remains to note the following fact. For each place  $v \in S \setminus S_p$ , respectively  $v \in S_p$ , we write  $V_{p,v}$  and  $\phi_v$  for  $V_{p,F}(A)^{I_v}$  and  $\text{Fr}_v^{-1}$ , respectively  $D_{\text{cr},v}(V_{p,F}(A))$  and  $\varphi_v$ , and then  $V_{p,v}^\bullet$  for the complex  $V_{p,v} \xrightarrow{1-\phi_v} V_{p,v}$ , with the first term placed in degree zero. Our definition of  $\lambda_{A,F}^{\text{exp},j}$  implicitly uses the morphism  $[V_{p,v}^\bullet]_{\mathbb{Q}_p[G]} \rightarrow \mathbf{1}_{\mathbb{Q}_p[G]}$  induced by the acyclicity of  $V_{p,v}^\bullet$  whereas the definition of  $\vartheta_p$  uses (via [16, (19) and (22)]) the morphism  $[V_{p,v}^\bullet]_{\mathbb{Q}_p[G]} \rightarrow \mathbf{1}_{\mathbb{Q}_p[G]}$  induced by the identity map on  $V_{p,v}$ ; the occurrence of the morphism  $\alpha'$  in the equality (12) is thus accounted for by applying the remark made immediately after [16, (24)] to each of the complexes  $V_{p,v}^\bullet$  and noting that  $\text{Nrd}_{\mathbb{Q}_p[G]}(1 - \phi_v | V_{p,v}) = L_v(A, F/k)$ .

Now, taking into account the equality (12), the term  $R\Omega_j(h^1(A/F)(1), \mathbb{Z}[G])$  is defined in [16] to be equal to

$$\left[ [C_{A,F}^{c,\bullet}]_{\mathbb{Z}_p[G]}, (\mathbb{C}_p \otimes_{\mathbb{R},j} \vartheta_\infty) \circ (\mathbb{C}_p \otimes_{\mathbb{Q}_p} \vartheta_p)^{-1} \right] = \left[ [C_{A,F}^{c,\bullet}]_{\mathbb{Z}_p[G]}, \alpha' \circ \alpha \right].$$

The product structure of  $\pi_0(V(\mathbb{Z}_p[G]) \times_{V(\mathbb{C}_p[G])} \mathcal{P}_0)$  then combines with the commutativity of (11) to imply that it is also equal to

$$\begin{aligned}
& \left[ [C_{A,F}^{c,\bullet}]_{\mathbb{Z}_p[G]}, \alpha \right] + [\mathbf{1}_{\mathbb{Z}_p[G]}, \alpha'] \\
&= \left[ [C_{A,F}^{\text{loc},\bullet}[-1]]_{\mathbb{Z}_p[G]}, (\lambda_{A,F}^{\text{exp},j})_{\text{Triv}} \right] + \left[ [C_{A,F}^{f,\bullet}]_{\mathbb{Z}_p[G]}, (\lambda_{A,F}^{\text{NT},j})_{\text{Triv}} \right] + [\mathbf{1}_{\mathbb{Z}_p[G]}, \alpha'] \\
&= - \left[ [C_{A,F}^{\text{loc},\bullet}]_{\mathbb{Z}_p[G]}, (\lambda_{A,F}^{\text{exp},j})_{\text{Triv}} \right] + \left[ [C_{A,F}^{f,\bullet}]_{\mathbb{Z}_p[G]}, (\lambda_{A,F}^{\text{NT},j})_{\text{Triv}} \right] \\
&\quad + \left[ \mathbf{1}_{\mathbb{Z}_p[G]}, \prod_{v \in S_{US_p}} L_v(A, F/k) \right].
\end{aligned}$$

This implies the claimed result since (9) implies that

$$\left[ [C_{A,F}^{\text{loc},\bullet}]_{\mathbb{Z}_p[G]}, (\lambda_{A,F}^{\text{exp},j})_{\text{Triv}} \right] = \chi_j^{\text{loc}}(A, F/k)$$

(as  $\delta_{G,p}(\text{Nrd}_{\mathbb{Q}_p[G]}(-\text{id} \mid \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1(C_{A,F}^{\text{loc},\bullet}))) = 0$  because  $\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1(C_{A,F}^{\text{loc},\bullet})$  is a free  $\mathbb{Q}_p[G]$ -module) and

$$\left[ [C_{A,F}^{f,\bullet}]_{\mathbb{Z}_p[G]}, (\lambda_{A,F}^{\text{NT},j})_{\text{Triv}} \right] = -\chi_j(A, F/k)$$

(because  $\prod_{i=1}^{i=2} \text{Nrd}_{\mathbb{Q}_p[G]}(-\text{id} \mid \mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^i(C_{A,F}^{f,\bullet}))^{(-1)^i} = 1$ ) whilst the explicit description of the isomorphism (8) implies that

$$\begin{aligned}
\left[ \mathbf{1}_{\mathbb{Z}_p[G]}, \prod_{v \in S_{US_p}} L_v(A, F/k) \right] &= \delta_{G,p} \left( \prod_{v \in S_{US_p}} L_v(A, F/k) \right) \\
&= \sum_{v \in S_{US_p}} \delta_{G,p}(L_v(A, F/k)).
\end{aligned}$$

□

**4.4. The local term.** In this section we explicitly compute the Euler characteristic  $\chi_j^{\text{loc}}(A, F/k)$  that occurs in Proposition 4.2 in terms of both archimedean periods and global Galois-Gauss sums.

In the sequel we sometimes suppress explicit reference to the fixed identification of fields  $j : \mathbb{C} \cong \mathbb{C}_p$ . In addition, for each natural number  $m$  we will write  $[m]$  for the set of integers  $i$  which satisfy  $1 \leq i \leq m$ .

**4.4.1. Periods and Galois Gauss sums.** We fix Néron models  $\mathcal{A}^t$  for  $A^t$  over  $\mathcal{O}_k$  and  $\mathcal{A}_v^t$  for  $A_{/k_v}^t$  over  $\mathcal{O}_{k_v}$  for each  $v$  in  $S_p^k$ , and then fix a  $k$ -basis  $\{\omega_b\}_{b \in [d]}$  of the space of invariant differentials  $H^0(A^t, \Omega_{A^t}^1)$  which gives  $\mathcal{O}_{k_v}$ -bases of  $H^0(\mathcal{A}_v^t, \Omega_{\mathcal{A}_v^t}^1)$  for each  $v$  in  $S_p^k$  and is also such that each  $\omega_b$  extends to an element of  $H^0(\mathcal{A}^t, \Omega_{\mathcal{A}^t}^1)$ .

For each place  $v$  in  $S_{\mathbb{R}}$  we fix  $\mathbb{Z}$ -bases  $\{\gamma_{v,a}^+\}_{a \in [d]}$  and  $\{\gamma_{v,a}^-\}_{a \in [d]}$  of  $H_1(\sigma_v(A^t)(\mathbb{C}), \mathbb{Z})^{c=1}$  and  $H_1(\sigma_v(A^t)(\mathbb{C}), \mathbb{Z})^{c=-1}$ , where  $c$  denotes complex conjugation, and then set

$$\Omega_v^+(A) := \left| \det \left( \int_{\gamma_{v,a}^+} \omega_b \right)_{a,b} \right|, \quad \Omega_v^-(A) := \left| \det \left( \int_{\gamma_{v,a}^-} \omega_b \right)_{a,b} \right|,$$

where in both matrices  $(a, b)$  runs over  $[d] \times [d]$ . For each  $v$  in  $S_{\mathbb{C}}$  we fix a  $\mathbb{Z}$ -basis  $\{\gamma_{v,a}\}_{a \in [2d]}$  of  $H_1(\sigma_v(A^t)(\mathbb{C}), \mathbb{Z})$  and set

$$\Omega_v(A) := \left| \det \left( \int_{\gamma_{v,a}} \omega_b, c \left( \int_{\gamma_{v,a}} \omega_b \right) \right)_{a,b} \right|$$

where  $(a, b)$  runs over  $[2d] \times [d]$ . (By explicitly computing integrals these periods can be related to those obtained by integrating measures as occurring in the classical formulation of the Birch and Swinnerton-Dyer conjecture – see, for example, Gross [30, p. 224]).

For any  $\psi \in \text{Ir}(G)$  and  $v \in S_{\mathbb{R}}$ , we set  $\psi_v^+(1) := \dim_{\mathbb{C}} V_{\psi}^{G_{k_v}}$  and  $\psi_v^-(1) := \psi(1) - \psi_v^+(1)$ . Then we define the periods

$$\Omega_v(A, \psi) := \begin{cases} \Omega_v^+(A)^{\psi_v^+(1)} \cdot \Omega_v^-(A)^{\psi_v^-(1)} & \text{if } v \in S_{\mathbb{R}} \text{ and} \\ \Omega_v(A)^{\psi(1)} & \text{if } v \in S_{\mathbb{C}}; \end{cases}$$

and  $\Omega(A, \psi) := \prod_{v \in S_{\infty}} \Omega_v(A, \psi)$  and finally set

$$\Omega(A, F/k) := \sum_{\psi \in \text{Ir}(G)} \Omega(A, \psi) e_{\psi} \in \zeta(\mathbb{C}_p[G])^{\times}.$$

For each  $v$  in  $S_{\mathbb{R}}$ , respectively. in  $S_{\mathbb{C}}$ , we also define  $w_v(\psi)$  to be equal to  $i^{\psi_v^-(1)}$ , respectively.  $i^{\psi(1)}$ , and then set  $w_{\infty}(\psi) := \prod_{v \in S_{\infty}} w_v(\psi)$  and

$$w_{\infty}(F/k) := \sum_{\psi \in \text{Ir}(G)} w_{\infty}(\psi) e_{\psi} \in \zeta(\mathbb{C}_p[G])^{\times}.$$

To describe the relevant Galois Gauss sums we first define for each non-archimedean place  $v$  of  $k$  the ‘non-ramified characteristic’  $u_v$  to be the image under the natural induction map  $\zeta(\mathbb{C}_p[\overline{G}_v])^{\times} \rightarrow \zeta(\mathbb{C}_p[G])^{\times}$  of the element  $(1 - e_{\overline{I}_v}) + (-\text{Fr}_w^{-1})e_{\overline{I}_v}$  of  $\zeta(\mathbb{Q}[\overline{G}_v])^{\times}$ .

For each character  $\psi$  in  $\text{Ir}(G)$  we then define a modified equivariant global Galois-Gauss sum by setting

$$\tau^*(F/k) := \left( \prod_{v \in S_f^k} u_v \right) \sum_{\psi \in \text{Ir}(G)} e_{\psi} \tau(\mathbb{Q}, \text{Ind}_k^{\mathbb{Q}} \psi) \in \zeta(\mathbb{Q}^c[G])^{\times},$$

where the individual Galois Gauss sums  $\tau(\mathbb{Q}, -)$  are as defined by Martinet in [37].

**4.4.2. Computation of the local Euler characteristic.** The explicit computation of the Euler characteristic  $\chi_j^{\text{loc}}(A, F/k)$  is made considerably more difficult by the presence of  $p$ -adic places which ramify in any of the relevant field extensions. For simplicity in the sequel, and to focus attention on the key ideas in the present article, we therefore impose the following additional hypothesis

(h)  $p$  is unramified in  $F/\mathbb{Q}$ .

A full treatment of the terms  $\chi_j^{\text{loc}}(A, F/k)$  in the general (ramified) case will then be given in a future article.

In the following result we use the elements  $L_v(A, F/k)$  of  $\zeta(\mathbb{Q}_p[G])^{\times}$  that are defined in Proposition 4.2. We will also write  $j_*$  for the isomorphism  $\zeta(\mathbb{C}[G])^{\times} \cong \zeta(\mathbb{C}_p[G])^{\times}$  that is induced by  $j$ . We finally recall that  $d$  denotes the dimension of  $A$ .

**Theorem 4.3.** *If  $A$  and  $F$  satisfy the hypotheses (a)–(h), then one has*

$$\chi_j^{\text{loc}}(A, F/k) = \delta_{G,p} \left( j_* \left( \frac{w_{\infty}(F/k)^d \cdot \Omega(A, F/k)}{\tau^*(F/k)^d} \right) \prod_{v \in S_b \cup S_p} L_v(A, F/k) \right).$$

*Proof.* We set  $H_{A,v}^{F/k} := H^0(k_v, Y_{v,F} \otimes_{\mathbb{Z}} H_1(\sigma_v(A^t)(\mathbb{C}), \mathbb{Z}))$  for each  $v$  in  $S_{\infty}$  and then also  $H_A^{F/k} := \bigoplus_{v \in S_{\infty}} H_{A,v}^{F/k}$  and  $\tilde{C}_{A,F}^{\text{loc}, \bullet} := H_{A,p}^{F/k}[0] \oplus A^t(F_p) \wedge_p[-1]$ . Then, as  $p$  is odd and  $R\Gamma_f(k_v, T_{p,F}(A))$  is acyclic

for all  $v$  in  $S_r$  (by Lemma 4.1(i)), the comparison isomorphisms (5) induce a natural isomorphism

$$\kappa : C_{A,F}^{\text{loc},\bullet} \cong \tilde{C}_{A,F}^{\text{loc},\bullet} \oplus \bigoplus_{v \in S_b} H_f^1(k_v, T_{p,F}(A))[-1]$$

in  $D^{\text{p}}(\mathbb{Z}_p[G])$  and hence an equality in  $K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$

$$(13) \quad \chi_j^{\text{loc}}(A, F/k) - \chi_{G,p}(\tilde{C}_{A,F}^{\text{loc},\bullet}, \tilde{\lambda}_{A,F}^{\text{exp}}) = \sum_{v \in S_b} \chi_{G,p}(H_f^1(k_v, T_{p,F}(A))[-1], 0) \\ = \delta_{G,p} \left( \prod_{v \in S_b} L_v(A, F/k) \right).$$

Here we set  $\tilde{\lambda}_{A,F}^{\text{exp}} := (\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^1(\kappa)) \circ \lambda_{A,F}^{\text{exp}} \circ (\mathbb{Q}_p \otimes_{\mathbb{Z}_p} H^0(\kappa))^{-1}$  and the second equality follows by combining for each  $v$  in  $S_b$  the explicit definition of the term  $L_v(A, F/k)$  together with the facts that there is an exact sequence of  $\mathbb{Z}_p[G]$ -modules

$$0 \longrightarrow T_{p,F}(A)^{I_v} \xrightarrow{1 - \text{Fr}_v^{-1}} T_{p,F}(A)^{I_v} \longrightarrow H_f^1(k_v, T_{p,F}(A)) \longrightarrow 0,$$

and that  $T_{p,F}(A)^{I_v}$  is a projective  $\mathbb{Z}_p[G]$ -module (as a consequence of hypothesis (e)).

We next note that  $\tilde{\lambda}_{A,F}^{\text{exp}} := \mu_2 \circ \mu_1$ , where  $\mu_1$  is the second isomorphism that occurs in the definition of  $\lambda_{A,F}^{\text{exp},j}$  and  $\mu_2 = \bigoplus_{v \in S_p} \mu_2^v$  where each  $\mu_2^v$  is induced by the classical exponential map (7).

For each  $v$  in  $S_p$  we set  $\mathcal{O}_{F_v} := \mathcal{O}_F \otimes_{\mathcal{O}_k} \mathcal{O}_{k_v}$ . Then hypothesis (h) implies that each such place  $v$  is unramified in  $F_w/k_v$  and hence, by Noether's Theorem, that the  $\mathbb{Z}_p[G]$ -module  $\mathcal{O}_{F_v} \cong \prod_{w'|v} \mathcal{O}_{F_{w'}}$  is free. In particular, the  $\mathbb{Z}_p[G]$ -module

$$J_{A,F_p} := \bigoplus_{v \in S_p} \mathcal{O}_{F_v} \otimes_{\mathcal{O}_{k_v}} \text{Hom}_{\mathcal{O}_{k_v}}(H^0(\mathcal{A}_v^t, \Omega_{\mathcal{A}_v^t}^1), \mathcal{O}_{k_v}),$$

is free and so in  $K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$  one has an equality

$$\chi_{G,p}(\tilde{C}_{A,F}^{\text{loc},\bullet}, \tilde{\lambda}_{A,F}^{\text{exp}}) \\ = \chi_{G,p}(H_{A,p}^{F/k}[0] \oplus J_{A,F_p}[-1], \mu_1) + \chi_{G,p}(J_{A,F_p}[0] \oplus A^t(F_p)_p^\wedge[-1], \mu_2).$$

Combining this equality with (13) and the explicit computations in Lemmas 4.4 and 4.5 below one finds that  $\chi_j^{\text{loc}}(A, F/k)$  is equal to

$$\delta_{G,p} \left( j_*(w_\infty(F/k)^d \Omega(A, F/k)) \prod_{v \in S_b \cup S_p} L_v(A, F/k) \right) - d \cdot (\mathcal{O}_{F,p}, \pi_F, Y_{F,p}).$$

Here we have set  $Y_F := \prod_{\Sigma(F)} \mathbb{Z}$ , endowed with its natural action of  $G$ , and written  $\pi_F : \mathbb{C}_p \otimes_{\mathbb{Q}_p} F_p \cong \mathbb{C}_p \otimes_{\mathbb{Z}_p} Y_{F,p}$  for the natural isomorphism. To deduce the claimed result from this expression it suffices to show  $(\mathcal{O}_{F,p}, \pi_F, Y_{F,p})$  is equal to  $\delta_{G,p}(j_*(\tau^*(F/k)))$  and, since no  $p$ -adic place of  $k$  ramifies in  $F/k$ , this follows directly from equation (34), Proposition 7.1 and Corollary 7.6 in [6].  $\square$

**Lemma 4.4.** *If at each place  $v$  in  $S_p$  the extension  $F_w/\mathbb{Q}_p$  is unramified and  $A$  has good reduction, then one has*

$$\chi_{G,p}(J_{A,F_p}[0] \oplus A^t(F_p)_p^\wedge[-1], \mu_2) = \delta_{G,p} \left( \prod_{v \in S_p} L_v(A, F/k) \right).$$

*Proof.* We fix  $v$  in  $S_p$  and write  $\mathcal{A}_{v,F}^t$  for the Néron model  $\mathcal{A}_v^t \times_{\mathcal{O}_{k_v}} \mathcal{O}_{F_v}$  of  $A^t$  over  $\mathcal{O}_{F_v} := \prod_{w'|v} \mathcal{O}_{F_w'}$ . Then  $\mathrm{Hom}_{\mathcal{O}_{F_v}}(H^0(\mathcal{A}_{v,F}^t, \Omega_{\mathcal{A}_{v,F}^t}^1), \mathcal{O}_{F_v})$  is naturally isomorphic to the free  $\mathbb{Z}_p[G]$ -module  $J_{A,F_v} := \mathcal{O}_{F_v} \otimes_{\mathcal{O}_{k_v}} \mathrm{Hom}_{\mathcal{O}_{k_v}}(H^0(\mathcal{A}_v^t, \Omega_{\mathcal{A}_v^t}^1), \mathcal{O}_{k_v})$ .

In addition, the stated hypotheses on  $v$  imply that there exists a full free  $\mathbb{Z}_p[G]$ -submodule

$$\mathcal{D}_v := D_{\mathrm{cr},v}(T_{p,F}(A)) \cong \mathcal{O}_{F_v} \otimes_{\mathcal{O}_{k_v}} D_{\mathrm{cr},v}(T_p(A))$$

of  $D_{\mathrm{cr},v}(V_{p,F}(A))$ , where  $D_{\mathrm{cr},v}$  is the quasi-inverse to the functor of Fontaine and Lafaille used by Niziol in [42], and the theory of Fontaine and Messing [28] implies that the canonical comparison isomorphism

$$\mathrm{Hom}_{F_v}(H^0(\mathcal{A}_{F_v}^t, \Omega_{\mathcal{A}_{F_v}^t}^1), F_v) \cong D_{\mathrm{dR},v}(V_{p,F}(A))/F^0$$

maps  $J_{A,F_v}$  to  $\mathcal{D}_v/F^0\mathcal{D}_v$  (see §5 in [8]).

In this case it is also shown in [8] that there is a natural short exact sequence of perfect complexes of  $\mathbb{Z}_p[G]$ -modules (with vertical differentials)

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{D}_v/F^0\mathcal{D}_v & \xrightarrow{(0,\mathrm{id})} & \mathcal{D}_v \oplus \mathcal{D}_v/F^0\mathcal{D}_v & \xrightarrow{(\mathrm{id},0)} & \mathcal{D}_v \longrightarrow 0 \\ & & \uparrow & & \uparrow & & \uparrow \\ 0 & \longrightarrow & 0 & \longrightarrow & \mathcal{D}_v & \xrightarrow{\mathrm{id}} & \mathcal{D}_v \longrightarrow 0. \end{array}$$

$(1-\varphi_v, \pi)$        $1-\varphi_v$

Here the term  $\mathcal{D}_v/F^0\mathcal{D}_v$  in the first complex occurs in degree 1 and  $\pi$  is the tautological projection. Further, the exponential map of Bloch and Kato maps the cohomology in degree 1 of the second complex bijectively to  $H_f^1(k_v, T_{p,F}(A)) = A^t(F_v)_p^\wedge$  and the differential  $1 - \varphi_v$  of the third complex is injective. For a proof of all these claims see Lemma 4.5 (together with Example 3.11) in loc. cit.. The long exact sequence of cohomology of the above exact sequence thus gives rise to a short exact sequence of  $\mathbb{Z}_p[G]$ -modules  $0 \rightarrow J_{A,F_v} \rightarrow A^t(F_v)_p^\wedge \rightarrow \mathrm{cok}(1 - \varphi_v) \rightarrow 0$ , in which (following [8, Example 3.11]) the second arrow is equal to  $\mu_2^v$ . This sequence then implies that the term  $\chi_{G,p}(J_{A,F_v}[0] \oplus A^t(F_v)_p^\wedge[-1], \mu_2^v)$  is equal to

$$\chi_{G,p}(\mathrm{cok}(1 - \varphi_v)[-1], 0) = \partial_{G,p}((1 - \varphi_v | D_{\mathrm{cr},v}(V_{p,F}(A)))) = \delta_{G,p}(L_v(A, F/k))$$

and by summing over all places  $v$  in  $S_p$  this implies the claimed equality.  $\square$

For each  $\sigma \in \Sigma(k)$  we fix an embedding  $\hat{\sigma} \in \Sigma_\sigma(F)$ .

**Lemma 4.5.** *In  $K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$  one has*

$$\begin{aligned} \chi_{G,p}\left(H_{A,p}^{F/k}[0] \oplus J_{A,F_p}[-1], \mu_1\right) \\ = -d \cdot (\mathcal{O}_{F,p}, \pi_F, Y_{F,p}) + \delta_{G,p}(j_*(w_\infty(F/k)^d \Omega(A, F/k))). \end{aligned}$$

*Proof.* For each place  $v$  in  $S_{\mathbb{R}}$  we define  $\tau_v$  in  $G$  via the equality  $\tau_v(\hat{\sigma}_v) = c \circ \hat{\sigma}_v$ . For each integer  $a$  in  $[d]$  we then define an element

$$x_{v,a} := \frac{1}{2}(1 + \tau_v)\hat{\sigma}_v \otimes_{\mathbb{Z}} \gamma_{v,a}^+ + \frac{1}{2}(1 - \tau_v)\hat{\sigma}_v \otimes_{\mathbb{Z}} \gamma_{v,a}^-$$

and we note that, since  $p$  is odd, the set  $\mathcal{X}_v := \{x_{v,a}\}_{a \in [d]}$  is a  $\mathbb{Z}_p[G]$ -basis of  $H_{A,v,p}^{F/k}$ .

For  $v$  in  $S_{\mathbb{C}}$  and  $a$  in  $[2d]$  we set  $x_{v,a} := \hat{\sigma}_v \otimes_{\mathbb{Z}} \gamma_{v,a}$  and note that  $\mathcal{X}_v := \{x_{v,a}\}_{a \in [2d]}$  is a  $\mathbb{Z}_p[G]$ -basis of  $H_{A,v,p}^{F/k}$ .

We next set  $n := [k : \mathbb{Q}] = |S_{\mathbb{R}}| + 2|S_{\mathbb{C}}|$  and fix an  $\mathcal{O}_{k,p}[G]$ -generator  $Z$  of  $\mathcal{O}_{F_p}$  and a  $\mathbb{Z}_p$ -basis  $\{z_m\}_{m \in [n]}$  of  $\mathcal{O}_{k,p}$  and set  $t_{m,b} := Zz_m \otimes_k \omega_b^*$  with  $\omega_b^*$  the element of  $\text{Hom}_k(H^0(A^t, \Omega_{A^t}^1), k)$  that is dual to  $\omega_b$ . Then the set  $\mathcal{T} := \{t_{m,b}\}_{(m,b) \in [n] \times [d]}$  is a  $\mathbb{Z}_p[G]$ -basis of  $J_{A,F_p}$ .

The key to our argument is to compute the matrix of  $\mu_1$  with respect to the bases  $\mathcal{T}$  and  $\mathcal{X} := \bigcup_{v \in S_{\infty}} \mathcal{X}_v$  of  $\mathbb{R} \otimes_{\mathbb{Q}} (F \otimes_k \text{Hom}_k(H^0(A^t, \Omega_{A^t}^1), k))$  and  $\mathbb{R} \otimes_{\mathbb{Z}} H_A^{F/k}$ . To do this we find it convenient to introduce an auxiliary basis. Thus, for  $v$  in  $S_{\mathbb{R}}$  we set  $\mathcal{Y}_v := \{y_{v,b}\}_{b \in [d]}$  with  $y_{v,b} := \hat{\sigma}_v \otimes_{\mathbb{Z}} \sigma_{v,*}(\omega_b^*)$ , and for  $v$  in  $S_{\mathbb{C}}$  we set  $\mathcal{Y}_v := \{y_{v,b}\}_{b \in [2d]}$  with  $y_{v,b} := \hat{\sigma}_v \otimes_{\mathbb{Z}} \sigma_{v,*}(\omega_b^*)$  if  $b \in [d]$  and  $y_{v,b} := \hat{\sigma}_v \otimes_{\mathbb{Z}} c(\sigma_{v,*}(\omega_b^*))$  if  $b \in [2d] \setminus [d]$ . Then  $\mathcal{Y} := \bigcup_{v \in S_{\infty}} \mathcal{Y}_v$  is an  $\mathbb{R}[G]$ -basis of  $\bigoplus_{v \in S_{\infty}} k_v Y_{v,F} \otimes_{k_v} (k_v \otimes_{k,\sigma_v} \text{Hom}_k(H^0(A^t, \Omega_{A^t}^1), k))$  and for each index  $a$  one has

$$\pi_v(x_{v,a}) = \begin{cases} \sum_{j=1}^d \frac{1}{2} (\Omega_{v,a,j}^+ (1 + \tau_v) + \Omega_{v,a,j}^- (1 - \tau_v)) y_{v,j}, & \text{if } v \in S_{\mathbb{R}}, \\ \sum_{j=1}^{2d} \Omega_{v,a,j} y_{v,j}, & \text{if } v \in S_{\mathbb{C}} \end{cases}$$

with  $\Omega_{v,a,j}^{\pm} := \int_{\gamma_{v,a}^{\pm}} \omega_j$  and  $\Omega_{v,a,j} := \int_{\gamma_{v,a}} \omega_j$  if  $a \in [d]$  and  $\Omega_{v,a,j} := c(\int_{\gamma_{v,a}} \omega_j)$  if  $a \in [2d] \setminus [d]$ . This formula implies that the matrix of  $\mu_1$  with respect to the bases  $\mathcal{X}$  and  $\mathcal{T}$  is  $M^{-1}\Phi$  where  $\Phi = \text{diag}((\Phi_v)_{v \in S_{\infty}})$  is a diagonal block matrix with blocks

$$\Phi_v := \begin{cases} (\Omega_{v,a,j}^+ (1 + \tau_v)/2 + \Omega_{v,a,j}^- (1 - \tau_v)/2)_{(a,j) \in [d] \times [d]} & \text{if } v \in S_{\mathbb{R}}, \\ (\Omega_{v,a,j})_{(a,j) \in [2d] \times [2d]} & \text{if } v \in S_{\mathbb{C}} \end{cases}$$

and  $M$  is the matrix in  $\text{GL}_{nd}(\mathbb{C}[G])$  that represents the isomorphism (6) with respect to the bases  $\mathcal{T}$  and  $\mathcal{Y}$  so that

$$M_{(a,j),(v,\alpha)} = \begin{cases} \sigma_v(z_a) \sum_{g \in G} \hat{\sigma}_v(g(Z)) g^{-1} & \text{if } v \in S_{\mathbb{R}} \text{ and } \alpha = j, \\ \sigma_v(z_a) \sum_{g \in G} \hat{\sigma}_v(g(Z)) g^{-1} & \text{if } v \in S_{\mathbb{C}} \text{ and } \alpha = j, \\ c \circ \sigma_v(z_a) \sum_{g \in G} c \circ \hat{\sigma}_v(g(Z)) g^{-1} & \text{if } v \in S_{\mathbb{C}} \text{ and } \alpha = j + d, \\ 0 & \text{otherwise.} \end{cases}$$

Writing  $[M^{-1}\Phi]$  for the class of  $M^{-1}\Phi$  in  $K_1(\mathbb{C}_p[G])$  one therefore has

$$(14) \quad \chi_{G,p} \left( H_{A,p}^{F/k}[0] \oplus J_{A,F_p}[-1], \mu_1 \right) = \partial_{G,p}([M^{-1}\Phi]) \\ = \delta_{G,p}(\text{Nrd}_{\mathbb{C}_p[G]}(M^{-1}\Phi)) = -\delta_{G,p}(\text{Nrd}_{\mathbb{C}_p[G]}(M)) + \delta_{G,p}(\text{Nrd}_{\mathbb{C}_p[G]}(\Phi)).$$

Now  $M$  is equal to the product  $M_1 M_2$  for the block matrices  $M_1 = (\sigma(z_a) I_d)_{\sigma \in \Sigma(k), a \in [n]}$  and  $M_2 = \text{diag}((\sum_{g \in G} \hat{\sigma}(g(Z)) g^{-1}) I_d)_{\sigma \in \Sigma(k)}$  and so  $\text{Nrd}_{\mathbb{C}[G]}(M)$  is equal to the product

$$\text{Nrd}_{\mathbb{C}[G]}(M_1) \text{Nrd}_{\mathbb{C}[G]}(M_2) = \text{Nrd}_{\mathbb{C}[G]}((\sigma(z_a))_{\sigma,a})^d \text{Nrd}_{\mathbb{C}[G]} \left( \text{diag} \left( \sum_{g \in G} \hat{\sigma}(g(Z)) g^{-1} \right)_{\sigma} \right)^d \\ = \text{Nrd}_{\mathbb{C}[G]} \left( \left( \sigma(z_a) \sum_{g \in G} \hat{\sigma}(g(Z)) g^{-1} \right)_{a,\sigma} \right)^d.$$

In addition,  $(\sigma(z_a) \sum_{g \in G} \hat{\sigma}(g(Z)) g^{-1})_{a,\sigma}$  is the matrix of the natural isomorphism  $\pi_F : \mathbb{C}_p \otimes_{\mathbb{Q}_p} F_p \cong \mathbb{C}_p \otimes_{\mathbb{Z}_p} Y_{F,p}$  with respect to the  $\mathbb{Z}_p[G]$ -bases  $\{Zz_a\}_{a \in [n]}$  and  $\{\hat{\sigma}\}_{\sigma \in \Sigma(k)}$  of  $\mathcal{O}_{F,p}$  and  $Y_{F,p}$  and so

$$(15) \quad \delta_{G,p}(\text{Nrd}_{\mathbb{C}_p[G]}(M)) = d \cdot \partial_{G,p} \left( \left[ \left( \sigma(z_a) \sum_{g \in G} \hat{\sigma}(g(Z)) g^{-1} \right)_{a,\sigma} \right] \right) = d \cdot (\mathcal{O}_{F,p}, \pi_F, Y_{F,p}).$$

Next we note that  $\text{Nrd}_{\mathbb{C}_p[G]}(\Phi) = \prod_{v \in S_\infty} \text{Nrd}_{\mathbb{C}_p[G]}(\Phi_v)$  and that for each  $v$  in  $S_\infty$  also  $\text{Nrd}_{\mathbb{C}_p[G]}(\Phi_v) = \sum_{\psi \in \text{Ir}(G)} e_\psi \det_{\mathbb{C}_p}(\Phi_v \mid V_\psi^{d[k_v:\mathbb{R}]})$  with

$$\det_{\mathbb{C}_p}(\Phi_v \mid V_\psi^{d[k_v:\mathbb{R}]}) = \begin{cases} \det((\Omega_{v,a,j}^+)_{a,j})^{\psi_v^+(1)} \cdot \det((\Omega_{v,a,j}^-)_{a,j})^{\psi_v^-(1)} & \text{if } v \in S_\mathbb{R}, \\ \det((\Omega_{v,a,j})_{a,j})^{\psi(1)} & \text{if } v \in S_\mathbb{C}. \end{cases}$$

Now if  $v$  is real, then  $\det((\Omega_{v,a,j}^+)_{a,j}) = \varpi_v^+ \cdot \Omega_v^+(A)$  and  $\det((\Omega_{v,a,j}^-)_{a,j}) = \varpi_v^- \cdot i^d \cdot \Omega_v^-(A)$  with  $\varpi_v^+$  and  $\varpi_v^-$  in  $\{\pm 1\}$ , whilst if  $v$  is complex, then  $\det((\Omega_{v,a,j})_{a,j}) = \varpi_v \cdot i^d \cdot \Omega_v(A)$  with  $\varpi_v$  in  $\{\pm 1\}$ . Thus, since each of the terms

$$\sum_{\psi \in \text{Ir}_p(G)} e_\psi (\varpi_v^+)^{\psi_v^+(1)} (\varpi_v^-)^{\psi_v^-(1)} = \text{Nrd}_{\mathbb{Q}_p[G]}(\varpi_v^+(1 + \tau_v)/2 + \varpi_v^-(1 - \tau_v)/2)$$

if  $v$  is real, and  $\sum_{\psi \in \text{Ir}_p(G)} e_\psi \varpi_v^{\psi(1)} = \text{Nrd}_{\mathbb{Q}_p[G]}(\varpi_v)$  if  $v$  is complex, belong to the kernel of  $\delta_{G,p}$ , we conclude that  $\delta_{G,p}(\text{Nrd}_{\mathbb{C}_p[G]}(\Phi))$  is equal to

$$\begin{aligned} & \delta_{G,p} \left( \sum_{\psi \in \text{Ir}(G)} e_\psi \prod_{v \in S_\mathbb{R}} \left( \Omega_v^+(A)^{\psi_v^+(1)} (i^d \cdot \Omega_v^-(A))^{\psi_v^-(1)} \right) \prod_{v \in S_\mathbb{C}} (i^d \cdot \Omega_v(A))^{\psi(1)} \right) \\ &= \delta_{G,p} \left( \left( \sum_{\psi \in \text{Ir}(G)} w_\infty(\psi)^d e_\psi \right) \left( \sum_{\psi \in \text{Ir}(G)} \Omega(A, \psi) e_\psi \right) \right) \\ &= \delta_{G,p} \left( w_\infty(F/k)^d \cdot \Omega(A, F/k) \right). \end{aligned}$$

This formula combines with (14) and (15) to give the claimed formula for the term  $\chi_{G,p}(H_{A,p}^{F/k}[0] \oplus J_{A,F_p}[-1], \mu_1)$ .  $\square$

This completes the proof of Theorem 4.3.

## 5. CONGRUENCES BETWEEN DERIVATIVES

We assume in the sequel that, in addition to the hypotheses (a)–(h), the following standard conjecture is also valid.

- (i) For each finite set of places  $\Sigma$  of  $k$  and each character  $\psi$  in  $\text{Ir}(G)$  the  $\Sigma$ -truncated  $\psi$ -twisted Hasse-Weil  $L$ -function  $L_\Sigma(A, \psi, s)$  of  $A$  has an analytic continuation to  $s = 1$  where it has a zero of order  $r_\psi := \dim_{\mathbb{C}}(V_\psi \otimes_{\mathbb{Z}} A(F))^G$ .

Here  $G$  acts diagonally on the tensor product and so  $r_\psi$  is equal to the multiplicity with which  $\psi$ , and hence also  $\bar{\psi}$ , appears in the representation  $\mathbb{C} \otimes_{\mathbb{Z}} A(F)$ .

For each  $\psi$  in  $\text{Ir}(G)$  we then write  $L_\Sigma^*(A, \psi, 1)$  for the coefficient of  $(s - 1)^{r_\psi}$  in the Taylor expansion at  $s = 1$  of  $L_\Sigma(A, \psi, s)$ .

In this section we use the computations of §4 to give a reinterpretation, under the hypotheses (a)–(i), of the appropriate case of the equivariant Tamagawa number conjecture of [16, Conjecture 4] as a family of congruence relations between the leading terms  $L_{S_p}^*(A, \psi, 1)$  as  $\psi$  varies over  $\text{Ir}(G)$ . We next discuss several consequences of this reinterpretation and then, motivated by the results of [18], we specialise to the case that the ( $p$ -completed) Mordell-Weil group  $A(F)_p$  is a projective  $\mathbb{Z}_p[G]$ -module. In this case we prove results that will subsequently enable us in §6 to give some important new theoretical and numerical verifications of [16, Conjecture 4].

**5.1. The general case.** If  $A$  and  $F$  satisfy the hypotheses (g) and (i), then [16, Conjecture 4] for the pair  $(h^1(A/F)(1), \mathbb{Z}[G])$  asserts the validity of an equality in  $K_0(\mathbb{Z}[G], \mathbb{R}[G])$ . In such a case we shall say that the ‘eTNC $_p$  for  $(h^1(A/F)(1), \mathbb{Z}[G])$  is valid’ if for every isomorphism of fields  $j : \mathbb{C} \cong \mathbb{C}_p$  the predicted equality is valid after projection under the homomorphism  $j_{G,*}$  defined in (4).

If  $p$  does not divide  $|G|$ , then the algebra  $\mathbb{Z}_p[G]$  is regular and it is straightforward to use the techniques described in [15, §1.7] to give an explicit interpretation of these projections. If  $p$  divides  $|G|$ , however, then obtaining an explicit interpretation is in general very difficult (see, for example, the efforts made by Bley in [3, 4]).

The following result is thus of some interest since, as we shall see later, it can be combined with the structure results obtained in [18] to show that under certain natural conditions one can explicitly interpret, and verify, the eTNC $_p$  for  $(h^1(A/F)(1), \mathbb{Z}[G])$  even if  $G$  is non-abelian,  $p$  divides  $|G|$  and the rank of  $A(F)$  is strictly positive.

For each non-archimedean place  $v$  of  $k$ , we decompose the non-ramified characteristic  $u_v$  as  $\sum_{\psi \in \text{Ir}(G)} u_{v,\psi} \cdot e_\psi$  with each  $u_{v,\psi}$  in  $\mathbb{C}^\times$ . For each  $\psi$  in  $\text{Ir}(G)$  we then define a modified global Galois-Gauss sum by setting

$$(16) \quad \tau^*(\mathbb{Q}, \text{Ind}_k^{\mathbb{Q}} \psi) := u_\psi \cdot \tau(\mathbb{Q}, \text{Ind}_k^{\mathbb{Q}} \psi).$$

with  $u_\psi := \prod_{v \in S_r^k} u_{v,\psi}$ .

**Theorem 5.1.** *Assume that  $A$  and  $F$  satisfy the hypotheses (a)–(i). Then the element*

$$\mathcal{L}_{A,F/k}^* := \sum_{\psi \in \text{Ir}(G)} e_\psi \frac{L_{S_r}^*(A, \check{\psi}, 1) \cdot \tau^*(\mathbb{Q}, \text{Ind}_k^{\mathbb{Q}} \psi)^d}{\Omega(A, \psi) \cdot w_\infty(\psi)^d}$$

*belongs to  $\zeta(\mathbb{C}[G])^\times$  and the eTNC $_p$  for  $(h^1(A/F)(1), \mathbb{Z}[G])$  is valid if and only if for every isomorphism of fields  $j : \mathbb{C} \cong \mathbb{C}_p$  one has*

$$(17) \quad \delta_{G,p}(j_*(\mathcal{L}_{A,F/k}^*)) = \chi_j(A, F/k)$$

*Proof.* Since  $L_{S_r}^*(A, \check{\psi}, 1) \neq 0$  for all  $\psi$  in  $\text{Ir}(G)$  the element  $\mathcal{L}_{A,F/k}^*$  clearly belongs to  $\zeta(\mathbb{C}[G])^\times$ .

We next recall that [16, Conjecture 4(iv)] for the pair  $(h^1(A/F)(1), \mathbb{Z}[G])$  asserts

$$R\Omega(h^1(A/F)(1), \mathbb{Z}[G]) = -\delta_G(L^*(\mathbb{Q}[G]h^1(A/F)(1), 0))$$

where  $\delta_G$  is the ‘extended boundary homomorphism’  $\zeta(\mathbb{R}[G])^\times \rightarrow K_0(\mathbb{Z}[G], \mathbb{R}[G])$  defined in [16, Lemma 9] and  $L^*(\mathbb{Q}[G]h^1(A/F)(1), 0)$  is the leading term at  $s = 0$  of the  $\zeta(\mathbb{C}[G])$ -valued  $L$ -function  $L(\mathbb{Q}[G]h^1(A/F)(1), s)$  defined in [16, §4.1].

Noting that for each isomorphism  $j : \mathbb{C} \cong \mathbb{C}_p$  one has  $j_{G,*} \circ \delta_G = \delta_{G,p} \circ j_*$ , and recalling the result of Proposition 4.2, it follows that the eTNC $_p$  for  $(h^1(A/F)(1), \mathbb{Z}[G])$  is valid if and only if for every isomorphism  $j$  one has

$$\begin{aligned} & \delta_{G,p}\left(j_*(L^*(\mathbb{Q}[G]h^1(A/F)(1), 0))\right) \\ &= \chi_j(A, F/k) + \chi_j^{\text{loc}}(A, F/k) - \sum_{v \in S \cup S_p} \delta_{G,p}(L_v(A, F/k)). \end{aligned}$$

Now hypotheses (e) and (h) combine to imply that  $S_r = (S \cup S_p) \setminus (S_b \cup S_p)$  and for each place  $v$  in this set the term  $L_v(A, F/k)$  is equal to the value at  $s = 0$  of the Euler factor at  $v$  that occurs in

the definition of  $L(\mathbb{Q}[G]h^1(A/F)(1), s)$  (by [16, Remark 7]). In view of the formula for  $\chi_j^{\text{loc}}(A, F/k)$  that is given in Theorem 4.3, one therefore finds that the above equality is valid if and only if

$$\delta_{G,p} \left( j_* \left( \frac{L_{S_r}^*(\mathbb{Q}[G]h^1(A/F)(1), 0) \cdot \tau^*(F/k)^d}{\Omega(A, F/k) \cdot w_\infty(F/k)^d} \right) \right) = \chi_j(A, F/k).$$

It now suffices to show that the quotient on the left hand side of this equality is equal to  $\mathcal{L}_{A,F/k}^*$  and this follows from a straightforward comparison of all of the terms involved and then noting that the definition of the truncated  $L$ -function  $L_{S_r}(\mathbb{Q}[G]h^1(A/F)(1), s)$  implies  $L_{S_r}^*(\mathbb{Q}[G]h^1(A/F)(1), 0) = \sum_{\psi \in \text{Ir}(G)} e_\psi L_{S_r}^*(A, \check{\psi}, 1)$ .  $\square$

If it is valid, then the equality (17) can be combined with the theory of organising matrices developed in [17] to extract from the element  $\mathcal{L}_{A,F/k}^*$  a range of detailed information about the arithmetic of  $A$  over  $F$ . To give an explicit example of such an implication we assume, motivated by the results of Theorem 2.7 and Corollary 2.10 in [18], that there exists a surjective homomorphism of  $\mathbb{Z}_p[G]$ -modules of the form

$$\pi : \text{Sel}_p(A_F)^\vee \rightarrow \Pi = \Pi^{\text{Pr}} \oplus \Pi^{\text{nPr}}$$

where  $\Pi$  is a trivial source  $\mathbb{Z}_p[G]$ -module,  $\Pi^{\text{Pr}}$  is a projective  $\mathbb{Z}_p[G]$ -module and  $\pi$  induces, upon passage to  $G$ -coinvariants, an isomorphism  $A(k)_p^* \cong \Pi_G$  (via the relevant canonical short exact sequence of the form (1)). The notion of ‘trivial source  $\mathbb{Z}_p[G]$ -module’ that we use here corresponds to the one defined in [18, §2.3.2]. For the purpose of applying the result [17, Corollary 2.13] to prove Proposition 5.2 below we however warn the reader that this terminology differs from the one introduced in §2.2 in loc. cit., where trivial source modules are instead called ‘permutation modules’. In this case we also write  $\Upsilon_{\text{pr}}$  for the subset of  $\text{Ir}(G)$  comprising characters for which the homomorphism  $e_\psi(\mathbb{C} \otimes_{\mathbb{Z}} \pi)$  is bijective and then define an idempotent in  $\zeta(\mathbb{Q}[G])$  by setting  $e_{\text{pr}} := \sum_{\psi \in \Upsilon_{\text{pr}}} e_\psi$ .

Given a natural number  $m$  and a matrix  $M$  in  $M_m(\mathbb{Z}_p[G])$  we write  $M'$  for the corresponding ‘generalised adjoint matrix’ in  $M_m(\mathbb{Q}_p[G])$  that is defined by Johnston and Nickel in [34, §3.6]. We then write  $\mathcal{A}_p(G)$  for the  $\zeta(\mathbb{Z}_p[G])$ -submodule of  $\zeta(\mathbb{Q}_p[G])$  given by the set

$$\left\{ x \in \zeta(\mathbb{Q}_p[G]) : \text{if } m > 0 \text{ and } M \in M_m(\mathbb{Z}_p[G]) \text{ then } xM' \in M_m(\mathbb{Z}_p[G]) \right\}.$$

For more details about this module see Remark 5.4 below.

**Proposition 5.2.** *Assume that  $A$  and  $F$  satisfy the hypotheses (a)–(i) and that the equality (17) is valid. Fix a surjective homomorphism of  $\mathbb{Z}_p[G]$ -modules*

$$\pi : \text{Sel}_p(A_F)^\vee \rightarrow \Pi$$

*as above and an element  $a$  of  $\mathcal{A}_p(G)$ . For each homomorphism  $\theta : A^t(F)_p \rightarrow A(F)_p^*$  of  $\mathbb{Z}_p[G]$ -modules and each isomorphism of fields  $j : \mathbb{C} \cong \mathbb{C}_p$  set*

$$R_j(\theta) := \text{Nrd}_{\mathbb{C}_p[G]}((\mathbb{C}_p \otimes_{\mathbb{Z}_p} \theta) \circ (\lambda_{A,F}^{\text{NT},j})^{-1}).$$

*Then for each such  $\theta$  and  $j$  the element  $a R_j(\theta) j_*(\mathcal{L}_{A,F/k}^* e_{\text{pr}})$  belongs to  $\mathbb{Z}_p[G]$  and annihilates both modules  $\text{III}_p(A_F^t)$  and  $\Pi^{\text{nPr}}$ . In particular, the element*

$$\mathcal{L}_{A,F/k} := \sum_{\psi \in \text{Ir}(G)} e_\psi \frac{L_{S_r}(A, \check{\psi}, 1) \cdot \tau^*(\mathbb{Q}, \text{Ind}_k^{\mathbb{Q}} \psi)^d}{\Omega(A, \psi) \cdot w_\infty(\psi)^d}$$

*is such that  $a \cdot j_*(\mathcal{L}_{A,F/k})$  belongs to  $\mathbb{Z}_p[G]$  and annihilates  $\text{III}_p(A_F^t)$ .*

*Proof.* Hypothesis (a) implies that the module  $A^t(F)_p$  is  $\mathbb{Z}_p$ -free. Lemma 4.1 therefore implies, in the terminology of [17], that  $R\Gamma_f(k, T_{p,F}(A))$  is an admissible complex of  $\mathbb{Z}_p[G]$ -modules and equation (17) asserts that  $j_*(\mathcal{L}_{A,F/k}^*)$  is a characteristic element for the pair  $(R\Gamma_f(k, T_{p,F}(A)), (\lambda_{A,F}^{\text{NT},j})^{-1})$ . The first claim is therefore a direct consequence of [17, Corollary 2.13] and the isomorphisms

$$\text{III}_p(A_F^t) \cong \text{III}_p(A_F)^\vee \cong (\text{Sel}_p(A_F)^\vee)_{\text{tor}} \cong H^2(R\Gamma_f(k, T_{p,F}(A)))_{\text{tor}},$$

where the first isomorphism is induced by the Cassels-Tate pairing, the second follows from the short exact sequence (1) (with  $L = F$ ) and the last is a consequence of Lemma 4.1.

To deduce the second claim we note that, under our hypotheses (a)–(i), the natural projection map

$$\text{Sel}_p(A_F)^\vee \rightarrow (\text{Sel}_p(A_F)^\vee)_G \cong \text{Sel}_p(A_k)^\vee \rightarrow A(k)_p^* =: \Pi$$

is a homomorphism  $\pi$  of the required type. Further, in this case one has  $\Pi^{\text{Pr}} = 0$  and so hypothesis (i) implies  $\Upsilon_{\text{pr}}$  is equal to  $\{\psi \in \text{Ir}(G) : L_{S_r}(A, \check{\psi}, 1) \neq 0\}$  and hence that  $\mathcal{L}_{A,F/k} = \mathcal{L}_{A,F/k} e_{\text{pr}} = \mathcal{L}_{A,F/k}^* e_{\text{pr}}$ . It therefore suffices to show that  $R_j(\theta) e_{\text{pr}} = e_{\text{pr}}$  and this is true because in this case the space  $e_{\text{pr}} \text{Hom}_{\mathbb{C}}(\mathbb{C} \cdot A(F), \mathbb{C})$  vanishes.  $\square$

*Remark 5.3.* The conjectural equality (17) implies, via Proposition 5.2, a family of explicit congruence relations between the complex numbers  $A(\psi)$  that are defined by the equalities  $A(\psi) e_\psi = a R_j(\theta) j_*(\mathcal{L}_{A,F/k}^*) e_\psi$  as  $\psi$  varies over  $\Upsilon_{\text{pr}}$ . This is because

$$a R_j(\theta) j_*(\mathcal{L}_{A,F/k}^*) e_{\text{pr}} = \sum_{\psi \in \Upsilon_{\text{pr}}} A(\psi) e_\psi = |G|^{-1} \sum_{g \in G} g \sum_{\psi \in \Upsilon_{\text{pr}}} \psi(1) \check{\psi}(g) A(\psi)$$

and this sum belongs to  $\zeta(\mathbb{Z}_p[G])$  if and only if the elements  $A(\psi)$  satisfy all of the following conditions:

- (i)  $A(\psi) \in \mathbb{Z}_p[\psi]$  for all  $\psi \in \Upsilon_{\text{pr}}$ ;
- (ii)  $\alpha(A(\psi)) = A(\alpha \circ \psi)$  for all  $\psi \in \Upsilon_{\text{pr}}$  and  $\alpha \in G_{\mathbb{Q}_p(\psi)/\mathbb{Q}_p}$ ;
- (iii)  $\sum_{\psi \in \Upsilon_{\text{pr}}} \psi(1) \check{\psi}(g) A(\psi) \equiv 0 \pmod{|G|\mathbb{Z}_p}$  for all  $g \in G$ .

*Remark 5.4.* Ideals of the form  $\mathcal{A}_p(G)$  were introduced by Nickel in [41] and have been computed extensively by Johnston and Nickel in [34]. For example, if  $M = I_m$ , then  $M' = I_m$  so that  $\mathcal{A}_p(G) \subseteq \zeta(\mathbb{Z}_p[G])$  and it is shown in loc. cit. that this inclusion is an equality if and only if the order of the commutator subgroup of  $G$  is not divisible by  $p$ . More generally, for each  $M$  in  $\text{M}_d(\mathbb{Z}_p[G])$  the matrix  $M'$  belongs to  $\text{M}_m(\mathcal{M})$  for any maximal order  $\mathcal{M}$  in  $\mathbb{Q}_p[G]$  that contains  $\mathbb{Z}_p[G]$  (cf. [41, Lemma. 4.1]) and so Jacobinski's description in [33] of the central conductor of  $\mathcal{M}$  in  $\mathbb{Z}_p[G]$  implies, for example, that for any  $\mathbb{Q}_p^c$ -valued character  $\psi$  of  $G$  the element  $\psi(1)^{-1}|G|e_\psi$  belongs to  $\mathbb{Z}_p[\psi] \otimes_{\mathbb{Z}_p} \mathcal{A}_p(G)$  where  $\mathbb{Z}_p[\psi]$  is the subring of  $\mathbb{Q}_p^c$  that is generated over  $\mathbb{Z}_p$  by the values of  $\psi$ . This gives an easy 'lower bound' on  $\mathcal{A}_p(G)$  (but which is, in most cases, not best possible).

*Remark 5.5.* For the explicit computation of terms of the form  $\chi_j(A, F/k)$  and  $R_j(\theta)$  occurring in Theorem 5.1 and Proposition 5.2 respectively in the case that  $G$  is cyclic of  $p$ -power order we refer the reader to [7] where, in addition, Theorem 5.1 is used in order to discuss further explicit (conjectural) properties of elements of the form  $a R_j(\theta) j_*(\mathcal{L}_{A,F/k}^*) e_{\text{pr}}$  in such settings.

**5.2. The case of projective Mordell-Weil groups.** In the rest of this article we consider the conjectural equality (17) in the case that  $A(F)_p$  and  $A^t(F)_p$  are both projective  $\mathbb{Z}_p[G]$ -modules. (In this regard, note that if  $A$  is principally polarised, then the  $\mathbb{Z}_p[G]$ -modules  $A(F)_p$  and  $A^t(F)_p$  are isomorphic.) This corresponds to taking the module  $\Pi$  in Proposition 5.2 to be equal to  $\Pi^{\text{Pr}} = A(F)_p^*$  and the more general case that  $\Pi = A(F)_p^*$  is a trivial source  $\mathbb{Z}_p[G]$ -module will be considered in a future article.

In the following result we use the notion of non-commutative Fitting invariant that was introduced by Parker [44] and studied further by Nickel [41].

**Proposition 5.6.** *Assume that  $A$  and  $F$  satisfy (a)–(i). Assume also that  $A(F)_p$  and  $A^t(F)_p$  are both projective  $\mathbb{Z}_p[G]$ -modules.*

*Then the projective dimension of the  $\mathbb{Z}_p[G]$ -module  $\mathbb{III}_p(A_F^t)$  is at most one and there exists an isomorphism  $\iota_p : A(F)_p^* \cong A^t(F)_p$  of  $\mathbb{Z}_p[G]$ -modules.*

*For each  $\psi \in \text{Ir}(G)$  now set*

$$R_{\psi, \iota_p}^{\text{NT}, j}(A/F) := \det_{\mathbb{C}_p} \left( (\mathbb{C}_p \otimes_{\mathbb{Z}_p} \iota_p) \circ \lambda_{A, F}^{\text{NT}, j} \mid (V_{j \circ \psi} \otimes_{\mathbb{Z}} A^t(F))^G \right) \in \mathbb{C}_p^\times.$$

*Then the equality (17) is valid if and only if the (non-commutative) Fitting invariant of the  $\mathbb{Z}_p[G]$ -module  $\mathbb{III}_p(A_F^t)$  is generated by the set of elements of the form  $u \cdot \mathcal{L}_{A, F/k, j, \iota_p}^*$  where  $u$  is in  $\text{Nrd}_{\mathbb{Q}_p[G]}(K_1(\mathbb{Z}_p[G]))$  and*

$$\mathcal{L}_{A, F/k, j, \iota_p}^* := \sum_{\psi \in \text{Ir}(G)} j_* \left( e_\psi \cdot \frac{L_{S_r}^*(A, \check{\psi}, 1) \cdot \tau^*(\mathbb{Q}, \text{Ind}_k^{\mathbb{Q}} \psi)^d}{\Omega(A, \psi) \cdot w_\infty(\psi)^d} \right) \frac{1}{R_{\psi, \iota_p}^{\text{NT}, j}(A/F)}.$$

*Proof.* The assumed projectivity of  $A(F)_p$  implies that its  $\mathbb{Z}_p$ -linear dual  $A(F)_p^*$  is also a projective  $\mathbb{Z}_p[G]$ -module. The existence of an isomorphism  $\iota_p$  therefore follows from Swan's Theorem [22, Theorem 32.1] and the fact that  $\lambda_{A, F}^{\text{NT}, j}$  induces an isomorphism of  $\mathbb{C}_p[G]$ -modules  $\mathbb{C}_p \cdot A^t(F)_p \cong \text{Hom}_{\mathbb{C}_p}(\mathbb{C}_p \otimes_{\mathbb{Z}} A(F), \mathbb{C}_p) = \mathbb{C}_p \cdot A(F)_p^*$ .

We now write  $C^\bullet$  for the complex  $A^t(F)_p \xrightarrow{0} A(F)_p^*$ , where the first term occurs in degree one. Then, since  $A(F)_p^*$  is a projective  $\mathbb{Z}_p[G]$ -module, we may choose a  $\mathbb{Z}_p[G]$ -equivariant section to the natural surjection

$$H^2(R\Gamma_f(k, T_{p, F}(A))) \cong \text{Sel}_p(A_F)^\vee \rightarrow A(F)_p^* = H^2(C^\bullet).$$

Since the kernel of this surjection is isomorphic (via the Cassels-Tate pairing) to  $\mathbb{III}_p(A_F^t)$ , such a section induces a short exact sequence of  $\mathbb{Z}_p[G]$ -modules

$$0 \rightarrow H^2(C^\bullet) \rightarrow H^2(R\Gamma_f(k, T_{p, F}(A))) \rightarrow \mathbb{III}_p(A_F^t) \rightarrow 0$$

and hence also an exact triangle in  $D^{\text{P}}(\mathbb{Z}_p[G])$  of the form

$$C^\bullet \rightarrow R\Gamma_f(k, T_{p, F}(A)) \rightarrow \mathbb{III}_p(A_F^t)[-2] \rightarrow C^\bullet[1].$$

In particular, since  $\mathbb{III}_p(A_F^t)[-2]$  belongs to  $D^{\text{P}}(\mathbb{Z}_p[G])$ , the projective dimension of the finite  $\mathbb{Z}_p[G]$ -module  $\mathbb{III}_p(A_F^t)$  is finite, and hence at most one (by [12, Chapter VI, (8.12)]), as claimed.

Further, if we use the cohomology sequence of the above triangle to identify  $\mathbb{C}_p \cdot H^i(C^\bullet)$  and  $\mathbb{C}_p \cdot H^i(R\Gamma_f(k, T_{p, F}(A))[1])$  in all degrees  $i$ , then this triangle combines with the additivity criterion of [11, Corollary 6.6] to imply that the element  $\chi_j(A, F/k) = -\chi_{G, p}(R\Gamma_f(k, T_{p, F}(A)), \lambda_{A, F}^{\text{NT}, j})$  is equal to

$$\begin{aligned} & -\chi_{G, p}(C^\bullet, \lambda_{A, F}^{\text{NT}, j}) - \chi_{G, p}(\mathbb{III}_p(A_F^t)[-2], 0) \\ & = -\chi_{G, p}(C^\bullet, \lambda_{A, F}^{\text{NT}, j}) + \chi_{G, p}(C^\bullet, (\mathbb{C}_p \otimes_{\mathbb{Z}_p} \iota_p)^{-1}) - \chi_{G, p}(\mathbb{III}_p(A_F^t)[-2], 0) \\ & = \delta_{G, p}(\text{Nrd}_{\mathbb{C}_p[G]}((\mathbb{C}_p \otimes_{\mathbb{Z}_p} \iota_p) \circ \lambda_{A, F}^{\text{NT}, j})) - \chi_{G, p}(\mathbb{III}_p(A_F^t)[-2], 0). \end{aligned}$$

Here the first displayed equality is valid as  $\chi_{G,p}(C^\bullet, (\mathbb{C}_p \otimes_{\mathbb{Z}_p} \iota_p)^{-1}) = 0$  and the second because the difference  $-\chi_{G,p}(C^\bullet, \lambda_{A,F}^{\text{NT},j}) + \chi_{G,p}(C^\bullet, (\mathbb{C}_p \otimes_{\mathbb{Z}_p} \iota_p)^{-1})$  is represented by the triple  $(A^t(F)_p, (\mathbb{C}_p \otimes_{\mathbb{Z}_p} \iota_p) \circ \lambda_{A,F}^{\text{NT},j}, A^t(F)_p)$ .

The equality (17) is therefore valid if and only if one has

$$\begin{aligned} & \delta_{G,p} \left( j_* (\mathcal{L}_{A,F/k}^* \cdot \text{Nrd}_{\mathbb{C}_p[G]} ((\mathbb{C}_p \otimes_{\mathbb{Z}_p} \iota_p) \circ \lambda_{A,F}^{\text{NT},j})^{-1}) \right) \\ &= \delta_{G,p} (j_* (\mathcal{L}_{A,F/k}^*)) - \delta_{G,p} \left( \text{Nrd}_{\mathbb{C}_p[G]} ((\mathbb{C}_p \otimes_{\mathbb{Z}_p} \iota_p) \circ \lambda_{A,F}^{\text{NT},j}) \right) \\ &= \chi_j(A, F/k) - \delta_{G,p} \left( \text{Nrd}_{\mathbb{C}_p[G]} ((\mathbb{C}_p \otimes_{\mathbb{Z}_p} \iota_p) \circ \lambda_{A,F}^{\text{NT},j}) \right) \\ &= -\chi_{G,p}(\text{III}_p(A_F^t)[-2], 0). \end{aligned}$$

In addition, one has  $\text{Nrd}_{\mathbb{C}_p[G]} ((\mathbb{C}_p \otimes_{\mathbb{Z}_p} \iota_p) \circ \lambda_{A,F}^{\text{NT},j}) e_{j \circ \psi} = R_{\psi, \iota_p}^{\text{NT},j}(A/F) e_{j \circ \psi}$  for each  $\psi$  in  $\text{Ir}(G)$  and so

$$j_* (\mathcal{L}_{A,F/k}^* \cdot \text{Nrd}_{\mathbb{C}_p[G]} ((\mathbb{C}_p \otimes_{\mathbb{Z}_p} \iota_p) \circ \lambda_{A,F}^{\text{NT},j})^{-1}) = \mathcal{L}_{A,F/k,j,\iota_p}^*.$$

Given this, a straightforward exercise (comparing the explicit definitions of refined Euler characteristic and non-commutative Fitting invariants) shows that the above formula for  $\chi_{G,p}(\text{III}_p(A_F^t)[-2], 0)$  is valid if and only if  $\text{Fit}_{\mathbb{Z}_p[G]}(\text{III}_p(A_F^t))$  is generated by the set of elements  $u \cdot \mathcal{L}_{A,F/k,j,\iota_p}^*$  with  $u$  in  $\text{Nrd}_{\mathbb{Q}_p[G]}(K_1(\mathbb{Z}_p[G]))$ , as claimed.  $\square$

**5.3. Dihedral congruences for elliptic curves.** We now investigate the criterion of Proposition 5.6 in the case that  $A$  is an elliptic curve (so  $A = A^t$ ) and  $F/k$  is dihedral (in the sense of Mazur and Rubin [40]).

Thus, as before, we have an odd prime  $p$  and a Galois extension  $F/k$  of group  $G$  with  $p$ -Sylow subgroup  $P$  and we assume that  $P$  is an abelian (normal) subgroup of  $G$  of index two and that the conjugation action of any lift to  $G$  of the generator of  $G/P$  inverts elements of  $P$ . In particular, the degree of  $F/k$  is equal to  $2p^n$  for some  $n \geq 1$  and  $K/k$  is a quadratic extension. We fix an element  $\tau$  of order 2 in  $G$ . We set  $\mathbf{1} := \mathbf{1}_G$  and write  $\epsilon$  for the unique non-trivial linear character of  $G$ .

In the following result, we will be interested in the case when  $A$  has rank one over  $K$ . In this case we write  $\rho_A$  for the unique linear character which does *not* occur in the  $\mathbb{C}[G]$ -module  $\mathbb{C} \otimes_{\mathbb{Z}} A(K)$ . Hence  $\rho_A = \mathbf{1}$  if  $\text{rk}(A_k) = 0$  and  $\rho_A = \epsilon$  otherwise.

We also set  $\mathbb{Z}' := \mathbb{Z}[\frac{1}{2}]$ .

**Proposition 5.7.** *Assume that the elliptic curve  $A$ , odd prime  $p$  and dihedral extension  $F/k$  satisfy the hypotheses (a)–(e) and (g), that all places above  $p$  split in  $K/k$ , that  $\text{rk}(A_K) = 1$  and that  $\text{III}_p(A_K) = 0$ .*

*Then  $\text{III}_p(A_F) = 0$  and there is a point  $Q$  in  $A(F)$  with  $\tau(Q) = -(-1)^{\text{rk}(A_k)} Q$  which generates a  $\mathbb{Z}'[G]$ -module that is isomorphic to  $\mathbb{Z}'[G](1 - (-1)^{\text{rk}(A_k)} \tau)$  and has finite, prime-to- $p$ , index in  $\mathbb{Z}' \otimes_{\mathbb{Z}} A(F)$ .*

*In particular, one has  $r_{\rho_A} = 0$  and  $r_\psi = 1$  for all  $\psi \in \text{Ir}(G) \setminus \{\rho_A\}$ .*

*Proof.* Under the stated hypotheses, [18, Corollary 2.10(ii)] implies that  $\text{III}_p(A_F)$  vanishes, that  $\text{Sel}_p(A_F)^\vee$  is a projective  $\mathbb{Z}_p[G]$ -module and that the multiplicity with which each  $\rho$  in  $\text{Ir}(P)$  occurs in the representation  $\mathbb{C}_p \cdot \text{Sel}_p(A_F)^\vee$  is equal to one.

Roiter's Lemma (cf. [22, (31.6)]) therefore implies (via the exact sequence (1)) the existence of an exact sequence of  $\mathbb{Z}'[G]$ -modules

$$0 \longrightarrow \mathbb{Z}'[G](1 - (-1)^{\text{rk}(A_k)} \tau) \longrightarrow \mathbb{Z}' \otimes_{\mathbb{Z}} A(F)_{\text{tf}} \longrightarrow X \longrightarrow 0,$$

where the group  $X$  is both finite and of order prime to  $p$ .

Since the group  $A(F)_{\text{tor}}$  is also finite of order prime to  $p$  (by hypothesis (a)) it follows that any point  $Q$  of  $A(F)$  whose projection in  $A(F)_{\text{tf}}$  is equal to the image of  $1 - (-1)^{\text{rk}(A_k)}\tau$  multiplied by a large enough power of 2 has the properties described above.

The above description of  $\mathbb{Z}' \otimes_{\mathbb{Z}} A(F)$  also implies that the  $\mathbb{C}[G]$ -module  $\mathbb{C} \otimes_{\mathbb{Z}} A(F)$  is isomorphic to  $\mathbb{C}[G](1 - (-1)^{\text{rk}(A_k)}\tau)$  and the claimed formulas for  $r_\psi$  are then easily verified by explicit computation.  $\square$

For each subgroup  $H$  of  $G$  and character  $\rho$  in  $\text{Ir}(H)$  we set

$$T_\rho := \sum_{h \in H} \rho(h^{-1})h \in \zeta(\mathbb{C}[H]).$$

For any point  $R$  of  $A(F)$  and any  $\psi \in \text{Ir}(G)$  we then define a non-zero complex number

$$h_{F,\psi}(R) := \frac{\psi(1)}{2|G|} \cdot \left\langle T_\psi(R), T_{\check{\psi}}(R) \right\rangle_F$$

where  $\langle \cdot, \cdot \rangle_F$  is the  $\mathbb{C}$ -linear extension of the Néron-Tate height on  $A$ , defined relative to the field  $F$ .

In the next result we assume the hypotheses of Proposition 5.7 to be satisfied and fix a point  $Q$  as in that result. For each  $\psi \in \text{Ir}(G)$  we then obtain a non-zero complex number  $\mathcal{Q}_\psi = \mathcal{Q}_{Q,\psi}$  by setting

$$(18) \quad \mathcal{Q}_\psi = u_\psi \cdot \frac{\sqrt{d_\psi} \cdot L_{S_r}^*(A, \psi, 1)}{\Omega(A, \psi) \cdot H_\psi}$$

where the quantity  $u_\psi$  is as in (16). Further we define

$$d_1 = |d_k|, \quad d_\epsilon = |d_K/d_k|, \quad \text{and} \quad d_{\text{Ind}_P^G(\chi)} = |d_K| \cdot \text{Nf}(\chi)$$

for all  $\chi \in \text{Ir}(P) \setminus \{\mathbf{1}_P\}$  and

$$H_{\rho_A} = 1 \quad \text{and} \quad H_\psi = h_{F,\psi}(Q), \quad \text{for all } \psi \neq \rho_A.$$

Here  $d_E$  denotes the absolute discriminant of a number field  $E$  and for any finite dimensional complex character  $\psi$  of  $G_E$  we write  $\text{Nf}(\psi)$  for the absolute norm of its Artin conductor.

We also note that hypothesis (i) combines with Proposition 5.7 to imply that the leading term  $L_{S_r}^*(A, \psi, 1)$  is equal to the value  $L_{S_r}(A, \psi, 1)$  for  $\psi = \rho_A$  and to the first derivative  $L'_{S_r}(A, \psi, 1)$  for  $\psi$  in  $\text{Ir}(G) \setminus \{\rho_A\}$ .

**Theorem 5.8.** *Fix an odd prime  $p$ , a dihedral extension  $F/k$  of degree  $2p^n$  and an elliptic curve  $A$  over  $k$ . Assume that  $A$  and  $F$  satisfy the hypotheses (a)–(h), that all places above  $p$  split in  $K/k$ , that  $\text{rk}(A_K) = 1$  and that  $\text{III}_p(A_K) = 0$ . Fix a point  $Q$  in  $A(F)$  as given by Proposition 5.7.*

*Then the equality (17) is valid if and only if the following conditions are satisfied.*

- (i) *For each  $\psi$  in  $\text{Ir}(G)$  the number  $\mathcal{Q}_\psi$  defined above belongs to  $\mathbb{Q}(\psi)$ , is a unit at all primes above  $p$  and satisfies  $(\mathcal{Q}_\psi)^\alpha = \mathcal{Q}_{\psi^\alpha}$  for all  $\alpha$  in  $\text{Gal}(\mathbb{Q}(\psi)/\mathbb{Q})$ .*
- (ii) *For all  $\pi \in P$  one has a congruence*

$$(19) \quad \mathcal{Q}_{\mathbf{1}_G} \cdot \mathcal{Q}_\epsilon \equiv - \sum_{\chi \in \text{Ir}(P) \setminus \{\mathbf{1}_P\}} \check{\chi}(\pi) \mathcal{Q}_{\text{Ind}_P^G(\chi)} \pmod{p^n \mathbb{Z}_{(p)}}$$

where  $\mathbb{Z}_{(p)}$  denotes the localisation of  $\mathbb{Z}$  at  $p$ .

*Remark 5.9.* If  $Q'$  is any element of  $A(F)$  with  $T_\psi(Q') \neq 0$  for all  $\psi \in \text{Ir}(G) \setminus \{\rho_A\}$ , then for each  $\psi \in \text{Ir}(G)$  one can define a non-zero complex number  $\mathcal{Q}'_\psi = \mathcal{Q}_{Q',\psi}$  just as in (18). Our proof of Theorem 5.8 will actually show that if the conditions (i) and (ii) are valid with each  $\mathcal{Q}_\psi$  replaced by  $\mathcal{Q}'_\psi$ , then  $Q'$  is a  $\mathbb{Z}_p[G]$ -generator of  $A(F)_p$  and the equality (17) is valid.

*Remark 5.10.* If  $n = 1$ , so the extension  $F/k$  in Theorem 5.8 is dihedral of degree  $2p$ , then each term  $\tilde{\chi}(\pi)$  is congruent to 1 modulo the unique prime above  $p$  in  $\mathbb{Q}(\chi)$  and so the congruences (19) reduce to a single congruence

$$(20) \quad \mathcal{Q}_{1_G} \cdot \mathcal{Q}_\epsilon \equiv -2 \sum_{\substack{\psi \in \text{Ir}(G) \\ \dim(\psi)=2}} \mathcal{Q}_\psi \pmod{p\mathbb{Z}_{(p)}}.$$

*Proof of Theorem 5.8.* It suffices to prove that the criterion of Proposition 5.6 is valid if and only if both the condition (i) and the congruences in (19) are valid. Now, since  $\text{III}_p(A_F) = 0$  (by [18, Corollary 2.10(ii)]), the criterion of Proposition 5.6 is equivalent to asking that the element  $\mathcal{L}_{A,F/k,j,\iota_p}^*$  belongs to  $\ker(\delta_{G,p})$ . In view of Lemma 5.11 below it is thus enough to show that the condition (i) and the congruences in (19) are valid if and only if the element  $\mathcal{L}' := j_*(\sum_{\psi \in \text{Ir}(G)} \mathcal{Q}_\psi e_\psi)$  belongs to  $\ker(\delta_{G,p})$ .

To investigate the element  $\delta_{G,p}(\mathcal{L}')$  we fix a maximal  $\mathbb{Z}_p$ -order  $\mathfrak{M}_p$  in  $\mathbb{Q}_p[G]$  that contains  $\mathbb{Z}_p[G]$ . Then  $\delta_{G,p}(\mathcal{L}')$  belongs to the subgroup  $K_0(\mathbb{Z}_p[G], \mathbb{Q}_p[G])_{\text{tor}}$  of  $K_0(\mathbb{Z}_p[G], \mathbb{C}_p[G])$  if and only if  $\mathcal{L}' \in \text{Nrd}_{\mathbb{Q}_p[G]}(\mathfrak{M}_p^\times)$  and this condition is satisfied if and only if the conditions of Theorem 5.8(i) are valid (for more details of these equivalences see the proof of [16, Lemma 11]).

It thus suffices to show that an element  $\mathcal{E} = \sum_{\psi \in \text{Ir}(G)} \mathcal{E}_\psi e_\psi$  of  $\text{Nrd}_{\mathbb{Q}_p[G]}(\mathfrak{M}_p^\times) \subset \bigoplus_{\psi \in \text{Ir}(G)} \mathbb{Q}_p(\psi)$  belongs to  $\ker(\delta_{G,p})$  if and only if the congruences in (19) are valid with each term  $\mathcal{Q}_\psi$  replaced by  $\mathcal{E}_\psi$  and with  $\mathbb{Z}_{(p)}$  replaced by  $\mathbb{Z}_p$ . But, from the results of Lemma 5.12(i) and (ii) below, one has  $\delta_{G,p}(\mathcal{E}) = 0$  if and only if  $\text{res}(\mathcal{E}) \in \mathbb{Z}_p[P]^\times$ , and by Lemma 5.12(iii) this is true if and only if the congruences in (19) are valid after making the changes described above.

This therefore completes the proof of Theorem 5.8.  $\square$

**Lemma 5.11.** *There exists an isomorphism of  $\mathbb{Z}_p[G]$ -modules  $\iota_p : A(F)_p^* \rightarrow A(F)_p$  such that  $\mathcal{L}_{A,F/k,j,\iota_p}^*$  is equal to the element  $\mathcal{L}' := j_*(\sum_{\psi \in \text{Ir}(G)} \mathcal{Q}_\psi e_\psi)$  defined above.*

*Proof.* We claim first that for each  $\rho \in \text{Ir}(G)$  there is an equality

$$(21) \quad \frac{\tau^*(\mathbb{Q}, \text{Ind}_k^{\mathbb{Q}} \rho)}{w_\infty(\rho)} = \begin{cases} u_{1_G} \sqrt{|d_k|} = (-1)^{|S_r|} \sqrt{|d_k|}, & \text{if } \rho = 1_G \\ u_\epsilon \sqrt{|d_K/d_k|} = (-1)^{|S_r|} \sqrt{|d_K/d_k|}, & \text{if } \rho = \epsilon \\ u_\rho \sqrt{|d_K| Nf(\chi)}, & \text{if } \rho = \text{Ind}_P^G \chi \end{cases}$$

where  $\chi \in \text{Ir}(P) \setminus \{1_P\}$  and with  $S_r'$  denoting the subset of  $S_r$  comprising places which split in  $K/k$ .

To prove this we note that for each  $\rho$  in  $\text{Ir}(G)$  one has

$$(22) \quad u_\rho^{-1} \cdot \tau^*(\mathbb{Q}, \text{Ind}_k^{\mathbb{Q}} \rho) = \tau(\mathbb{Q}, \text{Ind}_k^{\mathbb{Q}} \rho) = \left( i^{|S_{cl}|} \sqrt{|d_k|} \right)^{\rho(1)} \cdot \tau(k, \rho),$$

where the first equality follows straight from the definition (16) and the second from the result of [37, Theorem 8.1(iii)].

Now if  $\rho = 1_G$ , then  $\tau(k, \rho) = 1$  and  $V_\rho^{I_w} = \mathbb{C}_p$  for all  $v$  in  $S_r$  so  $u_\rho = (-1)^{|S_r|}$ , whilst it is clear that  $w_\infty(\rho) = i^{|S_{cl}|}$ , and so in this case the equality (21) is an immediate consequence of (22).

Next we note that  $\epsilon = \text{Ind}_P^G(\mathbf{1}_P) - \mathbf{1}_G$  and hence that [37, Theorem 8.1(iii)] implies

$$\tau(k, \epsilon) = \frac{\tau(k, \text{Ind}_P^G(\mathbf{1}_P))}{\tau(k, \mathbf{1}_G)} = \tau(k, \text{Ind}_P^G(\mathbf{1}_P)) = i^{|S_{\mathbb{R}}^{\epsilon}|} \sqrt{d_{K/k}} = i^{|S_{\mathbb{R}}^{\epsilon}|} \cdot \frac{\sqrt{|d_K|}}{|d_k|},$$

where  $S_{\mathbb{R}}^{\epsilon}$  is the set of real places of  $k$  that ramify in  $K/k$  and  $d_{K/k}$  the absolute norm of the different of  $K/k$ . One then obtains the claimed equality (21) by substituting this formula for  $\tau(k, \epsilon)$  into (22) and then using that fact that  $w_{\infty}(\epsilon) = i^{|S_{\mathbb{C}}| + |S_{\mathbb{R}}^{\epsilon}|}$  whilst  $u_{\epsilon} = (-1)^{|S_{\mathbb{R}}^{\epsilon}|}$  since  $\det(-\text{Fr}_w | V_{\epsilon}^{I_w})$  is equal to  $-1$  for  $v \in S_{\mathbb{R}}^{\epsilon}$  and to  $1$  for  $v \in S_{\mathbb{R}} \setminus S_{\mathbb{R}}^{\epsilon}$ .

Finally we assume that  $\rho = \text{Ind}_P^G \chi$  with  $\chi \in \text{Ir}(P) \setminus \{\mathbf{1}_P\}$ . Then, just as above, one finds that

$$\begin{aligned} \tau(k, \rho) &= \tau(k, \text{Ind}_P^G(\mathbf{1}_P)) \cdot \tau(K, \chi) \\ &= i^{|S_{\mathbb{R}}^{\epsilon}|} \frac{\sqrt{|d_K|}}{|d_k|} \tau(K, \chi) \\ &= i^{|S_{\mathbb{R}}^{\epsilon}|} \frac{\sqrt{|d_K|}}{|d_k|} \frac{W(\tilde{\chi})}{W_{\infty}(\chi)} \sqrt{Nf(\chi)}, \end{aligned}$$

where  $W(\tilde{\chi})$  is the Artin root number of  $\tilde{\chi}$  and  $W_{\infty}(\chi)$  the infinite part of the Artin root number of  $\chi$  and the final equality follows from the very definition of  $\tau(K, \chi)$ . Now  $W_{\infty}(\chi) = 1$  since no archimedean place ramifies in  $F/K$ . In addition, the inductivity of Artin root numbers implies  $W(\tilde{\chi}) = W(\tilde{\rho})$  and so, since  $\tilde{\rho}$  is an orthogonal character, the main result of Fröhlich and Queyrut in [29] implies that  $W(\tilde{\chi}) = 1$ . Thus, upon substituting the last displayed expression into (22), and noting that  $w_{\infty}(\rho) = i^{\rho(1)|S_{\mathbb{C}}| + |S_{\mathbb{R}}^{\epsilon}|}$ , one obtains the claimed equality (21) in this case.

Having proved (21), we now write  $\theta_Q$  for the generator of the  $\mathbb{Z}_p[G]$ -module  $A(F)_p^*$  that sends  $Q$  to  $1$  and  $g(Q)$  to zero for each non-trivial element  $g$  of  $P$ . We then define  $\iota_p$  to be the isomorphism of  $\mathbb{Z}_p[G]$ -modules  $A(F)_p^* \rightarrow A(F)_p$  that sends  $\theta_Q$  to  $Q$ .

One computes that  $((\mathbb{C}_p \otimes_{\mathbb{Z}_p} \iota_p) \circ \lambda_{A,F}^{\text{NT},j})(Q) = j_*(R_Q)(Q)$ , where  $R_Q$  is the resolvent element  $\sum_{g \in P} \langle Q, g(Q) \rangle_F \cdot g$  in  $\mathbb{C}_p[G]$ , and also that  $\theta_Q(\iota_p(\vartheta)) = \vartheta(Q)$  for all  $\vartheta \in A(F)_p^*$ .

Proposition 5.7 implies  $r_{\rho_A} = 0$  so  $R_{\rho_A, \iota_p}^{\text{NT},j}(A/F) = 1 = H_{\rho_A}$  and also that for each  $\psi \in \text{Ir}(G) \setminus \{\rho_A\}$ , the complex vector space  $(V_{\psi} \otimes_{\mathbb{Z}} A(F))^G = \mathbb{C}[G] \cdot T_{\psi}(Q)$  has dimension one and hence  $R_{\psi, \iota_p}^{\text{NT},j}(A/F) \cdot T_{\psi}(Q) = ((\mathbb{C}_p \otimes_{\mathbb{Z}_p} \iota_p) \circ \lambda_{A,F}^{\text{NT},j})(T_{\psi}(Q))$ .

Now, for any  $\vartheta \in A(F)_p^*$  and  $P \in A(F)$  one has  $T_{\check{\psi}}(\vartheta)(P) = \vartheta(T_{\check{\psi}}^{\#}(P))$  where we write  $x \mapsto x^{\#}$  for the  $\mathbb{Z}_p$ -linear involution on  $\mathbb{Z}_p[G]$  that inverts elements of  $G$ . In addition, for each  $\psi \neq \rho_A$  one has

$$\begin{aligned} T_{\check{\psi}}(\theta_Q)(T_{\psi}(Q)) &= \sum_{g \in G} \sum_{h \in G} \check{\psi}(g^{-1}) \psi(h^{-1}) \theta_Q(g^{-1} h Q) \\ &= \sum_{g \in G} \check{\psi}(g^{-1}) \psi(g^{-1}) + (-1)^{1 - \text{rk}(A_k)} \cdot \sum_{g \in G} \check{\psi}(g^{-1}) \psi(\tau g^{-1}) \end{aligned}$$

because  $g^{-1} h Q$  is a multiple of  $Q$  only when  $h = g$  or  $h = g\tau$ . The first sum here is always equal to  $|G|$ , while the second is equal to  $|G|$  for  $\psi = \mathbf{1}$ , to  $-|G|$  for  $\psi = \epsilon$  and to  $0$  otherwise. Hence, writing  $\vartheta$  for  $\lambda_{A,F}^{\text{NT},j}(T_{\psi}(Q))$ , we find that

$$\begin{aligned}
\frac{2|G|}{\psi(1)} R_{\psi, \iota_p}^{\text{NT}, j}(A/F) &= T_{\tilde{\psi}}(\theta_Q) \left( (\mathbb{C}_p \otimes_{\mathbb{Z}_p} \iota_p) \circ \lambda_{A, F}^{\text{NT}, j}(T_{\tilde{\psi}}(Q)) \right) \\
&= \theta_Q \left( T_{\tilde{\psi}}^{\#} \left( (\mathbb{C}_p \otimes_{\mathbb{Z}_p} \iota_p)(\vartheta) \right) \right) = \theta_Q \left( (\mathbb{C}_p \otimes_{\mathbb{Z}_p} \iota_p)(T_{\tilde{\psi}}^{\#}(\vartheta)) \right) \\
&= (T_{\tilde{\psi}}^{\#}(\vartheta))(Q) = \vartheta(T_{\tilde{\psi}}(Q)) = j(\langle T_{\tilde{\psi}}(Q), T_{\tilde{\psi}}(Q) \rangle_F) = \frac{2|G|}{\psi(1)} j(h_{F, \psi}(Q)).
\end{aligned}$$

Upon substituting this equality and (21) into the definition of  $\mathcal{L}_{A, F/k, j, \iota_p}^*$  one obtains the element  $\mathcal{L}'$ , as required.  $\square$

In the next result we write  $\mathcal{O}_L$  for the valuation ring of a finite extension  $L$  of  $\mathbb{Q}_p$ .

**Lemma 5.12.** *Write  $\mathfrak{M}'_p$  for the integral closure of  $\mathbb{Z}_p$  in  $\mathbb{Q}_p[P]$ .*

(i) *The following diagram commutes*

$$\begin{array}{ccc}
\text{Nrd}_{\mathbb{Q}_p[G]}(\mathfrak{M}'_p^\times) & \xrightarrow{\text{res}} & \mathfrak{M}'_p^\times \\
\text{Nrd}_{\mathbb{Q}_p[G]} \uparrow & & \uparrow \text{Nrd}_{\mathbb{Q}_p[P]} \\
\text{im}(\alpha : K_1(\mathfrak{M}'_p) \rightarrow K_1(\mathbb{Q}_p[G])) & \xrightarrow{\text{res}'} & \text{im}(\beta : K_1(\mathfrak{M}'_p) \rightarrow K_1(\mathbb{Q}_p[P])) \\
\partial'_{G, p} \downarrow & & \downarrow \partial'_{P, p} \\
K_0(\mathbb{Z}_p[G], \mathbb{Q}_p[G])_{\text{tor}} & \xrightarrow{\text{res}_{P, 0}^G} & K_0(\mathbb{Z}_p[P], \mathbb{Q}_p[P])_{\text{tor}}.
\end{array}$$

Here  $\text{res}$  is the homomorphism that sends an element  $\sum_{\psi \in \text{Ir}(G)} \xi_\psi e_\psi$  in  $\text{Nrd}_{\mathbb{Q}_p[G]}(\mathfrak{M}'_p^\times) \subset \zeta(\mathbb{C}_p[G])^\times = \sum_{\psi} \mathbb{C}_p^\times e_\psi$  to  $\xi_{1_G} \xi_\epsilon e_{1_P} + \sum_{\chi \in \text{Ir}(P) \setminus \{1_P\}} \xi_{\text{Ind}_P^G \chi} e_\chi$ , next  $\alpha$  and  $\beta$  are the natural scalar extension homomorphisms,  $\text{res}'$  and  $\text{res}_{P, 0}^G$  the natural restriction homomorphisms and  $\partial'_{G, p}$  and  $\partial'_{P, p}$  the restrictions of the connecting homomorphisms  $\partial_{G, p}$  and  $\partial_{P, p}$ .

(ii) *The homomorphism  $\text{res}_{P, 0}^G$  is injective.*

(iii) *Fix  $\mathcal{E} := \sum_{\chi \in \text{Ir}(P)} \mathcal{E}_\chi e_\chi$  inside  $\mathfrak{M}'_p^\times = \sum_{\chi \in \text{Ir}(P)} \mathcal{O}_{\mathbb{Q}_p(\chi)}^\times e_\chi$ . Then  $\mathcal{E}$  belongs to  $\mathbb{Z}_p[P]^\times$  if and only if  $\sum_{\chi \in \text{Ir}(P)} \chi(\pi)^{-1} \mathcal{E}_\chi$  belongs to  $|P| \cdot \mathbb{Z}_p$  for all  $\pi$  in  $P$ .*

*Proof.* To prove claim (i) we fix a set of representatives  $\text{Ir}(P)^\dagger$  of the orbits of the action of  $G_{\mathbb{Q}_p}$  on  $\text{Ir}(P)$  and abbreviate the functor  $\text{Ind}_P^G(-)$  to  $\text{I}_P^G(-)$ .

The commutativity of the lower square of the diagram follows from the naturality of the long exact sequences of relative  $K$ -theory. To consider the upper square we use the  $\mathbb{Q}_p$ -algebra isomorphisms

$$\omega_G : \mathbb{Q}_p[G] \cong \mathbb{Q}_p \times \mathbb{Q}_p \times \prod_{\chi \in \text{Ir}(P)^\dagger \setminus \{1_P\}} \text{M}_2(\mathbb{Q}_p(\text{I}_P^G(\chi)))$$

and  $\omega_P : \mathbb{Q}_p[P] \cong \prod_{\chi \in \text{Ir}(P)^\dagger} \mathbb{Q}_p(\chi)$  where  $\omega_G(g) = (1, \epsilon(g), (S_{\text{I}_P^G(\chi)}(g))_\chi)$ , with  $S_{\text{I}_P^G(\chi)}$  a representation  $G \rightarrow \text{M}_2(\mathbb{Q}_p(\text{I}_P^G(\chi)))$  of character  $\text{I}_P^G(\chi)$ , and  $\omega_P(\pi) = (\chi(\pi))_\chi$  for each  $g \in G$  and  $\pi \in P$ . Taken together these isomorphisms induce a diagram

$$\begin{array}{ccc}
 \mathbb{Q}_p^\times \times \mathbb{Q}_p^\times \times \prod_{\substack{\chi \in \text{Ir}(P)^\dagger \\ \chi \neq \mathbf{1}_P}} \mathbb{Q}_p(\mathbb{I}_P^G(\chi))^\times & \xrightarrow{\widetilde{\text{res}}} & \prod_{\chi \in \text{Ir}(P)^\dagger} \mathbb{Q}_p(\chi)^\times \\
 \uparrow (\det, \det, (\det)_\chi) & & \uparrow (\det)_\chi \\
 K_1(\mathbb{Q}_p) \times K_1(\mathbb{Q}_p) \times \prod_{\substack{\chi \in \text{Ir}(P)^\dagger \\ \chi \neq \mathbf{1}_P}} K_1\left(M_2(\mathbb{Q}_p(\mathbb{I}_P^G(\chi)))\right) & & \prod_{\chi \in \text{Ir}(P)^\dagger} K_1(\mathbb{Q}_p(\chi)) \\
 \uparrow K_1(\omega_G) & & \uparrow K_1(\omega_P) \\
 K_1(\mathbb{Q}_p[G]) & \xrightarrow{\text{res}_{P,1}^G} & K_1(\mathbb{Q}_p[P])
 \end{array}$$

in which the left and right hand composite vertical arrows are equal to  $\text{Nrd}_{\mathbb{Q}_p[G]}$  and  $\text{Nrd}_{\mathbb{Q}_p[P]}$  and  $\widetilde{\text{res}}$  is defined to make the diagram commute. To complete the proof of claim (i) it thus suffices to show  $\widetilde{\text{res}}$  sends each element  $(\alpha, \tilde{\alpha}, (a_\chi)_\chi)$  to  $(\alpha\tilde{\alpha}, (a_\chi)_\chi)$  and this follows from the argument used by Breuning in [10, Lemma 3.9].

To prove claim (ii) we recall a group is said to be  $\mathbb{Q}_p$ -elementary if it is isomorphic to a group  $(\mathbb{Z}/n\mathbb{Z}) \rtimes J$  where  $J$  is an  $\ell$ -group for some prime  $\ell$  that is coprime to  $n$  and the image of the homomorphism  $J \rightarrow \text{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong \text{Gal}(\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q})$  belongs to the decomposition subgroup of  $p$ . This means that a subgroup of  $G$  is  $\mathbb{Q}_p$ -elementary if it is either a subgroup of  $P$  or of the form  $\langle C, \tau' \rangle$  where  $C$  is a cyclic subgroup of  $P$  and  $\tau'$  an element of order 2. We consider the exact commutative diagram

$$\begin{array}{ccccccc}
 K_1(\mathbb{Z}_p[G]) & \longrightarrow & K_1(\mathbb{Q}_p[G]) & \longrightarrow & K_0(\mathbb{Z}_p[G], \mathbb{Q}_p[G]) & \longrightarrow & 0 \\
 \downarrow \alpha_1 & & \downarrow \alpha_2 & & \downarrow \alpha_3 & & \\
 \varprojlim_H K_1(\mathbb{Z}_p[H]) & \longrightarrow & \varprojlim_H K_1(\mathbb{Q}_p[H]) & \longrightarrow & \varprojlim_H K_0(\mathbb{Z}_p[H], \mathbb{Q}_p[H]) & & 
 \end{array}$$

where the limits are over all  $\mathbb{Q}_p$ -elementary subgroups  $H$  of  $G$ . The transition maps are the homomorphisms induced by inclusions  $H \subseteq H'$  and by maps of the form  $H \rightarrow gHg^{-1}$  for  $g \in G$  and all vertical arrows are the natural restriction maps. By a theorem of Dress [27] (see also [43, Theorem 11.2]), the maps  $\alpha_1$  and  $\alpha_2$  are bijective and hence  $\alpha_3$  is injective. Now  $K_0(\mathbb{Z}_p[H], \mathbb{Q}_p[H])_{\text{tor}}$  is trivial whenever  $H$  has order prime to  $p$  and in [10, Proposition 3.2.(2)] Breuning has shown that the restriction map  $K_0(\mathbb{Z}_p[H], \mathbb{Q}_p[H])_{\text{tor}} \rightarrow K_0(\mathbb{Z}_p[C], \mathbb{Q}_p[C])_{\text{tor}}$  is injective for any subgroup  $H$  of the form  $\langle C, \tau' \rangle$ . The map  $\alpha_3$  therefore restricts to give an injective homomorphism

$$K_0(\mathbb{Z}_p[G], \mathbb{Q}_p[G])_{\text{tor}} \rightarrow \varprojlim_J K_0(\mathbb{Z}_p[J], \mathbb{Q}_p[J])_{\text{tor}} \cong K_0(\mathbb{Z}_p[P], \mathbb{Q}_p[P])_{\text{tor}},$$

where  $J$  runs over all subgroups of  $P$ , as required to prove claim (ii).

Claim (iii) follows from the equalities

$$\mathcal{E} = \sum_{\chi \in \text{Ir}(P)} \mathcal{E}_\chi \sum_{\pi \in P} |P|^{-1} \chi(\pi)^{-1} \pi = \sum_{\pi \in P} \left( |P|^{-1} \sum_{\chi \in \text{Ir}(P)} \chi(\pi)^{-1} \mathcal{E}_\chi \right) \pi$$

and the fact that  $\mathbb{Z}_p[P]^\times = \mathbb{Z}_p[P] \cap \mathfrak{M}_p^\times$ . □

## 6. SPECIAL CASES

In this section we use the criteria of Theorem 5.8 to give both theoretical and numerical verifications of the  $p$ -part of the equivariant Tamagawa number conjecture for pairs  $(h^1(A/F)(1), \mathbb{Z}[G])$  where  $A$  is an elliptic curve for which  $A(F)$  has strictly positive rank and  $G$  is both non-abelian and of order divisible by  $p$ .

We believe that, apart from the recent results of Bley in [5], where the group  $A(F)_p$  is assumed to be trivial and the field  $F$  to be an abelian extension of  $\mathbb{Q}$  of exponent  $p$ , these results constitute the first verifications of the  $p$ -part of the equivariant Tamagawa number conjecture for any elliptic curve and any Galois extension of degree divisible by  $p$ .

We begin by giving the proof of Theorem 1.1, which relies on the theory of Heegner points and makes crucial use of the theorem of Gross and Zagier. We note that the additional hypotheses in Theorem 1.1 imply the validity of hypothesis (i). In addition, Kolyvagin [31, Proposition 2.1] shows that in this case one has  $\text{III}_p(A_K) = 0$ . In particular one knows that the  $p$ -primary part of the Birch and Swinnerton-Dyer conjecture holds for  $A/K$ . Furthermore, the hypotheses (d) and (h) are obviously satisfied in the setting of Theorem 1.1.

**6.1. The proof of Theorem 1.1.** In view of Theorems 5.1 and 5.8 we are reduced to verifying the conditions (i) and (ii) that occur in the latter result.

To do this we fix a modular parametrisation  $\varphi: X_0(N) \rightarrow A$  of smallest degree. We also denote by  $c$  the Manin constant of  $\varphi$  and write  $Q$  for the trace in  $A(F)$  of the Heegner point that is defined over the Hilbert class field of  $K$ .

Set  $C := 4c_\infty \cdot c^{-2} \cdot |\mathcal{O}_K^\times|^{-2}$  and  $c_\infty = [A(\mathbb{R}) : A^0(\mathbb{R})]$  is the number of connected components of  $A(\mathbb{R})$ . Under our hypotheses, the theorem of Gross and Zagier (see, in particular, [32, §I, (6.5) and the discussion on p. 310]) implies that for each  $\chi \in \text{Ir}(P)$  one has

$$(23) \quad 0 \neq \frac{L'(A/K, \chi, 1) \sqrt{|d_K|}}{\Omega_\infty^+(A) \Omega_\infty^-(A)} = C \cdot \frac{1}{|P|} \langle T_\chi(Q), T_{\bar{\chi}}(Q) \rangle_F \\ = \begin{cases} C \cdot h_{F, \text{Ind}_P^G(\chi)}(Q), & \text{if } \chi \neq \mathbf{1}_P \\ C \cdot h_{F, \rho'_A}(Q), & \text{if } \chi = \mathbf{1}_P, \end{cases}$$

where  $\rho'_A$  is the linear character of  $G$  appearing in  $A(K)$  and  $\infty$  denotes the archimedean place of  $\mathbb{Q}$ . The second equality here follows from the equality  $T_{\text{Ind}_P^G \chi} = T_\chi + T_{\bar{\chi}}$  and the fact that  $\langle T_\chi(Q), T_\chi(Q) \rangle_F = 0$  (since the height pairing is  $G$ -invariant).

For each  $\psi$  in  $\text{Ir}(G)$  we set

$$(24) \quad \hat{Q}_\psi := \frac{L^*(A, \psi, 1) \cdot \sqrt{d_\psi}}{\Omega(A, \psi) \cdot H_\psi}$$

where the quantities  $d_\psi$  and  $H_\psi$  are as defined just before Theorem 5.8. We also write

$$(25) \quad t_\psi = \frac{L_{S_r}^*(A, \psi, 1)}{L^*(A, \psi, 1)}$$

for the correction term that accounts for the  $S_r$ -truncation in the leading terms for each  $\psi \in \text{Ir}(G)$ . Then the non-zero complex number  $\mathcal{Q}_\psi := u_\psi \cdot t_\psi \cdot \hat{Q}_\psi$  is as in Theorem 5.8 using our Heegner point  $Q$ . By using (23), and the fact that  $d_\psi = d_1 d_\epsilon = |d_K|$  for all  $\psi$  of dimension two (as  $F/K$  is unramified), one then finds that

$$(26) \quad \mathcal{Q}_1 \cdot \mathcal{Q}_\epsilon = u_1 t_1 u_\epsilon t_\epsilon \cdot C, \quad \text{and} \\ \mathcal{Q}_\psi = u_\psi t_\psi \cdot C \quad \text{if } \psi = \text{Ind}_P^G \chi \text{ for } \chi \in \text{Ir}(P) \setminus \{\mathbf{1}_P\}.$$

Our hypotheses imply that  $A(K)$  has rank one and  $\text{III}_p(A_K)$  vanishes by Kolyvagin [31] and hence all of the hypotheses of Theorem 5.8 are satisfied except for the requirement that  $p$  splits in  $K/\mathbb{Q}$ . However, the sole purpose of the latter hypothesis is to ensure (via the proof of Proposition 5.7) that the  $\mathbb{Q}[P]$ -module  $\mathbb{Q} \otimes_{\mathbb{Z}} A(F)$  has a free rank one direct summand and so, since (23) implies that the point  $Q$  generates such a summand, this hypothesis can be ignored in our case. Following Remark 5.9, it therefore suffices for us to prove that the terms  $\mathcal{Q}_\psi$  satisfy both the conditions of Theorem 5.8(i) and the congruences (19).

Since the  $p$ -part of the Birch and Swinnerton-Dyer conjecture holds for  $A/K$ , the hypotheses (a) and (b) and the known vanishing of  $\text{III}_p(A_K)$  combine to imply that  $\hat{\mathcal{Q}}_1$  and  $\hat{\mathcal{Q}}_\epsilon$  are both  $p$ -units. The hypothesis (c) implies that  $A$  has good reduction at  $p$  and so the hypothesis (ii) combines with [1, Theorem 2.7] to imply that the Manin constant  $c$  is a  $p$ -unit. Using also the fact that  $p$  is unramified, we find that  $C$  is a  $p$ -unit too.

We proceed to compute the values of  $u_\psi$  and  $t_\psi$ . Since  $F/K$  is unramified, we have that each ramified place  $v$  in  $S_r$  has ramification index 2 and  $v$  does not split in  $K/\mathbb{Q}$ . It is easy to see that  $u_\epsilon = 1$  and that  $u_1 = u_\psi = (-1)^{|S_r|}$  for all  $\psi$  of dimension two. Next, for any  $\psi$  in  $\text{Ir}(G)$ , we have

$$t_\psi = \prod_{v \in S_r} \text{Nrd}_{\mathbb{C}_p[G]} \left( 1 - \text{Fr}_w^{-1} |\kappa_v|^{-1} \left| (T_p(A) \otimes V_\psi)^{I_w} \right| \right)$$

and since no place of bad reduction is allowed to ramify by hypothesis (e), one has  $(T_p(A) \otimes V_\psi)^{I_w} = T_p(A) \otimes V_\psi^{I_w}$ . Hence  $t_\epsilon = 1$  and  $t_1 = t_\psi$  for all  $\psi$  of dimension two. Moreover, this last value  $t_1$  is equal to  $\prod_{v \in S_r} |A(\kappa_v)|/|\kappa_v|$ , which is a  $p$ -unit by hypothesis (f). Therefore  $\mathcal{Q}_\psi$  is a  $p$ -unit for all  $\psi \in \text{Ir}(G)$ .

Next we note that  $\mathcal{Q}_1 \cdot \mathcal{Q}_\epsilon = \mathcal{Q}_\psi$  for any  $\psi$  of dimension two as we have shown that  $u_1 t_1 u_\epsilon t_\epsilon = u_\psi t_\psi$ . Since each element  $\mathcal{Q}_\psi$  also belongs to  $\mathbb{Q}$ , this formula makes it clear that they satisfy the condition of Theorem 5.8(i). In addition, it shows that for any  $\pi \in P$  one has

$$- \sum_{\chi \in \text{Ir}(P) \setminus \{1_P\}} \check{\chi}(\pi) \mathcal{Q}_{\text{Ind}_P^G \chi} = -\mathcal{Q}_1 \mathcal{Q}_\epsilon \cdot \left( -1 + \sum_{\chi \in \text{Ir}(P)} \check{\chi}(\pi) \right).$$

Finally we note that the last sum in the above expression is equal to 0 if  $\pi \neq 1$  and to  $|P|$  otherwise. Hence the expression is in both cases congruent to  $\mathcal{Q}_1 \mathcal{Q}_\epsilon$  modulo  $p\mathbb{Z}_{(p)}$ , as required to complete the proof of Theorem 1.1.

**6.2.  $S_3$ -extensions.** In this section we investigate the case that  $F/K$  is a cyclic extension of degree  $p = 3$  and hence  $F/k$  is a non-abelian extension of degree six. We show that the conjecture of Birch and Swinnerton-Dyer (or ‘BSD’ for short) implies an explicit congruence modulo rational squares and then combine this congruence with Theorem 5.8 to prove the equality (17) for a natural family of examples.

We assume throughout that  $G$  is a non-abelian group of order six. In this case  $\text{Ir}(G)$  comprises  $1 := \mathbf{1}_G$ ,  $\epsilon$  and  $\psi = \text{Ind}_P^G \chi$  for a fixed  $\chi$  in  $\text{Ir}(P) \setminus \{1_P\}$ . We fix a subfield  $L$  of  $F$  that is of degree 3 over  $k$  and set  $H := G_{F/L}$ .

6.2.1. *An arithmetic congruence.* For each character  $\eta$  in  $\text{Ir}(G)$  we define

$$(27) \quad \tilde{\mathcal{Q}}_\eta := \frac{L^*(A, \eta, 1) \cdot \sqrt{d_\eta}}{\Omega(A, \eta) \cdot \tilde{H}_\eta}.$$

Here the quantities  $d_\eta$  are as defined just before Theorem 5.8 and we have set

$$(28) \quad \tilde{H}_1 := \text{Reg}(A/k), \quad \tilde{H}_\epsilon := \frac{\text{Reg}(A/K)}{\text{Reg}(A/k)}, \quad \text{and} \quad \tilde{H}_\psi := \frac{\text{Reg}(A/L)}{\text{Reg}(A/k)}$$

with  $\text{Reg}(A/E)$  denoting the regulator of  $\langle \cdot, \cdot \rangle_E$  on the Mordell-Weil group  $A(E)$  for any field  $E$ . These slight variations of the regulators that we used earlier fit well with BSD and do not require any knowledge of the explicit Galois structure of  $A(F)_p$ . In fact, BSD predicts that each expression  $\tilde{Q}_\eta$  is a non-zero rational number.

In the following result we include the assumed analytic continuation of the  $L$ -series and finiteness of the Tate-Shafarevich group in the assumption that BSD holds but do not assume any of the hypotheses (a)–(d) and (f)–(h). This result may therefore suggest one sort of congruence relation that might be expected to hold when our hypotheses fail. We note also that the remark made by Dokchitser and Dokchitser in the fourth paragraph after Conjecture 1.4 of [26] hints at the possibility of this sort of result in a more restrictive setting.

**Theorem 6.1.** *Let  $A$  be an elliptic curve over  $k$  and assume no place at which  $A$  has bad reduction ramifies in  $F/k$ . Then if the Birch and Swinnerton-Dyer conjecture holds for  $A/k$ ,  $A/K$  and  $A/L$  one has a congruence modulo non-zero rational squares*

$$(29) \quad \tilde{Q}_1 \cdot \tilde{Q}_\epsilon \equiv \tilde{Q}_\psi \pmod{\square}.$$

*Proof.* Fix a finite field extension  $E$  of  $k$ . If  $v$  is a (finite or infinite) place of  $E$ , write  $c(A/E_v)$  for the number of connected components  $[A(E_v) : A(E_v)^0]$  of  $A(E_v)$ . For a finite place  $v$  in  $E$ , also write  $\omega_v^{\text{Né}}$  for a Néron differential of  $A/E_v$ . Then BSD for the field  $E$  asserts that

$$(30) \quad \frac{L^*(A/E, 1) \sqrt{|d_E|}}{\Omega(A/E) \cdot \text{Reg}(A/E)} = \prod_{\text{all } v} c(A/E_v) \cdot \prod_{\text{finite } v} \left| \frac{\omega_A}{\omega_v^{\text{Né}}} \right|_v \cdot \frac{|\text{III}(A_E)|}{|A(E)_{\text{tor}}|^2}$$

where we write  $\Omega(A/E)$  for the period  $\prod_{v \in S_{\mathbb{R}}^E} \Omega_v^+(A) \cdot \prod_{v \in S_{\mathbb{C}}^E} \Omega_v(A)$  of  $A$  over  $E$ , as defined in §4.4.1 with respect to a fixed invariant differential  $\omega_A$  of  $A/k$ .

The term  $\tilde{Q}_1$  is equal to the left hand side of (30) with  $E = k$ . Furthermore the products  $\tilde{Q}_1 \tilde{Q}_\epsilon$  and  $\tilde{Q}_1 \tilde{Q}_\psi$  link to the left hand sides of (30) for the fields  $K$  and  $L$  respectively. More precisely, one has

$$\tilde{Q}_1 \cdot \tilde{Q}_\epsilon = \frac{L^*(A/K, 1) \sqrt{|d_K|}}{\Omega(A/K) \cdot \text{Reg}(A/K)} \cdot \prod_{v \in S_{\mathbb{R}}^K} c(A/k_v)$$

where, as before,  $S_{\mathbb{R}}^K$  denotes the set of real places of  $k$  that become complex places in  $K$ . The formula for  $\tilde{Q}_1 \tilde{Q}_\psi$  is modified by the same factor as there is exactly one complex place in  $L$  above each place in  $S_{\mathbb{R}}^K$ . In proving this last formula one also uses the fact that  $d_\psi = |d_K| \cdot Nf(\chi)$  is equal to  $|d_L/d_k|$  since  $\psi = \text{Ind}_H^G \mathbf{1}_H - \mathbf{1}$ .

In addition, since we are working modulo squares, we may neglect the terms  $|\text{III}(A_E)|$  and  $|A(E)_{\text{tor}}|^2$  which occur on the right hand side of the formula (30). The required congruence (29) will therefore be proved if we can show for each place  $v$  in  $k$  that

$$(31) \quad c(A/k_v) \cdot \prod_{\substack{w|v \\ \text{in } K}} c(A/K_w) \equiv \prod_{\substack{w|v \\ \text{in } L}} c(A/L_w) \pmod{\square}$$

and for each finite place  $v$  in  $k$  that

$$(32) \quad \left| \frac{\omega_A}{\omega_v^{\text{Né}}} \right|_v \cdot \prod_{\substack{w|v \\ \text{in } K}} \left| \frac{\omega_A}{\omega_w^{\text{Né}}} \right|_w = \prod_{\substack{w|v \\ \text{in } L}} \left| \frac{\omega_A}{\omega_w^{\text{Né}}} \right|_w.$$

Now, by our assumption, no place at which  $A$  has bad reduction is ramified in  $F/k$  and so the Néron differential for  $A$  over  $k_v$  remains a Néron differential for  $A$  over both of the fields  $K_w$  and

$L_w$ . Hence the equation (32) is valid for all finite places, because  $\omega_A/\omega_v^{N\acute{e}}$  is in  $k_v$  and one has  $[k : k] + [K : k] = [L : k]$ .

Next we note that the congruence (31) only needs to be checked at places at which  $A$  has bad reduction (and which therefore do not ramify in  $F/k$ ) and at infinite places. If the decomposition group  $G_v$  at a place above  $v$  in  $F$  is trivial, then both sides of this congruence are equal to  $c(A/k_v)^3$ . If  $G_v$  is cyclic of order 2, then there is one place  $w'$  in  $L$  with  $L_{w'} = k_v$  and one place  $w''$  with  $L_{w''} = K_w$  for the unique place  $w$  above  $v$  in  $K$  and so both sides of (31) are equal to  $c(A/k_v) \cdot c(A/K_w)$ . Finally we have to treat the case when  $G_v$  is cyclic of order 3 and hence the place  $v$  is finite. In this case the left hand side of (31) is equal to  $c(A/k_v)^3$  while the right hand side is equal to  $c(A/L_w)$  where  $L_w$  is an unramified cubic extension of  $k_v$ . If  $c(A/L_w) = c(A/k_v)$  then we have indeed a congruence modulo squares. However it is possible that the Tamagawa numbers change in an unramified extension. Luckily, the only possibility for this to happen in a cubic extension is when the Kodaira type is  $I_0^*$  and then the change is from  $c(A/k_v) = 1$  to  $c(A/L_w) = 4$ , see for instance Step 6 in [47] on page 367, and the congruence (31) holds in all cases.  $\square$

6.2.2. *The connection to  $eTNC_p$ .* We now use Theorem 6.1 to show that, under the hypotheses of Theorem 5.8, the relevant cases of BSD imply the equality (17).

**Corollary 6.2.** *We assume that the elliptic curve  $A$  and field  $F$  satisfy the hypotheses (a)–(h). We assume also that  $G$  and  $L$  are as in Theorem 6.1 (so  $p = 3$ ) and that the Birch and Swinnerton-Dyer conjecture holds for  $A$  over each of the fields  $k$ ,  $K$  and  $L$ .*

*Then the equality (17) is valid provided that  $\text{III}_p(A_K) = 0$ ,  $\text{rk}(A_K) = 1$  and there exists a point  $Q$  in  $A(F)$  which generates a  $G$ -module of finite prime-to- $p$  index in  $A(F)$  that is isomorphic to  $\mathbb{Z}[G](1 - (-1)^{\text{rk}(A_K)}\tau)$ .*

*Proof.* First, we note that given our hypotheses (a), (b) and (e), our choice of  $\omega_A$  (as in §4.4.1) and our assumption that  $\text{III}_p(A_K)$  vanishes, the validity of BSD implies that the term  $\tilde{Q}_\eta$  is a  $p$ -adic unit for all  $\eta \in \text{Ir}(G)$ .

Next we link  $\tilde{Q}_\eta$  to  $Q_\eta$  in Theorem 5.8, the difference being the terms  $\tilde{H}_\eta$  versus  $H_\eta$  and the terms  $u_\eta$  and  $t_\eta$  (as defined in (25)). Using the explicit structure of  $A(F)_p$ , it is easy to show that

$$H_\psi \equiv \tilde{H}_\psi, \quad H_\epsilon \equiv \begin{cases} \tilde{H}_\epsilon & \text{if } \rho_A = \mathbf{1} \\ \frac{1}{2} \tilde{H}_\epsilon & \text{if } \rho_A = \epsilon \end{cases} \quad \text{and} \quad H_{\mathbf{1}} \equiv \begin{cases} \tilde{H}_{\mathbf{1}} & \text{if } \rho_A = \mathbf{1} \\ 2 \tilde{H}_{\mathbf{1}} & \text{if } \rho_A = \epsilon. \end{cases}$$

where all congruences are modulo squares in  $\mathbb{Z}_{(3)}^\times$ ; namely the quotients are squares of indices, like the index of  $\mathbb{Z}[G]Q$  in  $A(F)$ . Up to squares in  $\mathbb{Z}_{(3)}^\times$  we therefore have a congruence

$$\frac{1}{u_{\mathbf{1}} t_{\mathbf{1}} u_\epsilon t_\epsilon} Q_{\mathbf{1}} Q_\epsilon \equiv \frac{1}{u_\psi t_\psi} Q_\psi.$$

An argument similar to the one that concludes the proof of Theorem 1.1 hence implies that we will have verified the criterion in Theorem 5.8 if we show that  $u_{\mathbf{1}} t_{\mathbf{1}} u_\epsilon t_\epsilon$  and  $u_\psi t_\psi$  are 3-adic units that are congruent modulo 3. Writing  $N_v = |A(\kappa_v)|$  for the number of points in the reduction at a place  $v$  and  $q_v = |\kappa_v|$ , we can summarise the computations of the local contribution to these terms at a place  $v \in S_r$  in the following table according to the type of ramification. Here  $e_v$  stands for the ramification index at a place in  $F$  above  $v$  and  $f_v$  for the residual degree.

$e_v$	$f_v$	$\det(-Fr_w   V_\eta^{I_w})$			$\det(1 - Fr_w^{-1} q_v^{-1}   (V_\eta \otimes T_p(A))^{I_w})$		
		$u_1$	$u_\epsilon$	$u_\psi$	$t_1$	$t_\epsilon$	$t_\psi$
2	1	-1	1	-1	$N_v/q_v$	1	$N_v/q_v$
3	1	-1	-1	1	$N_v/q_v$	$N_v/q_v$	1
3	2	-1	1	1	$N_v/q_v$	$N_w/q_w \cdot q_v/N_v$	1

In the last line  $w$  denotes the unique place  $w$  in  $K$  above  $v$ . If a place  $v$  were totally ramified it must be above 2 or 3 as the tame inertia group is cyclic and it can not be above 2 because the wild inertia group is normal in the inertia group. Hence there was no need to list the totally ramified case as all places above  $p = 3$  were assumed to be unramified by (h). From the table we can conclude that all the terms  $u_\eta$  and  $t_\eta$  are indeed 3-units by (f) and that

$$\frac{u_1 u_\epsilon}{u_\psi} \cdot \frac{t_1 t_\epsilon}{t_\psi} \equiv \prod_{v \in S_r''} \left( -\frac{N_w}{q_w} \right) \equiv \prod_{v \in S_r''} (-N_w) \pmod{\square}$$

with  $S_r'' := \{v \mid e_v = 3 \text{ and } f_v = 2\}$ .

Hence we are reduced to showing that  $-N_w \equiv 1 \pmod{3}$  when  $e_v = 3$  and  $f_v = 2$ . We first note that for such a place we must have  $q_v \equiv -1 \pmod{3}$ . Indeed, this is true because the map  $\theta_0 : \text{Gal}(F_{w'}/K_w) \rightarrow \mu_3(\kappa_w)$  in Corollaire IV.1 in [45] is  $G$ -equivariant and, since  $F_{w'}/k_v$  is dihedral, the action of  $\tau$  on  $\mu_3(\kappa_w)$  is non-trivial.

Finally, we have the equality  $N_w = N_v \cdot (2q_v + 2 - N_v)$  valid for all quadratic extension of finite fields. Hence  $N_w \equiv -N_v^2 \equiv -1 \pmod{3}$ .  $\square$

*Remark 6.3.* A closer analysis of the above argument shows that the hypotheses of Corollary 6.2 may be weakened a little. One can allow places above 3 to be tamely ramified in  $F/k$  and can omit any assumption about the reduction of  $A$  at such places. In addition, one need only assume that the group  $A(\kappa_v)[p]$  vanishes for places  $v$  that are both inert in  $K/k$  and ramify in  $F/K$ .

*Remark 6.4.* For any prime  $p > 3$ , the methods used in the proofs of Theorem 6.1 and Corollary 6.2 enable one to deduce from the assumed validity of suitable cases of the Birch-Swinnerton-Dyer Conjecture a congruence for the product  $\prod_{\dim(\psi)=2} \hat{Q}_\psi$ , rather than for the sum  $\sum_{\dim(\psi)=2} \hat{Q}_\psi$  that occurs in (17).

**6.3. Numerical examples.** In this final section we describe two numerical examples to further illustrate the predicted congruences in Theorem 5.8 and to explain how one can check these congruences for numerous examples. It is comparatively straightforward to give examples with  $p = 3$  but Corollary 6.2 implies that there is limited interest in doing so. We therefore discuss examples with  $p = 7$  and  $p = 5$ .

Our numerical computations were done using Sage [48], which uses underlying Pari-GP [49]. The computations of the  $L$ -values was done in Magma [9] which contains an implementation of [25]. The code can be obtained from the last named author's webpage.

**6.3.1. A Stark-Heegner point example.** We consider the example of the elliptic curve labelled 37a1 in Cremona's tables [20]

$$A: \quad y^2 + y = x^3 - x$$

over the Hilbert class field  $F$  of  $K = \mathbb{Q}(\sqrt{577})$ . The curve has rank 1 over  $\mathbb{Q}$  and  $K$ . The extension  $F/K$  is of degree  $p = 7$  defined by a root  $\xi$  of the polynomial

$$x^7 - 2x^6 - 7x^5 + 10x^4 + 13x^3 - 10x^2 - x + 1.$$

All hypotheses (a)–(h) except the finiteness of  $\text{III}(A_F)$  in (g) can be verified easily. We find in [23] that there is a point

$$Q = \left( 2\xi^6 - 4\xi^5 - 14\xi^4 + 17\xi^3 + 30\xi^2 - 7\xi - 3, 2\xi^6 - 19\xi^4 - 2\xi^3 + 32\xi^2 + \xi - 5 \right)$$

of infinite order on  $A$  defined over  $L = \mathbb{Q}(\xi)$  obtained from Darmon's construction of modular points. The trace of  $Q$  in  $L/\mathbb{Q}$  is equal to the generator  $R = (0, 0) \in A(\mathbb{Q})$ . Let  $\sigma$  be a generator of  $P$ . It is easy to check that

$$\mathbb{Z}R \oplus \mathbb{Z}Q \oplus \mathbb{Z}(\sigma + \sigma^{-1})Q \oplus \mathbb{Z}(\sigma^2 + \sigma^{-2})Q$$

has finite index coprime to  $p$  in  $A(L)$ . Hence we can take  $Q$  as the point whose existence is predicted by Proposition 5.7. (In the general case, we may have to take a linear combination of a new point in  $A(L)$  and the generator in  $A(\mathbb{Q})$  to assure that the trace generates  $A(\mathbb{Q})$ .) In fact, in our case, we can check that  $A(F) = \mathbb{Z}[G]Q$  by using the bound given in [21].

Using modular symbols for the character  $\epsilon$  and a Heegner point computation for  $\mathbf{1}$ , we can prove that the formulae (24) evaluate to

$$\hat{Q}_{\mathbf{1}} = \frac{L'(A, 1)}{\Omega^+(A) \cdot H_{\mathbf{1}}} = 1 \quad \text{and} \quad \hat{Q}_{\epsilon} = \frac{L(A, \epsilon, 1) \cdot \sqrt{d_K}}{\Omega^+(A)} = 4$$

and hence conclude that BSD holds for  $A/\mathbb{Q}$  and  $A/K$  with  $\text{III}(A_{\mathbb{Q}}) = \text{III}(A_K) = 0$ . Next, we compute a numerical approximation to  $L'(A, \psi, 1)$  for a 2-dimensional representation  $\psi \in \text{Ir}(G)$ . The corresponding value of  $\hat{Q}_{\psi}$  is equal to 4.00000000000000 for all such  $\psi$ , but we know of no means of proving that this value is indeed algebraic and equal to the value 4. It predicts with good accuracy that BSD for  $A/L$  would imply that  $\text{III}(A_L)$  and  $\text{III}(A_F)$  are trivial. However assuming that  $\hat{Q}_{\psi} = 4$ , we compute the  $S_r$ -truncated version

$$Q_{\mathbf{1}} = -\frac{578}{577} \quad \text{and} \quad Q_{\epsilon} = 4 \quad \text{and} \quad Q_{\psi} = -\frac{2312}{577} \quad \text{for all } \dim(\psi) = 2$$

and hence find that the congruence (20) holds modulo  $p = 7$ . Note that in this particular case, the values  $\hat{Q}_{\psi}$  were all in  $\mathbb{Q}$ . In other words we have found convincing numerical evidence that a Gross-Zagier formula

$$\frac{L'(A/K, \chi, 1)\sqrt{d_K}}{\Omega^+(A)^2} = \frac{c_{\infty}^2}{c^2} \cdot \frac{1}{|P|} \langle T_{\chi}(Q), T_{\bar{\chi}}(Q) \rangle_F$$

analogous to (23) should hold for all  $\chi \in \text{Ir}(P)$  because  $c_{\infty} = 2$  and  $c = 1$ .

6.3.2. *A quintic example.* As a second example, we consider the curve

$$A: \quad y^2 + xy = x^3 - 4x - 1$$

labelled 21a1 in [20]. It has rank 0 over  $\mathbb{Q}$ , but rank 1 over  $K = \mathbb{Q}(i)$  and the group  $A(K)$  is generated by the point

$$R = \left( \frac{3}{2}, \frac{-3+7i}{4} \right).$$

Now we consider the extension  $F/K$  given by a solution  $\xi$  of the polynomial

$$x^5 - 2x^4 - 6x^3 + 10x^2 + 17x - 12$$

The extension  $F/K$  is only ramified at the place  $19\mathbb{Z}[i]$ . All of our hypotheses except (g) can be verified to hold in this example.

By a simple search for points, we find the point

$$T = \left( \frac{1}{8}(-\xi^4 - \xi^2 - 12\xi - 8), \frac{1}{32}(39\xi^4 - 7\xi^3 - 213\xi^2 - 127\xi + 196) \right)$$

of infinite order defined over  $L = \mathbb{Q}(\xi)$ . The bounds in [21] can then be used to prove that  $\mathbb{Z}T \oplus \mathbb{Z}(\sigma + \sigma^{-1})T$  generates  $A(L)_{\text{tf}}$  where  $\sigma$  is a generator of  $P$ . To find the point  $Q$  is a bit more elaborate than in the previous example as  $\rho_A = \mathbf{1}$ . In fact the  $\mathbb{Z}[G]$ -module generated by  $T$  and  $R$  will have index  $p$  in  $A(F)$  because [18, Corollary 2.5] tells us that  $A(F)_p$  is projective. We are going to use the relation

$$p \cdot \sigma^{(p+1)/2} = \text{Tr}_{F/K} + (\sigma - 1) \sum_{i=1}^{(p-1)/2} i (\sigma^i - \sigma^{-i})$$

in  $\mathbb{Z}[G]$  which is reminiscent of Kolyvagin's derivative construction. We now try to find a point  $T' = aT + b(\sigma + \sigma^{-1})T$  in  $A(L)$  with  $0 \leq a, b < p$  such that  $O \neq Q' = R + (\sigma - 1)(T')$  is divisible by  $p$  in  $A(F)$ . Then we can take  $Q$  such that  $p\sigma^{(p+1)/2}(Q) = Q'$  to be the point predicted by Proposition 5.7. In our concrete case this works with  $(a, b) = (4, 3)$ . It can be shown that  $A(F) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}[G]Q$  as a  $\mathbb{Z}[G]$ -module.

Using modular symbols and Heegner points, we can provably compute that

$$\hat{Q}_1 = \frac{1}{4} \quad \text{and} \quad \hat{Q}_\epsilon = \frac{1}{2}$$

and hence deduce that BSD holds for  $A/\mathbb{Q}$  and  $A/K$  with trivial Tate-Shafarevich groups in both cases. We compute to a high precision the derivatives of  $L(A, \psi, s)$  for the representations  $\psi = \psi_1$  and  $\psi_2$  of dimension two and we find, with an error less than  $10^{-28}$ , that  $\hat{Q}_{\psi_1} \cdot \hat{Q}_{\psi_2} \approx 256$ , predicting that  $|\text{III}(A_L)| = 4$  and  $\hat{Q}_{\psi_1} + \hat{Q}_{\psi_2} \approx 48$ . It also predicts that  $\text{III}(A_F)$  has order 32. We will now assume that these are actually equalities and conclude that  $\hat{Q}_{\psi_i} = 8 \cdot (3 \pm \sqrt{5})$ . One then computes the  $S_r$ -truncated values to be

$$Q_1 = \frac{8}{19}, \quad Q_\epsilon = \frac{24}{19} \quad \text{and} \quad Q_{\psi_1} + Q_{\psi_2} = -96$$

and this shows that the congruence (20) holds modulo  $p = 5$ .

## REFERENCES

1. A. Agashe, K. Ribet, and W. A. Stein, *The Manin constant*, Pure Appl. Math. Q. **2** (2006), no. 2, part 2, 617–636.
2. M. F. Atiyah and C. T. C. Wall, *Cohomology of groups*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 94–115.
3. W. Bley, *Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture*, Exp. Math. **20** (2011), no. 4, 426–456.
4. ———, *Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture (Part II)*, Math. Comp. **81** (2012), 1681–1705.
5. ———, *The equivariant Tamagawa number conjecture and modular symbols*, to appear in Math. Ann., 2013.
6. W. Bley and D. Burns, *Equivariant epsilon constants, discriminants and étale cohomology*, Proc. London Math. Soc. (3) **87** (2003), no. 3, 545–590.
7. W. Bley and D. Macias Castillo, *Congruences for critical values of higher derivatives of twisted Hasse-Weil L-functions*, to appear in J. reine u. angew. Math., 2015.
8. 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.
9. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).
10. M. Breuning, *On equivariant global epsilon constants for certain dihedral extensions*, Math. Comp. **73** (2004), no. 246, 881–898.
11. M. Breuning and D. Burns, *Additivity of Euler characteristics in relative algebraic K-groups*, Homology, Homotopy Appl. **7** (2005), no. 3, 11–36.
12. K. S. Brown, *Cohomology of groups*, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York, 1982.
13. D. Burns, *Equivariant Whitehead torsion and refined Euler characteristics*, Number theory, CRM Proc. Lecture Notes, vol. 36, Amer. Math. Soc., Providence, RI, 2004, pp. 35–59.

14. ———, *On leading terms and values of equivariant motivic  $L$ -functions*, Pure Appl. Math. Q. **6** (2010), no. 1, Special Issue: In honor of John Tate. Part 2, 83–172.
15. D. Burns and M. Flach, *Motivic  $L$ -functions and Galois module structures*, Math. Ann. **305** (1996), no. 1, 65–102.
16. ———, *Tamagawa numbers for motives with (non-commutative) coefficients*, Doc. Math. **6** (2001), 501–570.
17. D. Burns and D. Macias Castillo, *Organising matrices for arithmetic complexes*, to appear in Int. Math. Res. Not., 2013.
18. D. Burns, D. Macias Castillo, and C. Wuthrich, *On the Galois structure of Selmer groups*, to appear in Int. Math. Res. Not., 2015.
19. D. Burns and O. Venjakob, *On descent theory and main conjectures in non-commutative Iwasawa theory*, J. Inst. Math. Jussieu **10** (2011), 59–118.
20. J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.
21. J. E. Cremona, M. Prickett, and S. Siksek, *Height difference bounds for elliptic curves over number fields*, J. Number Theory **116** (2006), no. 1, 42–68.
22. C. W. Curtis and I. Reiner, *Methods of representation theory. Vol. I*, Wiley Classics Library, John Wiley & Sons Inc., New York, 1990, With applications to finite groups and orders, Reprint of the 1981 original, A Wiley-Interscience Publication.
23. H. Darmon and R. Pollack, *Efficient calculation of Stark-Heegner points via overconvergent modular symbols*, Israel J. Math. **153** (2006), 319–354.
24. P. Deligne, *Le déterminant de la cohomologie*, Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), Contemp. Math., vol. 67, Amer. Math. Soc., Providence, RI, 1987, pp. 93–177.
25. T. Dokchitser, *Computing special values of motivic  $L$ -functions*, Experiment. Math. **13** (2004), no. 2, 137–149.
26. T. Dokchitser and V. Dokchitser, *Computations in non-commutative Iwasawa theory*, Proc. Lond. Math. Soc. (3) **94** (2007), no. 1, 211–272, With an appendix by J. Coates and R. Sujatha.
27. A. W. M. Dress, *Induction and structure theorems for orthogonal representations of finite groups*, Ann. of Math. (2) **102** (1975), no. 2, 291–325.
28. J.-M. Fontaine and W. Messing,  *$p$ -adic periods and  $p$ -adic étale cohomology*, Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), Contemp. Math., vol. 67, Amer. Math. Soc., Providence, RI, 1987, pp. 179–207.
29. A. Fröhlich and J. Queyrut, *On the functional equation of the Artin  $L$ -function for characters of real representations*, Invent. Math. **20** (1973), 125–138.
30. B. H. Gross, *On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication*, Number theory related to Fermat’s last theorem (Cambridge, Mass., 1981), Progr. Math., vol. 26, Birkhäuser Boston, Mass., 1982, pp. 219–236.
31. ———, *Kolyvagin’s work on modular elliptic curves,  $L$ -functions and arithmetic* (Durham, 1989), London Math. Soc. Lecture Note Ser., vol. 153, Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.
32. B. H. Gross and D. B. Zagier, *Heegner points and derivatives of  $L$ -series*, Invent. Math. **84** (1986), no. 2, 225–320.
33. H. Jacobinski, *On extensions of lattices*, Michigan Math. J. **13** (1966), 471–475.
34. H. Johnston and A. Nickel, *Noncommutative Fitting invariants and improved annihilation results*, to appear in J. London Math. Soc., 2013.
35. G. Kings, *The equivariant Tamagawa number conjecture and the Birch-Swinnerton-Dyer conjecture*, Arithmetic of  $L$ -functions, IAS/Park City Math. Ser., vol. 18, Amer. Math. Soc., Providence, RI, 2011, pp. 315–349.
36. S. R. Louboutin, *On the divisibility of the class number of imaginary quadratic number fields*, Proc. Amer. Math. Soc. **137** (2009), no. 12, 4025–4028.
37. J. Martinet, *Character theory and Artin  $L$ -functions*, Algebraic number fields:  $L$ -functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 1–87.
38. B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266.
39. B. Mazur and K. Rubin, *Organizing the arithmetic of elliptic curves*, Adv. Math. **198** (2005), no. 2, 504–546.
40. ———, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), no. 2, 579–612.
41. A. Nickel, *Non-commutative Fitting invariants and annihilation of class groups*, J. Algebra **323** (2010), no. 10, 2756–2778.
42. W. Nizioł, *Cohomology of crystalline representations*, Duke Math. J. **71** (1993), no. 3, 747–791.
43. R. Oliver, *Whitehead groups of finite groups*, London Mathematical Society Lecture Note Series, vol. 132, Cambridge University Press, Cambridge, 1988.

44. A. Parker, *Equivariant Tamagawa numbers and non-commutative Fitting invariants*, Ph.D. thesis, King's College London, 2007, available at [http://www.mth.kcl.ac.uk/staff/dj\\_burns/former\\_students/andy\\_parker/ThesisAndrewParker.pdf](http://www.mth.kcl.ac.uk/staff/dj_burns/former_students/andy_parker/ThesisAndrewParker.pdf).
45. J.-P. Serre, *Corps locaux*, Hermann, Paris, 1968, Deuxième édition, Publications de l'Université de Nancago, No. VIII.
46. ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.
47. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.
48. W. A. Stein et al., *Sage Mathematics Software (Version 5.0)*, The Sage Development Team, 2011, <http://www.sagemath.org>.
49. The PARI Group, Bordeaux, *PARI/GP, version 2.5.0*, 2011, available from <http://pari.math.u-bordeaux.fr/>.
50. O. Venjakob, *From the Birch and Swinnerton-Dyer conjecture to non-commutative Iwasawa theory via the equivariant Tamagawa number conjecture—a survey*, *L-functions and Galois representations*, London Math. Soc. Lecture Note Ser., vol. 320, Cambridge Univ. Press, Cambridge, 2007, pp. 333–380.

KING'S COLLEGE LONDON, DEPARTMENT OF MATHEMATICS, LONDON WC2R 2LS, U.K.  
*E-mail address:*  `david.burns@kcl.ac.uk`

INSTITUTO DE CIENCIAS MATEMÁTICAS (ICMAT), 28049 MADRID, SPAIN.  
*E-mail address:*  `daniel.macias@icmat.es`

SCHOOL OF MATH. SCIENCES, UNIVERSITY OF NOTTINGHAM, NOTTINGHAM NG7 2RD, U.K.  
*E-mail address:*  `christian.wuthrich@nottingham.ac.uk`