THE ℓ-PARITY CONJECTURE OVER THE CONSTANT QUADRATIC EXTENSION

KĘSTUTIS ČESNAVIČIUS

Abstract. For a prime ℓ and an abelian variety A over a global field K, the ℓ-parity conjecture predicts that, in accordance with the ideas of Birch and Swinnerton-Dyer, the $\mathbb{Z}_\ell$-corank of the ℓ^∞-Selmer group and the analytic rank agree modulo 2. Assuming that $\operatorname{char} K > 0$, we prove that the ℓ-parity conjecture holds for the base change of A to the constant quadratic extension if ℓ is odd, coprime to $\operatorname{char} K$, and does not divide the degree of every polarization of A. The techniques involved in the proof include the étale cohomological interpretation of Selmer groups, the Grothendieck–Ogg–Shafarevich formula, and the study of the behavior of local root numbers in unramified extensions.

1. Introduction

1.1. The ℓ-parity conjecture. The Birch and Swinnerton-Dyer conjecture (BSD) predicts that the completed L-function $L(A, s)$ of an abelian variety A over a global field K extends meromorphically to the whole complex plane, vanishes to the order $\operatorname{rk} A$ at $s = 1$, and satisfies the functional equation

$$L(A, 2 - s) = w(A)L(A, s), \tag{1.1.1}$$

where $\operatorname{rk} A$ and $w(A)$ are the Mordell–Weil rank and the global root number of A. The vanishing assertion combines with (1.1.1) to give "BSD modulo 2," namely, the parity conjecture:

$$(-1)^{\operatorname{rk} A} \overset{?}{=} w(A).$$

Selmer groups tend to be easier to study than Mordell–Weil groups, so, fixing a prime ℓ, one sets

$$\operatorname{rk}_\ell A := \dim_{\mathbb{Q}_\ell} \operatorname{Hom}(\operatorname{Sel}_{\ell^\infty} A, \mathbb{Q}_\ell/\mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell,$$

where

$$\operatorname{Sel}_{\ell^\infty} A := \varinjlim \operatorname{Sel}_{\ell^n} A$$

is the ℓ^∞-Selmer group, notes that the conjectured finiteness of the Shafarevich–Tate group Ш(A) implies $\operatorname{rk}_\ell A = \operatorname{rk} A$, and instead of the parity conjecture considers the ℓ-parity conjecture:

$$(-1)^{\operatorname{rk}_\ell A} \overset{?}{=} w(A). \tag{1.1.2}$$

1.2. The status of the number field case. Over a number field K, in the elliptic curve case, the ℓ-parity conjecture was proved for $K = \mathbb{Q}$ in [DD10, Thm. 1.4] (see [Mon96], [Nek06, §0.17], [Kim07] for some preceding work), for totally real K excluding some cases of potential complex multiplication with $\ell = 2$ in [Nek13, Thm. A], [Nek15, 5.12], and [Nek16, Thm. E], and for curves with an ℓ-isogeny over a general K in [Čes16c, Thm. 1.4] (building on [DD08, Thm. 2], [DD11, Cor. 5.8],

---

Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
E-mail address: kestutis@berkeley.edu.
Date: June 21, 2017.
2010 *Mathematics Subject Classification.* Primary 11G10; Secondary 11G40, 11R58.
Key words and phrases. Parity conjecture, root number, arithmetic duality.

and [CFKS10, proof of Thm. 2.1]). The higher dimensional case in the presence of a suitable isogeny was addressed in [CFKS10, Thm. 2.1].

1.3. The status of the function field case. Over a global field K of positive characteristic p, the elliptic curve case of the p-parity conjecture was proved in [TW11, Thm. 1] under the assumption that $p > 3$. The function field case of the ℓ-parity conjecture was subsequently settled in full in [TY14, Thm. 1.1] (including the case $\ell = p$).

The main goal of this paper is to present another approach to the ℓ-parity conjecture in the positive characteristic case. Even though our techniques only reprove the special case stated in Theorem 1.4, they lead to intermediate results that have already been useful in other contexts—for instance, in the proof of the Kramer–Tunnell formula for certain classes of hyperelliptic Jacobians presented in the PhD thesis [Mor15] of Adam Morgan.

Theorem 1.4 (Theorem 7.1)**.** *Let K be a global field of positive characteristic, let $\mathbb{F}_q$ be its field of constants, let $\ell \nmid q$ be a prime, and let A be an abelian variety over K. Suppose that A has a polarization of degree prime to ℓ (e.g., a principal polarization) and, if $\ell = 2$, that the orders of the component groups of the reductions of $A_{K\overline{\mathbb{F}}_q}$ are odd. Then the ℓ-parity conjecture holds for $A_{K\mathbb{F}_{q^2}}$.*

Remark 1.5. Remark 6.7 isolates the difficulty in removing the additional component group condition in the case $\ell = 2$.

One of the key inputs to the proof of Theorem 1.4 is the following purely local result that allows us to control the root numbers over an unramified quadratic extension.

Theorem 1.6 (Corollary 4.6)**.** *For an abelian variety B over a nonarchimedean local field k, let B_{k_n} and $a(B)$ be its base change to a degree n unramified extension and conductor exponent, respectively. The local root number satisfies*

$$w(B_{k_n}) = \begin{cases} w(B), & \text{if } n \text{ is odd,} \\ (-1)^{a(B)}, & \text{if } n \text{ is even.} \end{cases}$$

Theorem 1.6 leads to the following extension of a theorem of Kisilevsky, [Kis04, Thm. 1], who treated the case when $K = \mathbb{Q}$ and B and B' are elliptic curves.

Theorem 1.7. *Let B and B' be abelian varieties over a global field K. If $w(B_L) = w(B'_L)$ for every separable quadratic extension L/K, then the conductor ideals of B and B' are equal up to square factors.*

Proof. Let Σ be the set of those finite places of K at which B or B' has bad reduction. For a $v \in \Sigma$, let L/K be a separable quadratic extension that is inert at v, split at every $v' \in \Sigma$ with $v' \neq v$, and split at every infinite place. For such an L we have

$$w(B_L) = w(B_{L_v}) \qquad \text{and} \qquad w(B'_L) = w(B'_{L_v}),$$

so Theorem 1.6 and the $w(B_L) = w(B'_L)$ assumption show that up to squares the conductor ideals of B and B' have the same factor at v. ☐

1.8. An overview of the proof of Theorem 1.4. The main idea of the proof is to interpret the ℓ-Selmer group as an étale cohomology group following [Čes16b], to use the Grothendieck–Ogg–Shafarevich formula together with the Hochschild–Serre spectral sequence to express the ℓ-Selmer parity as a sum of local terms, and then to compare place by place with the expression of the global root number as the product of local root numbers. The argument is carried out in §7 and rests on the following additional inputs:

- Due to possibly nontrivial Galois action, the Hochschild–Serre spectral sequence relates the étale cohomological ℓ-Selmer group to the Grothendieck–Ogg–Shafarevich formula only after a large constant extension. In order to descend the ℓ-parity conclusion to $K\mathbb{F}_{q^2}$, we use the self-duality of Galois representations furnished by ℓ^∞-Selmer groups. This self-duality is the subject of §2.
- For the main idea to be relevant, in §3 we implicitly recast the ℓ-parity conjecture in terms of ℓ-Selmer rather than ℓ^∞-Selmer groups. Special care is needed if $\ell = 2$, since Shafarevich–Tate groups need not be of square order even when they are finite and A is principally polarized. This is one of the places of the overall argument where the polarization assumption of Theorem 1.4 comes in (the polarization is also used in §§6–7 to get an isomorphism $A[l] \simeq A^\vee[l]$ and to apply suitable results from [PR12]).
- The comparison of the Grothendieck–Ogg–Shafarevich local terms and root numbers is possible due to Theorem 1.6, which, along with related local results, is treated in §4.
- In the presence of local Tamagawa factors that are divisible by ℓ, the ℓ-Selmer group may differ from its étale cohomological counterpart. Arithmetic duality results proved in §§5–6 control this difference modulo 2 through Theorem 6.6. The $\ell = 2$ case again leads to complications due to the difference between alternating and skew-symmetric pairings in characteristic 2.

1.9. Notation. For a field F, an algebraic (resp., separable) closure is denoted by $\overline{F}$ (resp., by F^s); when needed (e.g., for forming composita), the choice of $\overline{F}$ is made implicitly and compatibly with overfields. If F is a global field and v is its place, then F_v denotes the corresponding completion; if v is finite, then $\mathcal{O}_v$ and $\mathbb{F}_v$ denote the ring of integers and the residue field of F_v. For a prime ℓ and a torsion abelian group G, we denote by $G[\ell^\infty]$ (resp., by G_{nd}) the subgroup consisting of all the elements of ℓ-power order (resp., the quotient by the maximal divisible subgroup). In the case when $G = G[\ell^\infty]$, we say that G is *$\mathbb{Z}_\ell$-cofinite* if $\mathrm{Hom}(G, \mathbb{Q}_\ell/\mathbb{Z}_\ell)$ is finitely generated as a $\mathbb{Z}_\ell$-module. For a prime ℓ and an abelian variety B over a global field, the notation $\mathrm{rk}\, B$, $w(B)$, $\mathrm{rk}_\ell\, B$, $\mathrm{Sel}_{\ell^\infty} B$, $Ш(B)$ introduced in §1.1 remains in place throughout the paper. If B is an abelian variety over a local field, then $w(B)$ denotes the *local* root number instead. The dual abelian variety is denoted by $B^\vee$. All the representations that we consider are finite dimensional.

Acknowledgements. I thank the referee for a careful reading of the manuscript and for very helpful comments. I thank Tim Dokchitser, Vladimir Dokchitser, Adam Morgan, Bjorn Poonen, Padmavathi Srinivasan, Fabien Trihan, and Christian Wuthrich for helpful conversations or correspondence.

2. Self-duality of ℓ^∞-Selmer groups

Let F/K be a finite Galois extension of global fields, let ℓ be a prime number, and let A be an abelian variety over K. The goal of this section is to prove in Theorem 2.2 that if $\ell \neq \mathrm{char}\, K$, then the finite-dimensional $\mathbb{Q}_\ell$-representation

$$\mathcal{X}_\ell(A) := \mathrm{Hom}(\mathrm{Sel}_{\ell^\infty} A, \mathbb{Q}_\ell/\mathbb{Z}_\ell) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$$

of $\mathrm{Gal}(F/K)$ is isomorphic to its dual and to deduce in Corollary 2.5 that if, in addition, the degree of F/K is odd, then the ℓ-parity conjecture holds for A if and only if it holds for A_F. The self-duality is expected: if $Ш(A_F)[\ell^\infty]$ is finite as is conjectured, then $\mathcal{X}_\ell(A)$ is $\mathrm{Gal}(F/K)$-isomorphic to $A(F) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell$, which is self-dual. The utility of Theorem 2.2 lies in bypassing assumptions on Ш.

In the number field case, proofs of these results were given by T. and V. Dokchitser, see [DD09a, Prop. A.2] for a summary. In general, their arguments require only mild modifications and are explained in the proof of Theorem 2.2 below. In [TW11, proof of Prop. 4], Trihan and Wuthrich have also observed that extensions of the sort presented here are possible, but it seems worthwhile to indicate the necessary changes to the proofs.

A key input to the proof of the promised self-duality of ℓ^∞-Selmer groups is the following lemma, whose proof is based on the Selmer group analogue of the isogeny invariance of BSD quotients.

Lemma 2.1. *Let $\phi\colon X \to Y$ be an isogeny between abelian varieties over a global field K and set*

$$Q(\phi) := \prod_{\ell \mid \deg \phi} \#\,\mathrm{Coker}\left(\frac{\mathrm{Hom}(\mathrm{Sel}_{\ell^\infty} Y, \mathbb{Q}_\ell/\mathbb{Z}_\ell)}{\mathrm{Hom}(\mathrm{Sel}_{\ell^\infty} Y, \mathbb{Q}_\ell/\mathbb{Z}_\ell)_{\mathrm{tors}}} \xrightarrow{\phi^*} \frac{\mathrm{Hom}(\mathrm{Sel}_{\ell^\infty} X, \mathbb{Q}_\ell/\mathbb{Z}_\ell)}{\mathrm{Hom}(\mathrm{Sel}_{\ell^\infty} X, \mathbb{Q}_\ell/\mathbb{Z}_\ell)_{\mathrm{tors}}} \right),$$

and likewise for $Q(\phi^\vee)$. If $X = Y$ and $\deg \phi$ is prime to $\mathrm{char}\, K$, then $Q(\phi) = Q(\phi^\vee)$.

Proof. The proof of the number field case [DD10, Thm. 4.3] continues to work (as in *loc. cit.*, one bases the argument on [Mil06, I.(7.3.1)]). □

Theorem 2.2. *For a finite Galois extension F/K of global fields, a prime $\ell \neq \mathrm{char}\, K$, and an abelian variety A over K, the $\mathbb{Q}_\ell$-representation $\mathcal{X}_\ell(A_F)$ of $G := \mathrm{Gal}(F/K)$ is self-dual.*

Proof. We model the argument on the proof, given by T. and V. Dokchitser in [DD09b, Thm. 2.1], of the corresponding statement in the number field case. To begin with, since A and $A^\vee$ are isogenous, $\mathcal{X}_\ell(A_F) \simeq \mathcal{X}_\ell(A_F^\vee)$ as $\mathbb{Q}_\ell[G]$-modules, so the Zarhin trick allows us to assume that A is principally polarized.

We will apply Lemma 2.1 with $X = Y = \mathrm{Res}_{F/K}(A_F)$, which, due to the functoriality of the restriction of scalars $\mathrm{Res}_{F/K}$, comes equipped with a G-action. By the proof of [DD09b, Lemma 2.4] (originally given in the number field case), there is an isomorphism

$$\mathcal{X}_\ell(\mathrm{Res}_{F/K}(A_F)) \cong \mathcal{X}_\ell(A_F) \qquad \text{compatible with the } G\text{-action},$$

so it suffices to show that for every irreducible $\mathbb{Q}_\ell$-representation τ of G, the multiplicities of τ and τ^* in $\mathcal{X}_\ell(\mathrm{Res}_{F/K}(A_F))$ are equal. For this, we now suitably modify the proof of [DD09b, Thm. 2.3]. Letting d_τ denote the dimension of any irreducible constituent of $\tau \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$, we consider

$$P_\tau := d_\tau \cdot \textstyle\sum_{g \in G} \mathrm{Tr}(\tau(g)) g \in \mathbb{Z}_\ell[G].$$

By the contravariance of $\mathcal{X}_\ell(-)$ and by [Ser77, §2.6 Thm. 8 (ii) and §12.2], the operator P_τ kills every irreducible G-constituent $\tau' \not\simeq \tau$ of $\mathcal{X}_\ell(\mathrm{Res}_{F/K}(A_F))$ and acts as scaling by $m_\tau \cdot \#G$ on every copy of τ, where $m_\tau \in \mathbb{Z}_{>0}$ denotes the Schur index of τ. Therefore, there exists a small ℓ-adic neighborhood

$$U_\tau \quad \text{of} \quad m_\tau \cdot \#G \cdot 1_G + (p-1)P_\tau \quad \text{in} \quad \mathbb{Z}_\ell[G]$$

such that for any G-stable $\mathbb{Z}_\ell$-lattice $\Lambda_{\tau'}$ in an irreducible G-subrepresentation $\tau' \subset \mathcal{X}_\ell(\mathrm{Res}_{F/K}(A_F))$ with $\tau' \not\simeq \tau$ (resp., with $\tau' \simeq \tau$), any $x \in U_\tau$ acts as the $m_\tau \cdot \#G$-multiple (resp., as the $\ell \cdot m_\tau \cdot \#G$-multiple) of a $\mathbb{Z}_\ell$-automorphism of $\Lambda_{\tau'}$. Since, moreover, the $\mathbb{Z}_\ell$-linear automorphism ι of $\mathbb{Z}_\ell[G]$ determined by $\iota(g) = g^{-1}$ carries P_τ to P_{τ^*} and is continuous, we may find an element

$$\Phi_\tau = \textstyle\sum_{g \in G} x_{\tau, g} \cdot g \in \mathbb{Z}[G] \qquad \text{such that} \qquad \Phi_\tau \in U_\tau \quad \text{and} \quad \iota(\Phi_\tau) \in U_{\tau^*}.$$

Thanks to the $\ell \neq \mathrm{char}\, K$ assumption we may assume, in addition, that the determinant of the $\mathbb{Z}$-linear multiplication by Φ_τ endomorphism of $\mathbb{Z}[G]$ is prime to $\mathrm{char}\, K$. Then the endomorphism ϕ_τ of $\mathrm{Res}_{F/K}(A_F)$ determined by Φ_τ is an isogeny of degree prime to $\mathrm{char}\, K$, so Lemma 2.1 gives the equality

$$Q(\phi_\tau) = Q(\phi_\tau^\vee).$$

Under a principal polarization, $\phi_\tau^\vee$ is identified with the endomorphism of $\mathrm{Res}_{F/K}(A_F)$ determined by $\iota(\Phi_\tau)$. Therefore, letting $\mathrm{mult}(\tau, V)$ denote the multiplicity of the irreducible $\mathbb{Q}_\ell$-representation τ of G in a $\mathbb{Q}_\ell$-representation V of G (and likewise for τ^*), we conclude from the construction of Φ_τ that

$$\mathrm{ord}_\ell(Q(\phi_\tau)) = \mathrm{ord}_\ell(m_\tau \cdot \#G) \cdot \dim_{\mathbb{Q}_\ell} \mathcal{X}_\ell(\mathrm{Res}_{F/K}(A_F)) + \mathrm{mult}(\tau, \mathcal{X}_\ell(\mathrm{Res}_{F/K}(A_F))) \cdot \dim_{\mathbb{Q}_\ell} \tau,$$
$$\mathrm{ord}_\ell(Q(\phi_\tau^\vee)) = \mathrm{ord}_\ell(m_{\tau^*} \cdot \#G) \cdot \dim_{\mathbb{Q}_\ell} \mathcal{X}_\ell(\mathrm{Res}_{F/K}(A_F)) + \mathrm{mult}(\tau^*, \mathcal{X}_\ell(\mathrm{Res}_{F/K}(A_F))) \cdot \dim_{\mathbb{Q}_\ell} \tau^*.$$

Since $m_\tau = m_{\tau^*}$ and $\dim_{\mathbb{Q}_\ell} \tau = \dim_{\mathbb{Q}_\ell} \tau^*$, we obtain the desired equality

$$\mathrm{mult}(\tau, \mathcal{X}_\ell(\mathrm{Res}_{F/K}(A_F))) = \mathrm{mult}(\tau^*, \mathcal{X}_\ell(\mathrm{Res}_{F/K}(A_F))).$$ □

Remark 2.3. It is desirable to remove the assumption $\ell \neq \mathrm{char}\, K$ in Theorem 2.2. For this, the crux of the matter is to remove the degree restriction in Lemma 2.1.

With Theorem 2.2 in hand, we proceed to Corollary 2.5, whose proof will use the following lemma:

Lemma 2.4. *For a finite Galois extension F/K of global fields, a prime ℓ, and an abelian variety A over K, the map $\mathcal{X}_\ell(A_F) \to \mathcal{X}_\ell(A)$ induced by restriction to F supplies the second isomorphism in*

$$\mathcal{X}_\ell(A_F)^G \cong \mathcal{X}_\ell(A_F)_G \cong \mathcal{X}_\ell(A), \qquad \text{where } G := \mathrm{Gal}(F/K).$$

Proof. The proof for elliptic curves and number fields, [DD10, proof of Lemma 4.14], extends: the spectral sequence

$$H^i(G, H^j_{\mathrm{fppf}}(F, A[\ell^\infty])) \Rightarrow H^{i+j}_{\mathrm{fppf}}(K, A[\ell^\infty])$$

shows that $\#G$ kills the kernel and the cokernel of the map

$$H^1_{\mathrm{fppf}}(K, A[\ell^\infty]) \to H^1_{\mathrm{fppf}}(F, A[\ell^\infty])^G.$$

Thus, $\#G$ also kills the kernel of the map

$$\mathrm{Sel}_{\ell^\infty} A \to (\mathrm{Sel}_{\ell^\infty} A_F)^G. \tag{2.4.1}$$

Moreover, $\#G$ kills $\mathrm{Ker}(H^1(K_v, A) \to H^1(F_w, A))$ for all places w of F that extend a place v of K, so $(\#G)^2$ kills the cokernel of the map (2.4.1). In order to obtain the claim, it remains to pass to Pontryagin duals and to invert ℓ. □

Corollary 2.5. *For an odd degree Galois extension F/K of global fields, an abelian variety A over K, and a prime ℓ different from* char K*, one has*

(a) $\mathrm{rk}_\ell\, A \equiv \mathrm{rk}_\ell\, A_F \bmod 2$ *and*

(b) $w(A) = w(A_F)$.

In particular, the ℓ-parity conjecture holds for A if and only if it holds for A_F.

Proof.

(a) Combine the argument of [DD09b, Cor. 2.5] with Theorem 2.2 and Lemma 2.4.

(b) The number field proof [DD09a, A.2 (3)] also works for global fields. □

3. Replacing ℓ^∞-Selmer groups by ℓ-Selmer groups

To facilitate the Grothendieck–Ogg–Shafarevich input to our proof of Theorem 1.4, in Corollary 3.5 we (implicitly) reformulate the ℓ-parity conjecture by relating the ℓ^∞-Selmer rank and the ℓ-Selmer rank. A suitable polarization is handy for this—without it, controlling the parity of $\dim_{\mathbb{F}_\ell}(\text{Ш}(A)_{\text{nd}}[\ell])$ would become a major concern. In fact, even with it, this parity may vary in the $\ell = 2$ case, as Poonen and Stoll explain in [PS99]. As far as the proof of Theorem 1.4 is concerned, the goal of Theorem 3.2 and Lemma 3.4 below is to overcome this difficulty by proving that the said parity is even over every quadratic extension. Theorem 3.2 is a slight improvement to the main result of *op. cit.*—without this improvement, in the $\ell = 2$ case of Theorem 1.4 we would be forced to restrict to principally polarized abelian varieties, which were the main focus of Poonen and Stoll.

3.1. The Cassels–Tate pairing. For an abelian variety B over a global field F, let

$$\langle\ ,\ \rangle\colon \text{Ш}(B) \times \text{Ш}(B^\vee) \to \mathbb{Q}/\mathbb{Z}$$

be the Cassels–Tate bilinear pairing. For a self-dual homomorphism $\lambda\colon B \to B^\vee$, the pairing

$$\langle a, b\rangle_\lambda := \langle a, \lambda(b)\rangle \quad \text{for} \quad a, b \in \text{Ш}(B)$$

is antisymmetric [PS99, §6, Cor. 6]. Therefore, if λ is in addition an isogeny, then, for every prime $p \nmid 2\deg\lambda$, the pairing induced by $\langle\ ,\ \rangle_\lambda$ on the abelian group $\text{Ш}(B)[p^\infty]$ is alternating. In this case, since $\langle\ ,\ \rangle$ is nondegenerate modulo the divisible subgroups,[1] for every prime $p \nmid 2\deg\lambda$ we have

$$\dim_{\mathbb{F}_p}(\text{Ш}(B)_{\text{nd}}[p]) \equiv 0 \bmod 2.$$

For a self-dual homomorphism $\lambda\colon B \to B^\vee$, as in [PS99, §4, Cor. 2], we let

$$c_\lambda \in \text{Ш}(B^\vee)[2] \subset H^1(k, B^\vee)[2] \qquad \text{be the image of} \qquad \lambda \in (\text{NS}\, B)(F).$$

In addition, for a self-dual isogeny $\lambda\colon B \to B^\vee$ of odd degree, we let

$$\text{Ш}(\lambda)[2]\colon \text{Ш}(B)[2] \xrightarrow{\sim} \text{Ш}(B^\vee)[2]$$

be the induced isomorphism and set

$$c := (\text{Ш}(\lambda)[2])^{-1}(c_\lambda) \in \text{Ш}(B)[2].$$

For such λ,

$$\dim_{\mathbb{F}_2}(\text{Ш}(B)_{\text{nd}}[2]) \mod 2 \qquad \text{is governed by} \qquad \langle c, c\rangle_\lambda \in \{0, \tfrac{1}{2}\};$$

indeed, Poonen and Stoll observed this in [PS99, §6, Thm. 8] in the case when λ is a principal polarization, and the general case follows from their argument:

Theorem 3.2. *Let $\lambda\colon B \to B^\vee$ be a self-dual isogeny of odd degree d.*

(a) *If $\langle c, c\rangle_\lambda = 0$, then $\#\text{Ш}(B)_{\text{nd}}[n]$ is a perfect square for every $n \in \mathbb{Z}_{\geqslant 1}$ prime to d.*

(b) *If $\langle c, c\rangle_\lambda = \frac{1}{2}$, then $\#\text{Ш}(B)_{\text{nd}}[n]$ is twice a perfect square for every even $n \in \mathbb{Z}_{\geqslant 1}$ prime to d and is a perfect square for every odd $n \in \mathbb{Z}_{\geqslant 1}$ prime to d.*

Proof. The proof of [PS99, §6, Thm. 8] given for the case $d = 1$ continues to work if throughout that proof one replaces Ш_{nd} by its subgroup $\text{Ш}_{\text{nd}}(d')$ consisting of the elements of order prime to d. ☐

[1] The first published complete proof of the fact that the left and the right kernels of $\langle\ ,\ \rangle$ are the maximal divisible subgroups of $\text{Ш}(B)$ and $\text{Ш}(B^\vee)$, respectively, seems to be the combination of [HS05, Thm. 0.2], [HS05e], and [GA09, Thm. 1.2] (although *op. cit.* does not treat the prime to the characteristic torsion subgroups, its MathSciNet review remarks that the corresponding claim for such subgroups follows from the proof of [HS05, Thm. 0.2]).

Remark 3.3. Under the assumptions of Theorem 3.2, the replacement indicated in the proof also gives the following extension of [PS99, §6, Cor. 9]: if $Ш(B)_{\mathrm{nd}}$ is finite, then there exists a finite abelian group T such that, letting $(-)(d')$ denote the "prime to d" subgroup,

$$\begin{array}{llll} \text{in the case} & \langle c, c\rangle_\lambda = 0, & \text{one has} & Ш(B)_{\mathrm{nd}}(d') \simeq T \times T; \\ \text{in the case} & \langle c, c\rangle_\lambda = \frac{1}{2}, & \text{one has} & Ш(B)_{\mathrm{nd}}(d') \simeq \mathbb{Z}/2\mathbb{Z} \times T \times T. \end{array}$$

Due to Lemma 3.4 below, the obstruction $\langle c, c\rangle_\lambda$ vanishes over an even degree extension. Lemma 3.4 was pointed out to us by Bjorn Poonen and was also observed by Adam Morgan.

Lemma 3.4. *For a finite extension F'/F of global fields, there is a commutative diagram*

$$\begin{array}{ccc} Ш(B) \times Ш(B^\vee) & \xrightarrow{\langle\,,\rangle} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{Res}} & & \downarrow{\scriptstyle [F':F]} \\ Ш(B_{F'}) \times Ш(B^\vee_{F'}) & \xrightarrow{\langle\,,\rangle} & \mathbb{Q}/\mathbb{Z}. \end{array}$$

Proof. Combine the definition [PS99, §3.1] of the pairings with the well-known commutativity of the diagram

$$\begin{array}{ccc} \mathrm{Br}(F_v) & \xrightarrow{\mathrm{inv}_v} & \mathbb{Q}/\mathbb{Z} \\ {\scriptstyle \mathrm{Res}}\downarrow & & \downarrow{\scriptstyle [F'_{v'}:F_v]} \\ \mathrm{Br}(F'_{v'}) & \xrightarrow{\mathrm{inv}_{v'}} & \mathbb{Q}/\mathbb{Z} \end{array}$$

for a finite extension $F'_{v'}/F_v$ of local fields (for the commutativity, see [Ser67, §1.1, Thm. 3]). ☐

We are ready to reduce to working with ℓ-Selmer groups instead of ℓ^∞-Selmer groups in Theorem 1.4.

Corollary 3.5. *For a prime ℓ, if an abelian variety B over a global field F has a polarization of degree prime to ℓ, then for every quadratic extension F'/F one has*

$$\mathrm{rk}_\ell\, B_{F'} \equiv \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell\, B_{F'} - \dim_{\mathbb{F}_\ell} B[\ell](F') \bmod 2.$$

Proof. For any prime ℓ and any abelian variety A over a global field K one has

$$\mathrm{rk}_\ell\, A = \mathrm{rk}\, A + \dim_{\mathbb{F}_\ell} Ш(A)[\ell] - \dim_{\mathbb{F}_\ell} Ш(A)_{\mathrm{nd}}[\ell] = \dim_{\mathbb{F}_\ell} \mathrm{Sel}_\ell\, A - \dim_{\mathbb{F}_\ell} A[\ell](K) - \dim_{\mathbb{F}_\ell} Ш(A)_{\mathrm{nd}}[\ell].$$

Moreover, for $A = B_{F'}$, the dimension $\dim_{\mathbb{F}_\ell} Ш(B_{F'})_{\mathrm{nd}}[\ell]$ is even by Theorem 3.2 (a) and Lemma 3.4. The desired congruence follows. ☐

Remark 3.6. Even though the proof continues to work, no generality is gained by requiring a self-dual isogeny instead of a polarization in Corollary 3.5 (or Theorem 1.4): for an $n \in \mathbb{Z}_{>0}$, if an abelian variety B over a field F has a self-dual isogeny of degree prime to n, then it also has a polarization of degree prime to n. Indeed, one knows that the degree function[2] $\deg\colon (\mathrm{NS}\, B)(F) \to \mathbb{Z}$ is a polynomial with rational coefficients on the lattice $(\mathrm{NS}\, B)(F)$; consequently, deg modulo n is translation invariant with respect to a sublattice, and it remains to note that the cone of polarizations spans $(\mathrm{NS}\, B)(F)$.

[2] The degree of a self-dual homomorphism that is not an isogeny is defined to be 0.

4. Local root numbers in unramified extensions

The goal of this section is Corollary 4.6, which details the behavior of the local root number of an abelian variety upon an unramified extension of degree m of the nonarchimedean local base field. In fact, this behavior manifests itself for a wider class of representations than those coming from abelian varieties, as we observe in Corollary 4.5. To summarize, for every representation in this class the local root number "stabilizes" upon unramified base change of sufficiently divisible degree to a value determined by the parity of the conductor.[3] Such behavior, which is crucial for our proof of Theorem 1.4, seems not to have been pointed out previously.

Throughout §4, we let k be a nonarchimedean local field and let $\mathfrak{o}$, $\mathbb{F}$, p, and k^s be its ring of integers, its residue field, its residue characteristic, and a choice of a separable closure, respectively. We denote the unramified subextension of k^s/k of degree m and its ring of integers by k_m and $\mathfrak{o}_m$, respectively. We let $W(k^s/k)$ and I denote the Weil group and its inertia subgroup. We denote a geometric Frobenius in $W(k^s/k)$ by Frob_k. For a field F with $\mathrm{char}\, F \neq p$, we let

$$|\cdot|_k : W(k^s/k) \to F^\times$$

be the unramified character characterized by the equality $|\mathrm{Frob}_k|_k = (\#\mathbb{F})^{-1}$; for an integer n and a representation V of $W(k^s/k)$ over F, we set $V(n) := V \otimes_F |\cdot|_k^n$, where the second factor denotes a copy of F on which $W(k^s/k)$ acts through the n^{th} power of $|\cdot|_k$.

4.1. ϵ-factors of Weil–Deligne representations. For a field F with $\mathrm{char}\, F \neq p$, a *Weil–Deligne representation* of $W(k^s/k)$ over F is a pair

$$\rho' = (\rho, N)$$

that consists of

- a finite dimensional representation ρ of $W(k^s/k)$ over F such that the restriction of ρ to some open subgroup of I is trivial, and
- a $W(k^s/k)$-homomorphism $N\colon \rho \to \rho(-1)$.

Subject to the choices of a nontrivial additive character $\psi\colon k \to F^\times$ and a nonzero F-valued Haar measure dx on $(k, +)$, the ϵ-factor of ρ' is defined by

$$\epsilon(\rho', \psi, dx) := \epsilon_0(\rho, \psi, dx) \det(-\mathrm{Frob}_k \mid (\mathrm{Ker}\, N)^I)^{-1}, \tag{4.1.1}$$

where for the appearing ϵ_0-factor as well as for the definitions of an additive character and an F-valued Haar measure we refer to [Del73, §6] (or to [Čes16a, 1.1 and §§2.3–4]). The *Artin conductor* of ρ' is

$$a(\rho') := \mathrm{Sw}\, \rho + \dim_F \rho - \dim_F (\mathrm{Ker}\, N)^I; \tag{4.1.2}$$

for the definition of the Swan conductor $\mathrm{Sw}\, \rho$, see [Del73, §6.2] or [Čes16a, §2.9].

Before proceeding, for later use we record the following lemma about conductors of abelian varieties.

Lemma 4.2. *Let $B \to \mathrm{Spec}\, k$ be an abelian variety, let $a(B)$ be its conductor exponent, let $\mathcal{B}_{\mathbb{F}}$ be the special fiber of the Néron model of B, and let Φ be the component group scheme of $\mathcal{B}_{\mathbb{F}}$. For every prime ℓ different from* $\mathrm{char}\, \mathbb{F}$, *one has*

$$a(B) = a(B[\ell]) + \dim_{\mathbb{F}_\ell}(\Phi[\ell](\overline{\mathbb{F}})),$$

where the Artin conductor $a(B[\ell])$ is defined by (4.1.2) (*with $N = 0$*).

[3] We do not use conductor ideals, so 'conductor' abbreviates what some authors call 'conductor exponent.'

Proof. Let $(V_\ell B)^{\mathrm{ss}}$ be the semisimplification of the ℓ-adic Tate module of B. Then

$$a(B) = \mathrm{Sw}((V_\ell B)^{\mathrm{ss}}) + \dim_{\mathbb{Q}_\ell}(V_\ell B) - \dim_{\mathbb{Q}_\ell}(V_\ell B)^I,$$
$$a(B[\ell]) = \mathrm{Sw}(B[\ell]) + \dim_{\mathbb{F}_\ell}(B[\ell]) - \dim_{\mathbb{F}_\ell}(B[\ell]^I).$$

The identification of $B[\ell]^I$ and $(V_\ell B)^I$ with $\mathcal{B}_{\mathbb{F}}[\ell]$ and $V_\ell(\mathcal{B}_{\mathbb{F}})$ explained in [ST68, Lemma 2] gives

$$\dim_{\mathbb{Q}_\ell}(V_\ell B)^I = \dim_{\mathbb{Q}_\ell} V_\ell(\mathcal{B}_{\mathbb{F}}) = \dim_{\mathbb{F}_\ell}(\mathcal{B}_{\mathbb{F}}[\ell]) - \dim_{\mathbb{F}_\ell}(\Phi[\ell](\overline{\mathbb{F}})) = \dim_{\mathbb{F}_\ell}(B[\ell]^I) - \dim_{\mathbb{F}_\ell}(\Phi[\ell](\overline{\mathbb{F}})),$$

so it remains to note that $\mathrm{Sw}((V_\ell B)^{\mathrm{ss}}) = \mathrm{Sw}(B[\ell])$ because the Swan conductor is additive and is compatible with reduction mod ℓ. □

Returning to the setup of §4.1, we turn to the analysis of the epsilon factor of $\rho'|_{k_m}$.

Proposition 4.3. *In the setup of §4.1, for the restriction $\rho'|_{k_m}$ of ρ' to $W(k^s/k_m)$ one has*

$$\epsilon(\rho'|_{k_m}, \psi \circ \mathrm{Tr}_{k_m/k}, dx_m) = \begin{cases} \epsilon(\rho', \psi, dx)^m, & \text{if } m \text{ is odd,} \\ (-1)^{a(\rho')}\epsilon(\rho', \psi, dx)^m, & \text{if } m \text{ is even.} \end{cases}$$

Here dx_m denotes the Haar measure on $(k_m, +)$ characterized by $\int_{\mathfrak{o}_m} dx_m = (\int_{\mathfrak{o}} dx)^m$.

Proof. For the ϵ_0-factor appearing in (4.1.1), the inductivity in degree 0 gives the equality

$$\epsilon_0(\rho|_{k_m}, \psi \circ \mathrm{Tr}_{k_m/k}, dx_m) = \epsilon_0(\mathbf{1}_{k_m}, \psi \circ \mathrm{Tr}_{k_m/k}, dx_m)^{\dim_F \rho} \cdot \frac{\epsilon_0((\mathrm{Ind}_{k_m}^k \mathbf{1}_{k_m}) \otimes \rho, \psi, dx)}{\epsilon_0(\mathrm{Ind}_{k_m}^k \mathbf{1}_{k_m}, \psi, dx)^{\dim_F \rho}}. \quad (4.3.1)$$

Since $\mathrm{Ind}_{k_m}^k \mathbf{1}_{k_m}$ is unramified, [Del73, 5.5.3] (or [Čes‌16a, 3.2.2] for general F) simplifies the fraction to

$$\det(\mathrm{Ind}_{k_m}^k \mathbf{1}_{k_m})(\mathrm{Frob}_k)^{\mathrm{Sw}\,\rho} \cdot \frac{\epsilon_0(\rho, \psi, dx)^m}{\epsilon_0(\mathbf{1}_k, \psi, dx)^{m \dim_F \rho}} = (-1)^{(m-1)\,\mathrm{Sw}\,\rho} \cdot \frac{\epsilon_0(\rho, \psi, dx)^m}{\epsilon_0(\mathbf{1}_k, \psi, dx)^{m \dim_F \rho}}. \quad (4.3.2)$$

Let $n(\psi)$ denote the largest integer n such that $\psi|_{\pi^{-n}\mathfrak{o}} = 1$, where $\pi \in \mathfrak{o}$ is a uniformizer. Since k_m/k is unramified, $n(\psi \circ \mathrm{Tr}_{k_m/k}) = n(\psi)$ by [Del73, §4.11]; we use this in the following computation:

$$\epsilon_0(\mathbf{1}_k, \psi, dx)^m = \left(-(\#\mathbb{F})^{n(\psi)} \cdot \int_{\mathfrak{o}} dx\right)^m = (-1)^{m-1}\epsilon_0(\mathbf{1}_{k_m}, \psi \circ \mathrm{Tr}_{k_m/k}, dx_m). \quad (4.3.3)$$

The equations (4.3.1), (4.3.2), and (4.3.3) combine to give the equality

$$\epsilon_0(\rho|_{k_m}, \psi \circ \mathrm{Tr}_{k_m/k}, dx_m) = (-1)^{(m-1)(\mathrm{Sw}\,\rho + \dim_F \rho)}\epsilon_0(\rho, \psi, dx)^m. \quad (4.3.4)$$

It remains to put (4.3.4) together with the evident equality

$$\det(-\mathrm{Frob}_{k_m} \mid (\mathrm{Ker}\, N)^I)^{-1} = (-1)^{-(m-1)\dim_F (\mathrm{Ker}\, N)^I} \det(-\mathrm{Frob}_k \mid (\mathrm{Ker}\, N)^I)^{-m}. \quad □$$

4.4. Root numbers. Assume that $F = \mathbb{C}$ and $\int_{\mathfrak{o}} dx \in \mathbb{R}^+$ in §4.1. The *root number* of ρ' is

$$w(\rho', \psi) := \frac{\epsilon(\rho', \psi, dx)}{|\epsilon(\rho', \psi, dx)|}.$$

It does not depend on the choice of dx as long as $\int_{\mathfrak{o}} dx \in \mathbb{R}^+$. If $\det \rho$ is $\mathbb{R}^+$-valued, then $w(\rho', \psi)$ does not depend on the choice of ψ either, thanks to the formula [Del73, 5.4]. In this case we abbreviate $w(\rho', \psi)$ by $w(\rho')$. If B is an abelian variety over k, then

$$\bigwedge^{2g} H^1_{\text{ét}}(B, \mathbb{Q}_\ell) \cong H^{2g}_{\text{ét}}(B, \mathbb{Q}_\ell) \cong \mathbb{Q}_\ell(-g),$$

so the independence of ψ is witnessed if ρ' is the complex Weil–Deligne representation σ'_B that one associates to $H^1_{\text{ét}}(B, \mathbb{Q}_\ell) \cong (V_\ell B)^*$ for a prime ℓ different from p using the Grothendieck quasi-unipotence theorem and an embedding $\iota\colon \mathbb{Q}_\ell \hookrightarrow \mathbb{C}$. By [Sab07, 1.15], the isomorphism class of σ'_B does not depend on ℓ and ι,[4] and hence neither does the root number of B defined by

$$w(B) := w(\sigma'_B).$$

Due to the Weil pairing, the presence of a polarization of B, and [Del73, 5.7.1], one has $w(B) \in \{\pm 1\}$.

Corollary 4.5. *For a Weil–Deligne representation ρ' of $W(k^s/k)$ over $\mathbb{C}$ such that $\det \rho$ is $\mathbb{R}^+$-valued and $w(\rho')$ is an m_0^{th} root of unity,*

$$w(\rho'|_{k_m}) = (-1)^{a(\rho')}$$

for every even m divisible by m_0.

Proof. This follows from Proposition 4.3. ☐

Corollary 4.6. *Let B be an abelian variety over k, and let $a(B)$ be its conductor exponent. Then*

$$w(B_{k_m}) = \begin{cases} w(B), & \text{if } m \text{ is odd,} \\ (-1)^{a(B)}, & \text{if } m \text{ is even.} \end{cases}$$

Proof. Combine Proposition 4.3 and the equality $a(B) = a(\sigma'_B)$ that results from the definitions (for which one may consult [Ser70, §2]). ☐

Remark 4.7. For elliptic curves, excluding the troublesome additive reduction case if $p \leqslant 3$, one may also prove Corollary 4.6 by the means of explicit case-by-case formulae for $w(B)$ and $a(B)$.

5. Arithmetic duality generalities: comparing Selmer sizes modulo squares

The main goal of this section is to prove Theorem 5.9, which in §6 will specialize to the arithmetic duality input needed for the proof of Theorem 1.4. Theorem 5.9 generalizes [KMR13, Thm. 3.9] to the case of commutative self-dual finite group schemes over global fields from the case of self-dual 2-dimensional $\mathbb{F}_p$-vector space group schemes over number fields. Although its proof is loosely modeled on that of *loc. cit.*, modifications are necessary due to the possibility that $\operatorname{char} F \mid \#\mathcal{G}$, when various cohomology groups are no longer finite. The simpler case of Theorem 5.9 when $\operatorname{char} F \nmid \#\mathcal{G}$ suffices for the proof of Theorem 1.4, but it seems unnatural to confine the general techniques in this way. Consequently, Theorem 6.6 does not exclude the more subtle cases when $\operatorname{char} F \mid n$.

In the buildup to Theorem 5.9 we follow an axiomatic approach by introducing further assumptions as we need them. This way, in Proposition 5.6 we arrive at a generalization of [MR07, Prop. 1.3 (i)] that removes the self-duality, $\mathbb{F}_p$-vector space, and number field assumptions from *loc. cit.*

In this section and in §6 all the cohomology groups are fppf. Identifications with étale or Galois cohomology are implicit. Likewise implicit is the Tate modification: if v is archimedean, then we write $H^i(K_v, -)$ for $\widehat{H}^i(K_v, -)$ (this has no effect if $i \geqslant 1$).

5.1. The basic setup. Let F be a global field. If $\operatorname{char} F = 0$, let S be the spectrum of the ring of integers of F; if $\operatorname{char} F > 0$, let S be the connected smooth proper curve over a finite field such that the function field of S is F. Let $U \subset S$ be a nonempty open subscheme. We denote by v a place of

[4] *Loc. cit.* does not use its additional $\operatorname{char} k = 0$ assumption in the proof. Also, we bypass this issue by analyzing the right hand side of (1.1.2) through the second case of Corollary 4.6, the proof of which works for every ℓ and ι.

F and identify the nonarchimedean v with the closed points of S; writing $v \notin U$ signifies that v does not correspond to a closed point of U (and hence could be archimedean).

Let

$$\mathcal{G} \to U \qquad \text{and} \qquad \mathcal{H} \to U$$

be commutative finite flat group schemes, and suppose that there is a perfect bilinear pairing

$$\mathcal{G} \times_U \mathcal{H} \xrightarrow{b} \mathbb{G}_m \qquad \text{that identifies } \mathcal{G} \text{ and } \mathcal{H} \text{ as Cartier duals.}$$

The cohomology groups $H^1(U, \mathcal{G})$ and $H^1(U, \mathcal{H})$ are "cut out by local conditions," i.e., as noted in [Česk16b, 4.3], the squares

$$\begin{array}{ccc} H^1(U,\mathcal{G}) & \hookrightarrow & H^1(F,\mathcal{G}) \\ \downarrow & & \downarrow \\ \prod_{v \in U} H^1(\mathcal{O}_v,\mathcal{G}) & \hookrightarrow & \prod_{v\in U} H^1(F_v,\mathcal{G}), \end{array} \qquad \begin{array}{ccc} H^1(U,\mathcal{H}) & \hookrightarrow & H^1(F,\mathcal{H}) \\ \downarrow & & \downarrow \\ \prod_{v \in U} H^1(\mathcal{O}_v,\mathcal{H}) & \hookrightarrow & \prod_{v\in U} H^1(F_v,\mathcal{H}) \end{array}$$

are Cartesian. The main result of this section, Theorem 5.9, investigates further subgroups cut out by also imposing local conditions at all $v \notin U$. Its proof hinges on, among other things, the Tate–Shatz local duality [Sha64, Duality theorem on p. 411] (alternatively, [Mil06, I.2.3, I.2.13 (a), III.6.10]), which says that for every place v and integer i the cup product pairing

$$H^i(F_v, \mathcal{G}) \times H^{2-i}(F_v, \mathcal{H}) \longrightarrow H^2(F_v, \mathbb{G}_m) \xhookrightarrow{\mathrm{inv}_v} \mathbb{Q}/\mathbb{Z} \tag{5.1.1}$$

that uses b identifies $H^i(F_v, \mathcal{G})$ and $H^{2-i}(F_v, \mathcal{H})$ as Pontryagin duals of each other. The Pontryagin duality in question is that of locally compact Hausdorff abelian topological groups—see [Česk15, 3.1–3.2 and 1.4] for the definition and properties of the topology on these cohomology groups. These groups are finite and discrete if $\mathrm{char}\, F_v \nmid \#\mathcal{G}$; this case suffices for the proof of Theorem 1.4.

Example 5.2. Our main case of interest in the setup of §5.1 is when $B \to \mathrm{Spec}\, F$ and $B^\vee \to \mathrm{Spec}\, F$ are dual abelian varieties, $\mathcal{B} \to S$ and $\mathcal{B}^\vee \to S$ are their Néron models, $U \subset S$ is such that $\mathcal{B}_U \to U$ and $\mathcal{B}_U^\vee \to U$ are abelian schemes, and $\mathcal{G} = \mathcal{B}[n]_U$, $\mathcal{H} = \mathcal{B}^\vee[n]_U$ for some $n \in \mathbb{Z}_{>0}$. Cartier–Nishi duality [Oda69, Thm. 1.1] supplies the pairing b in this case.

The following lemma is crucial for the arithmetic duality results derived below.

Lemma 5.3. *In the setup of* §5.1*, for every integer i the images of the pullback maps*

$$H^i(U, \mathcal{G}) \xrightarrow{\mathrm{loc}^i(\mathcal{G})} \bigoplus_{v \notin U} H^i(F_v, \mathcal{G}) \qquad \text{and} \qquad H^{2-i}(U, \mathcal{H}) \xrightarrow{\mathrm{loc}^{2-i}(\mathcal{H})} \bigoplus_{v \notin U} H^{2-i}(F_v, \mathcal{H})$$

are orthogonal complements under the sum of the pairings (5.1.1).

Proof. In the case when $\#\mathcal{G} \in \Gamma(U, \mathcal{O}_U^\times)$, the Poitou–Tate sequence gives the claim once one explicates its morphisms and interprets the global cohomology groups as Galois cohomology with restricted ramification (for this interpretation consult, e.g., [Mil06, II.2.9]). To treat the general case we will use an extension of the Poitou–Tate sequence, namely, the compactly supported flat cohomology sequence

$$\cdots \to H^i_c(U, \mathcal{G}) \to H^i(U, \mathcal{G}) \xrightarrow{\mathrm{loc}^i(\mathcal{G})} \bigoplus_{v \notin U} H^i(F_v, \mathcal{G}) \xrightarrow{\delta^i_c(\mathcal{G})} H^{i+1}_c(U, \mathcal{G}) \to \cdots \tag{5.3.1}$$

of [Mil06, III.0.4 (a)]. The pairings in the diagram

$$\begin{array}{ccccccc} H^i(U,\mathcal{G}) & \times & H^{3-i}_c(U,\mathcal{H}) & \xrightarrow{\text{[Mil06, III.3.2 and III.8.2]}} & H^3_c(U,\mathbb{G}_m) & \xrightarrow{\text{tr}} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{loc}^i(\mathcal{G})} & & \uparrow{\scriptstyle \delta_c^{2-i}(\mathcal{H})} & & \uparrow{\scriptstyle \delta_c^{2}(\mathbb{G}_m)} & & \| \\ \bigoplus_{v\notin U} H^i(F_v,\mathcal{G}) & \times & \bigoplus_{v\notin U} H^{2-i}(F_v,\mathcal{H}) & \xrightarrow{\sum_v (5.1.1)} & \bigoplus_{v\notin U} H^2(F_v,\mathbb{G}_m) & \xrightarrow{\sum_v \mathrm{inv}_v} & \mathbb{Q}/\mathbb{Z} \end{array} \qquad (\dagger)$$

are perfect, so the exactness of (5.3.1) reduces the desired claim to the commutativity of both squares of (†) (and of their analogues with $\mathcal{G}$ and $\mathcal{H}$ interchanged and i replaced by $2-i$). The right square of (†) commutes by [Mil06, (b) in the beginning of II.§3].

The cup product (5.1.1) in the bottom left arrow of (†) agrees with the Ext-product as in [GH71, 3.1], which in turn agrees with the Yoneda edge product as in [GH70, 4.5], so the left square of (†) is identified with the square

$$\begin{array}{ccccc} \mathrm{Ext}^i_U(\mathcal{H},\mathbb{G}_m) & \times & H^{3-i}_c(U,\mathcal{H}) & \xrightarrow{\text{[Mil06, III.0.4 (e)]}} & H^3_c(U,\mathbb{G}_m) \\ \downarrow & & \uparrow{\scriptstyle \delta_c^{2-i}(\mathcal{H})} & & \uparrow{\scriptstyle \delta_c^{2}(\mathbb{G}_m)} \\ \bigoplus_{v\notin U} \mathrm{Ext}^i_{F_v}(\mathcal{H},\mathbb{G}_m) & \times & \bigoplus_{v\notin U} H^{2-i}(F_v,\mathcal{H}) & \longrightarrow & \bigoplus_{v\notin U} H^2(F_v,\mathbb{G}_m). \end{array} \qquad (\ddagger)$$

The desired commutativity of (‡) then results from the definitions and from the inspection of the proof of [Mil06, III.0.4 (e)]: if one fixes injective resolutions

$$\mathcal{H} \to I^\bullet(\mathcal{H}) \qquad \text{and} \qquad \mathbb{G}_m \to I^\bullet(\mathbb{G}_m)$$

over U and interprets elements of $\mathrm{Ext}^i(\mathcal{H},\mathbb{G}_m)$ and $\bigoplus_{v\notin U} H^{2-i}(F_v,\mathcal{H})$ as homotopy classes of maps

$$I^\bullet(\mathcal{H}) \xrightarrow{a} I^\bullet(\mathbb{G}_m)[i] \qquad \text{and} \qquad \mathbb{Z} \xrightarrow{d} \Gamma\left(\bigoplus_{v\notin U} F_v, I^\bullet(\mathcal{H})|_{\bigoplus_{v\notin U} F_v}\right)[2-i],$$

then both ways to pair a and d in (‡) result in the element of $H^3_c(U,\mathbb{G}_m)$ that is represented by the homotopy class of the map

$$\mathbb{Z} \xrightarrow{\left(0,\, \Gamma(\bigoplus_{v\notin U} F_v,\, a|_{\bigoplus_{v\notin U} F_v})[2-i]\circ d\right)} \Gamma\left(U, I^\bullet(\mathbb{G}_m)\right)[3] \oplus \Gamma\left(\bigoplus_{v\notin U} F_v, I^\bullet(\mathbb{G}_m)|_{\bigoplus_{v\notin U} F_v}\right)[2]. \qquad \square$$

5.4. Local conditions at $v \notin U$. In the setup of §5.1, suppose that for every $j \in \{1,2\}$ and $v \notin U$ we have open compact subgroups

$$\mathrm{Sel}^j(\mathcal{G}_{F_v}) \subset H^1(F_v,\mathcal{G}) \qquad \text{and} \qquad \mathrm{Sel}^j(\mathcal{H}_{F_v}) \subset H^1(F_v,\mathcal{H})$$

that are orthogonal complements under (5.1.1). For $j \in \{1,2\}$, define the Selmer groups $\mathrm{Sel}^j(\mathcal{G})$ and $\mathrm{Sel}^j(\mathcal{H})$ by requiring the sequences

$$0 \to \mathrm{Sel}^j(\mathcal{G}) \to H^1(U,\mathcal{G}) \to \bigoplus_{v\notin U} H^1(F_v,\mathcal{G})/\mathrm{Sel}^j(\mathcal{G}_{F_v}),$$
$$0 \to \mathrm{Sel}^j(\mathcal{H}) \to H^1(U,\mathcal{H}) \to \bigoplus_{v\notin U} H^1(F_v,\mathcal{H})/\mathrm{Sel}^j(\mathcal{H}_{F_v})$$

to be exact. For $v \notin U$, [HR79, 24.10] gives further orthogonal complements

$$\mathrm{Sel}^{1+2}(\mathcal{G}_{F_v}) := \mathrm{Sel}^1(\mathcal{G}_{F_v}) + \mathrm{Sel}^2(\mathcal{G}_{F_v}) \qquad \text{and} \qquad \mathrm{Sel}^{1\cap 2}(\mathcal{H}_{F_v}) := \mathrm{Sel}^1(\mathcal{H}_{F_v}) \cap \mathrm{Sel}^2(\mathcal{H}_{F_v}),$$

and one defines the corresponding Selmer groups $\mathrm{Sel}^{1+2}(\mathcal{G})$ and $\mathrm{Sel}^{1\cap 2}(\mathcal{H})$ by the exactness of the sequences

$$0 \to \mathrm{Sel}^{1+2}(\mathcal{G}) \to H^1(U,\mathcal{G}) \to \bigoplus_{v\notin U} H^1(F_v,\mathcal{G})/\mathrm{Sel}^{1+2}(\mathcal{G}_{F_v}),$$
$$0 \to \mathrm{Sel}^{1\cap 2}(\mathcal{H}) \to H^1(U,\mathcal{H}) \to \bigoplus_{v\notin U} H^1(F_v,\mathcal{H})/\mathrm{Sel}^{1\cap 2}(\mathcal{H}_{F_v}).$$

Example 5.5. In Example 5.2 the local conditions of most interest to us arise when one takes the images of the local Kummer maps for Sel^1 and, under appropriate restrictions, their fppf cohomological counterparts $H^1(\mathcal{O}_v, \mathcal{B}[n])$ and $H^1(\mathcal{O}_v, \mathcal{B}^\vee[n])$ for Sel^2. In §6, we will justify that the results of §5 can be applied in this setting to compare $\#\,\mathrm{Sel}_n\, B$ and $\#H^1(S, \mathcal{B}[n])$ modulo squares.

Proposition 5.6. *In the setup of §5.4, the Selmer groups* $\mathrm{Sel}^j(\mathcal{G})$ *and* $\mathrm{Sel}^j(\mathcal{H})$ *for* $j \in \{1, 2\}$*, as well as* $\mathrm{Sel}^{1+2}(\mathcal{G})$ *and* $\mathrm{Sel}^{1\cap 2}(\mathcal{H})$*, are finite and*

$$\#\left(\frac{\mathrm{Sel}^{1+2}(\mathcal{G})}{\mathrm{Sel}^1(\mathcal{G})}\right) \cdot \#\left(\frac{\mathrm{Sel}^1(\mathcal{H})}{\mathrm{Sel}^{1\cap 2}(\mathcal{H})}\right) = \prod_{v\notin U} \#\left(\frac{\mathrm{Sel}^{1+2}(\mathcal{G}_{F_v})}{\mathrm{Sel}^1(\mathcal{G}_{F_v})}\right) = \prod_{v\notin U} \#\left(\frac{\mathrm{Sel}^1(\mathcal{H}_{F_v})}{\mathrm{Sel}^{1\cap 2}(\mathcal{H}_{F_v})}\right).$$

Proof. The finiteness is a special case of [Česk17, 3.2] (whose proof uses Lemma 5.3 but no other results of this paper).

Due to Lemma 5.3 and the choice of $\mathrm{Sel}^1(\mathcal{G}_{F_v})$ and $\mathrm{Sel}^1(\mathcal{H}_{F_v})$, [HR79, 24.10] shows that the subgroups

$$\mathrm{Im}(\mathrm{loc}^1(\mathcal{G})) + \textstyle\bigoplus_{v\notin U} \mathrm{Sel}^1(\mathcal{G}_{F_v}) \subset \bigoplus_{v\notin U} H^1(F_v, \mathcal{G}) \quad \text{and} \quad \mathrm{Im}(\mathrm{loc}^1(\mathcal{H})|_{\mathrm{Sel}^1(\mathcal{H})}) \subset \bigoplus_{v\notin U} H^1(F_v, \mathcal{H})$$

are orthogonal complements. Therefore, so are the subgroups

$$\tfrac{H^1(U,\mathcal{G})}{\mathrm{Sel}^1(\mathcal{G})} \subset \textstyle\bigoplus_{v\notin U} \tfrac{H^1(F_v,\mathcal{G})}{\mathrm{Sel}^1(\mathcal{G}_{F_v})} \quad \text{and} \quad \mathrm{Im}(\mathrm{loc}^1(\mathcal{H})|_{\mathrm{Sel}^1(\mathcal{H})}) \subset \bigoplus_{v\notin U} \mathrm{Sel}^1(\mathcal{H}_{F_v}).$$

Likewise, the subgroups

$$\textstyle\bigoplus_{v\notin U} \tfrac{\mathrm{Sel}^{1+2}(\mathcal{G}_{F_v})}{\mathrm{Sel}^1(\mathcal{G}_{F_v})} \subset \bigoplus_{v\notin U} \tfrac{H^1(F_v,\mathcal{G})}{\mathrm{Sel}^1(\mathcal{G}_{F_v})} \quad \text{and} \quad \bigoplus_{v\notin U} \mathrm{Sel}^{1\cap 2}(\mathcal{H}_{F_v}) \subset \bigoplus_{v\notin U} \mathrm{Sel}^1(\mathcal{H}_{F_v})$$

are also orthogonal complements. By combining the last two claims we deduce that the subgroups

$$\tfrac{\mathrm{Sel}^{1+2}(\mathcal{G})}{\mathrm{Sel}^1(\mathcal{G})} \subset \textstyle\bigoplus_{v\notin U} \tfrac{H^1(F_v,\mathcal{G})}{\mathrm{Sel}^1(\mathcal{G}_{F_v})} \quad \text{and} \quad \mathrm{Im}(\mathrm{loc}^1(\mathcal{H})|_{\mathrm{Sel}^1(\mathcal{H})}) + \bigoplus_{v\notin U} \mathrm{Sel}^{1\cap 2}(\mathcal{H}_{F_v}) \subset \bigoplus_{v\notin U} \mathrm{Sel}^1(\mathcal{H}_{F_v})$$

are orthogonal complements, too, and hence so are the subgroups

$$\tfrac{\mathrm{Sel}^{1+2}(\mathcal{G})}{\mathrm{Sel}^1(\mathcal{G})} \subset \textstyle\bigoplus_{v\notin U} \tfrac{\mathrm{Sel}^{1+2}(\mathcal{G}_{F_v})}{\mathrm{Sel}^1(\mathcal{G}_{F_v})} \quad \text{and} \quad \tfrac{\mathrm{Sel}^1(\mathcal{H})}{\mathrm{Sel}^{1\cap 2}(\mathcal{H})} \subset \bigoplus_{v\notin U} \tfrac{\mathrm{Sel}^1(\mathcal{H}_{F_v})}{\mathrm{Sel}^{1\cap 2}(\mathcal{H}_{F_v})}.$$

Both $\mathrm{Sel}^1(\mathcal{H}_{F_v})$ and $\mathrm{Sel}^{1\cap 2}(\mathcal{H}_{F_v})$ are open and compact, so the groups in the last display are finite and the conclusion follows from the fact that dual finite abelian groups have the same cardinality. □

5.7. Breaking the symmetry. In the setup of §5.4, suppose that one has the following data.

- An isomorphism
$$\theta \colon \mathcal{G} \xrightarrow{\sim} \mathcal{H}$$
of U-group schemes such that $H^1(F_v, \theta)$ identifies the subgroup
$$\mathrm{Sel}^j(\mathcal{G}_{F_v}) \subset H^1(F_v, \mathcal{G}) \quad \text{with} \quad \mathrm{Sel}^j(\mathcal{H}_{F_v}) \subset H^1(F_v, \mathcal{H}) \qquad \text{for every } v \notin U \text{ and } j \in \{1, 2\},$$
so that, consequently, the isomorphism $H^1(U, \theta)$ identifies the subgroup
$$\mathrm{Sel}^j(\mathcal{G}) \subset H^1(U, \mathcal{G}) \quad \text{with} \quad \mathrm{Sel}^j(\mathcal{H}) \subset H^1(U, \mathcal{H}) \qquad \text{for every } j \in \{1, 2\}.$$

- For each $v \notin U$, a map $q_v \colon H^1(F_v, \mathcal{G}) \to \mathbb{Q}/\mathbb{Z}$ subject to the following requirements.
  (i) One has $q_v(ax) = a^2 q_v(x)$ for all $a \in \mathbb{Z}$ and $x \in H^1(F_v, \mathcal{G})$.

(ii) The map
$$(x, y) \mapsto q_v(x+y) - q_v(x) - q_v(y)$$
agrees with the bilinear form $\langle x, y\rangle_v$ defined by the commutativity of the diagram

$$\begin{array}{ccccc} \langle\ ,\ \rangle_v\colon H^1(F_v, \mathcal{G}) \times H^1(F_v, \mathcal{G}) & \longrightarrow & H^2(F_v, \mathbb{G}_m) & \xhookrightarrow{\mathrm{inv}_v} & \mathbb{Q}/\mathbb{Z} \\ \downarrow{\scriptstyle \mathrm{id} \times H^1(F_v, \theta)}\ \wr & & \| & & \| \\ H^1(F_v, \mathcal{G}) \times H^1(F_v, \mathcal{H}) & \xrightarrow{(5.1.1)} & H^2(F_v, \mathbb{G}_m) & \xhookrightarrow{\mathrm{inv}_v} & \mathbb{Q}/\mathbb{Z}. \end{array} \tag{5.7.1}$$

(iii) One has $q_v(\mathrm{Sel}^j(\mathcal{G}_{F_v})) = 0$ for $j \in \{1, 2\}$.

(iv) For every $x \in H^1(U, \mathcal{G})$, its pullbacks $x_v \in H^1(F_v, \mathcal{G})$ satisfy $\sum_{v \notin U} q_v(x_v) = 0$.

Since $\mathrm{Sel}^j(\mathcal{G}_{F_v})$ and $\mathrm{Sel}^j(\mathcal{H}_{F_v})$ are orthogonal complements, these conditions ensure that for every $v \notin U$ the subgroups $\mathrm{Sel}^j(\mathcal{G}_{F_v}) \subset H^1(F_v, \mathcal{G})$ are maximal isotropic for the quadratic form q_v.

Remark 5.8. In practice, the quadratic forms q_v come into play only when $\#\mathcal{G}$ is even. Indeed, for odd $\#\mathcal{G}$, the equality $\langle x, x\rangle_v = 2q_v(x)$ determines q_v, so if one insists that θ is such that the pairing
$$b_{F_v}(-, \theta_{F_v}(\cdot))\colon \mathcal{G}_{F_v} \times_{F_v} \mathcal{G}_{F_v} \to \mathbb{G}_m \qquad \text{for } v \notin U$$
is antisymmetric, then (ii) holds because the bilinear form $\langle\ ,\ \rangle_v$ is symmetric (as may be seen using Čech cohomology), (iii) follows from the isotropy of the subgroups $\mathrm{Sel}^j(\mathcal{G}_{F_v})$, (iv) follows from the reciprocity for the Brauer group, whereas (i) results from the relation between q_v and $\langle\ ,\ \rangle_v$.

Theorem 5.9. *In the setup of* §5.7*,*
$$\frac{\#\,\mathrm{Sel}^1(\mathcal{G})}{\#\,\mathrm{Sel}^2(\mathcal{G})} \equiv \prod_{v \notin U} \#\left(\frac{\mathrm{Sel}^1(\mathcal{G}_{F_v})}{\mathrm{Sel}^1(\mathcal{G}_{F_v}) \cap \mathrm{Sel}^2(\mathcal{G}_{F_v})}\right) \quad \mathrm{mod}\ \mathbb{Q}^{\times 2}. \tag{5.9.1}$$

Proof. The proof will use the following Lemma 5.9.2, which is a variant of [KMR13, Lemma 2.3]. Before stating Lemma 5.9.2, we introduce the quadratic space
$$(V, q) = \left(\textstyle\bigoplus_{v \notin U} H^1(F_v, \mathcal{G}),\ \sum_{v \notin U} q_v\right), \quad \text{whose associated bilinear form is} \quad \langle\ ,\ \rangle := \textstyle\sum_{v \notin U} \langle\ ,\ \rangle_v\,.$$
Since $\langle\ ,\ \rangle$ is continuous and nondegenerate, it exhibits V as its own Pontryagin dual. The subgroups
$$X = \textstyle\bigoplus_{v \notin U} \mathrm{Sel}^1(\mathcal{G}_{F_v}), \qquad Y = \bigoplus_{v \notin U} \mathrm{Sel}^2(\mathcal{G}_{F_v}), \qquad Z = \mathrm{Im}(\mathrm{loc}^1(\mathcal{G})),$$
are maximal isotropic for q: indeed, X and Y due to §5.7 (iii), and Z due to Lemma 5.3 and §5.7 (iv).

Since $\mathrm{Sel}^1(\mathcal{G})$ is finite (see Proposition 5.6), so is its quotient $X \cap Z$, and likewise for $Y \cap Z$. In V, both X and $X \cap Y$ are open and compact, so $\frac{X+Y}{Y} \cong \frac{X}{X \cap Y}$ is finite. Thus, since
$$\tfrac{(X+Y)\cap Z}{Y \cap Z} \hookrightarrow \tfrac{X+Y}{Y},$$
the intersection $(X+Y) \cap Z$ is finite, too.

Lemma 5.9.2. *We have*
$$\#\left((X+Y) \cap Z\right) \equiv \#\left((X \cap Z) + (Y \cap Z)\right) \ \mathrm{mod}\ \mathbb{Q}^{\times 2}.$$

Proof. The proof of [KMR13, Lemma 2.3] extends; we outline this extension.

The vanishing of the restrictions $\langle\ ,\ \rangle|_X$ and $\langle\ ,\ \rangle|_Y$ allows us to define a $\mathbb{Q}/\mathbb{Z}$-valued bilinear pairing $[\ ,\ ]$ on $(X+Y) \cap Z$ by
$$[x+y, x'+y'] := \langle x, y'\rangle \quad \text{for} \quad x+y,\ x'+y' \in (X+Y) \cap Z \quad \text{with} \quad x, x' \in X \quad \text{and} \quad y, y' \in Y.$$

The isotropy of Z, X, and Y gives the vanishing

$$\langle x, y\rangle = q(x+y) - q(x) - q(y) = 0,$$

so $[\ ,\ ]$ is alternating. The resulting antisymmetry of $[\ ,\ ]$ ensures that the right and left kernels of $[\ ,\ ]$ agree; in particular, this common kernel K contains $(X \cap Z) + (Y \cap Z)$. We claim that also

$$K \subset (X \cap Z) + (Y \cap Z), \qquad \text{so that} \qquad K = (X \cap Z) + (Y \cap Z). \tag{5.9.3}$$

To argue (5.9.3), we fix x, y as above with

$$x + y \in K, \qquad \text{so that} \qquad x \in (((X+Y) \cap Z) + (X \cap Y))^{\perp},$$

where the orthogonal complement is taken in $(V, \langle\ ,\ \rangle)$. Since the appearing subgroups are closed, [HR79, 24.10] gives

$$(((X+Y) \cap Z) + (X \cap Y))^{\perp} = ((X \cap Y) + Z) \cap (X+Y) = ((X+Y) \cap Z) + (X \cap Y),$$

so the freedom of adjusting x and y by opposite elements of $X \cap Y$ allows us to assume that

$$x \in (X+Y) \cap Z \subset Z.$$

Then $y \in Z$ as well, which gives $x + y \in (X \cap Z) + (Y \cap Z)$, and (5.9.3) follows.

In conclusion, $[\ ,\ ]$ induces a nondegenerate alternating bilinear pairing on the quotient

$$\tfrac{(X+Y)\cap Z}{(X \cap Z)+(Y \cap Z)}.$$

A well-known argument, as for example [Dav10, proof of Lemma 4.2], then implies that $\frac{(X+Y)\cap Z}{(X\cap Z)+(Y\cap Z)}$ is a square of another finite abelian group, and hence is of square order, as desired. □

According to Proposition 5.6, the right hand side of (5.9.1) equals $\#\left(\frac{\mathrm{Sel}^{1+2}(\mathcal{G})}{\mathrm{Sel}^{1\cap 2}(\mathcal{G})}\right)$, which in turn equals $\#\left(\frac{(X+Y)\cap Z}{X\cap Y\cap Z}\right)$. Moreover,

$$\#\left(\frac{(X+Y)\cap Z}{X \cap Y \cap Z}\right) \overset{5.9.2}{\equiv} \#((X\cap Z) + (Y \cap Z)) \cdot \#(X \cap Y \cap Z) \equiv \frac{\#(X \cap Z)}{\#(Y \cap Z)} \mod \mathbb{Q}^{\times 2},$$

and it remains to observe that $\frac{\#(X\cap Z)}{\#(Y\cap Z)} = \frac{\#\,\mathrm{Sel}^1(\mathcal{G})}{\#\,\mathrm{Sel}^2(\mathcal{G})}$. □

6. Comparing Selmer sizes modulo squares in the main case of interest

In this section we specialize the results of §5 to the setup of Example 5.2, which we assume and recall: $\mathcal{B}$ and $\mathcal{B}^\vee$ are global Néron models of dual abelian varieties B and $B^\vee$ that have good reduction at all the points of U, and

$$\mathcal{G} = \mathcal{B}[n]_U, \qquad \mathcal{H} = \mathcal{B}^\vee[n]_U$$

for some $n \in \mathbb{Z}_{>0}$. Our main task is to justify that under suitable restrictions on B various general assumptions made in §5 are met if the local conditions are chosen as in Example 5.5 (we recall the choices in Proposition 6.1). This justification leads to Theorem 6.6, which in §7 will be a key ingredient in the proof of Theorem 1.4.

Proposition 6.1. *The following subgroups satisfy the hypotheses of §5.4, i.e., are open compact orthogonal complements.*

(a) *For* $v \notin U$,

$$\mathrm{Sel}^1(\mathcal{G}_{F_v}) = B(F_v)/nB(F_v) \quad \textit{and} \quad \mathrm{Sel}^1(\mathcal{H}_{F_v}) = B^\vee(F_v)/nB^\vee(F_v).$$

With these choices,

$$\mathrm{Sel}^1(\mathcal{G}) = \mathrm{Sel}_n(B) \qquad \textit{and} \qquad \mathrm{Sel}^1(\mathcal{H}) = \mathrm{Sel}_n(B^\vee);$$

both Selmer groups are finite.

(b) *For* $v \notin U$,

$$\begin{aligned} \mathrm{Sel}^2(\mathcal{G}_{F_v}) &= H^1(\mathcal{O}_v, \mathcal{B}[n]) \quad \textit{and} \quad \mathrm{Sel}^2(\mathcal{H}_{F_v}) = H^1(\mathcal{O}_v, \mathcal{B}^\vee[n]) \qquad \textit{if } v \nmid \infty, \\ \mathrm{Sel}^2(\mathcal{G}_{F_v}) &= B(F_v)/nB(F_v) \quad \textit{and} \quad \mathrm{Sel}^2(\mathcal{H}_{F_v}) = B^\vee(F_v)/nB^\vee(F_v) \qquad \textit{if } v \mid \infty \end{aligned}$$

under the assumption that B (and hence also $B^\vee$) has semiabelian reduction at all $v \in S \backslash U$ with $\mathrm{char}\, \mathbb{F}_v \mid n$. *With these choices,* $\mathrm{Sel}^2(\mathcal{G})$ *is the subgroup* $H^1(S, \mathcal{B}[n])' \subset H^1(S, \mathcal{B}[n])$ *consisting of the elements whose restrictions to every* $H^1(F_v, B[n])$ *with* $v \mid \infty$ *lie in* $B(F_v)/nB(F_v)$, *and similarly for* $\mathrm{Sel}^2(\mathcal{H})$; *both* $\mathrm{Sel}^2(\mathcal{G})$ *and* $\mathrm{Sel}^2(\mathcal{H})$ *are finite.*

Proof. The finiteness claims follow from the rest and from Proposition 5.6.

(a) The orthogonal complement claim is a well-known important step of the proof of Tate local duality, compare [Mil06, proof of III.7.8]. By [Česl5, 4.2 and 4.3 (b)], the connecting homomorphism

$$B(F_v) \to H^1(F_v, B[n])$$

is continuous and open (and likewise for $B^\vee$). Therefore, its image is open. Since $B(F_v)$ is compact, this image is also compact. The identification $\mathrm{Sel}^1(\mathcal{G}) = \mathrm{Sel}_n B$ results from the definition of $\mathrm{Sel}_n B$ and from [Česl6b, 2.5 (d) and 4.2] (and similarly for $\mathrm{Sel}^1(\mathcal{H})$).

(b) The $v \mid \infty$ case follows from (a), so we assume that $v \in S \backslash U$ (i.e., that $v \nmid \infty$). For such v, the given Sel^2 are subgroups due to [Česl6b, 4.4] (which does not use the assumption on semiabelian reduction). Their openness and compactness follow from [Česl5, 3.10].

The orthogonal complement claim is essentially [McC86, 4.14], but we must check that (5.1.1) agrees with the pairing used in *loc. cit.* More precisely, the cohomology with supports sequence

$$\cdots \to H^m_{\mathbb{F}_v}(\mathcal{O}_v, \mathcal{B}[n]) \to H^m(\mathcal{O}_v, \mathcal{B}[n]) \to H^m(F_v, B[n]) \to H^{m+1}_{\mathbb{F}_v}(\mathcal{O}_v, \mathcal{B}[n]) \to \cdots$$

of [Mil06, III.0.3 (c)] is exact and the pairings in the diagram

$$\begin{array}{ccccc} H^2_{\mathbb{F}_v}(\mathcal{O}_v, \mathcal{B}[n]) & \times & H^1(\mathcal{O}_v, \mathcal{B}^\vee[n]) & \xrightarrow{[\text{McC86, 4.14}]} & H^3_{\mathbb{F}_v}(\mathcal{O}_v, \mathbb{G}_m) \cong \mathbb{Q}/\mathbb{Z} \\ \uparrow & & \downarrow & & \uparrow \wr \\ H^1(F_v, B[n]) & \times & H^1(F_v, B^\vee[n]) & \xrightarrow{(5.1.1)} & H^2(F_v, \mathbb{G}_m) \cong \mathbb{Q}/\mathbb{Z} \end{array} \tag{6.1.1}$$

are perfect, so it suffices to prove that (6.1.1) and its analogue for $\mathcal{B}^\vee[n]$ commute. Let

$$i\colon \mathrm{Spec}\, \mathbb{F}_v \hookrightarrow \mathrm{Spec}\, \mathcal{O}_v \qquad \text{and} \qquad j\colon \mathrm{Spec}\, F_v \hookrightarrow \mathrm{Spec}\, \mathcal{O}_v$$

be the indicated immersions. Both pairings in (6.1.1) are Yoneda edge products—the top one due to its definition and the bottom one due to the observations made in the proof of

Lemma 5.3—so the commutativity of the diagram (6.1.1) will follow from that of

$$\begin{array}{ccccc}
\mathrm{Ext}^2(i_*\underline{\mathbb{Z}}_{\mathbb{F}_v}, \mathcal{B}[n]) & \times & \mathrm{Ext}^1(\mathcal{B}[n], \mathbb{G}_m) & \xrightarrow{\text{[McC86, 4.14]}} & \mathrm{Ext}^3(i_*\underline{\mathbb{Z}}_{\mathbb{F}_v}, \mathbb{G}_m) \\
\uparrow & & \| & & \uparrow \wr \\
\mathrm{Ext}^1(j_!\underline{\mathbb{Z}}_{F_v}, \mathcal{B}[n]) & \times & \mathrm{Ext}^1(\mathcal{B}[n], \mathbb{G}_m) & \longrightarrow & \mathrm{Ext}^2(j_!\underline{\mathbb{Z}}_{F_v}, \mathbb{G}_m) \\
\wr\| & & \downarrow & & \wr\| \\
\mathrm{Ext}^1(\underline{\mathbb{Z}}_{F_v}, B[n]) & \times & \mathrm{Ext}^1(B[n], \mathbb{G}_m) & \xrightarrow{(5.1.1)} & \mathrm{Ext}^2(\underline{\mathbb{Z}}_{F_v}, \mathbb{G}_m),
\end{array} \tag{6.1.2}$$

where the identifications arise from the adjunction $j_! \dashv j^*$ as in [Mil06, proof of III.0.3 (b)]. To see the commutativity of the bottom part of (6.1.2), we replace $\mathcal{B}[n]$ and $\mathbb{G}_m$ by injective resolutions over $\mathrm{Spec}\, \mathcal{O}_v$, interpret elements of Ext groups as homotopy classes of maps (compare with the proof of Lemma 5.3 for this), and use the adjunction $j_! \dashv j^*$ together with the fact that j^* preserves injectives. To see the commutativity of the upper part, we observe that in the derived category the upper vertical arrows correspond to precomposition with the first morphism of the distinguished triangle

$$i_*\underline{\mathbb{Z}}_{\mathbb{F}_v}[-1] \to j_!\underline{\mathbb{Z}}_{F_v} \to \underline{\mathbb{Z}}_{\mathcal{O}_v} \to i_*\underline{\mathbb{Z}}_{\mathbb{F}_v}.$$

The identification

$$\mathrm{Sel}^2(\mathcal{G}) = H^1(S, \mathcal{B}[n])'$$

results from [Česk16b, 4.4]. □

Remark 6.2. In many cases

$$H^1(S, \mathcal{B}[n])' = H^1(S, \mathcal{B}[n]);$$

for instance, this happens if n is odd or if $B(F_v)$ is connected for every real v (which implies the same for $B^\vee$, cf. [GH81, §1]) because then $H^1(F_v, B[n]) = 0$ for all $v \mid \infty$, as *loc. cit.* proves. We resort to the somewhat artificial $H^1(S, \mathcal{B}[n])'$ to make our duality results apply even when $H^1(F_v, B[n]) \neq 0$ for some $v \mid \infty$.

We turn to the assumptions of §5.7 and note the following common source of suitable θ.

Proposition 6.3. *Let*

$$\theta \colon \mathcal{B}[n]_U \xrightarrow{\sim} \mathcal{B}^\vee[n]_U$$

be the isomorphism induced by a self-dual isogeny $\widetilde{\theta}$ of degree prime to n. Then $H^1(F_v, \theta)$ identifies the subgroup $B(F_v)/nB(F_v)$ with $B^\vee(F_v)/nB^\vee(F_v)$ for all v and identifies the subgroup $H^1(\mathcal{O}_v, \mathcal{B}[n])$ with $H^1(\mathcal{O}_v, \mathcal{B}^\vee[n])$ for all $v \nmid \infty$. □

To address the remaining assumptions of §5.7, we first construct the quadratic forms q_v.

6.4. Suitable quadratic forms q_v. Suppose that the assumptions of Proposition 6.1 (b) are met and that there is a self-dual isogeny

$$\widetilde{\theta}' \colon B \to B^\vee$$

of degree prime to n. Consider the self-dual isogeny

$$\widetilde{\theta} := \begin{cases} 2\widetilde{\theta}', & \text{if } n \text{ is odd}, \\ \widetilde{\theta}', & \text{if } n \text{ is even}, \end{cases}$$

which also has degree prime to n. Due to [PR12, Rem. 4.5], the self-dual isogeny $\lambda := n\widetilde{\theta}$ comes from a symmetric line bundle $\mathscr{L}$ on B, so the results of [PR12, §4] apply. In particular, for $v \notin U$, we can use the pullback $\mathscr{L}_v$ of $\mathscr{L}$ to B_{F_v} to define the quadratic form

$$q_v\colon H^1(F_v, B[n]) \hookrightarrow H^1(F_v, B[\lambda]) \xrightarrow{-\widetilde{q}_v} H^2(F_v, \mathbb{G}_m) \overset{\mathrm{inv}_v}{\hookrightarrow} \mathbb{Q}/\mathbb{Z},$$

where $\widetilde{q}_v\colon H^1(F_v, B[\lambda]) \to H^2(F_v, \mathbb{G}_m)$ is the quadratic form provided by [PR12, Cor. 4.7].

Proposition 6.5. *Assume the setup of §6.4.*

(a) *The bilinear pairing associated to q_v is the $\langle\ ,\ \rangle_v$ of (5.7.1) with θ supplied by Proposition 6.3.*

(b) *We have $q_v(B(F_v)/nB(F_v)) = 0$ for every $v \notin U$.*

(c) *We have $\sum_{v\notin U} q_v(x_v) = 0$ for every $x \in H^1(U, \mathcal{B}[n])$ with pullbacks $x_v \in H^1(F_v, B[n])$.*

(d) *We have $q_v(H^1(\mathcal{O}_v, \mathcal{B}[n])) = 0$ for every $v \in S\backslash U$ for which*

  (i) if $\operatorname{char} \mathbb{F}_v \mid n$, then B has semiabelian reduction at v, and

  (ii) if n is even, then the local Tamagawa factor $\#\Phi_v(\mathbb{F}_v)$ is odd (here $\Phi_v = \mathcal{B}_{\mathbb{F}_v}/\mathcal{B}^0_{\mathbb{F}_v}$).

In particular, if (i) and (ii) hold for every $v \in S\backslash U$, then the q_v meet the assumptions of §5.7.

Proof.

(a) By [PR12, Cor. 4.7], the bilinear pairing associated to q_v is the restriction to $H^1(F_v, B[n])$ of the cup product pairing

$$H^1(F_v, B[\lambda]) \times H^1(F_v, B[\lambda]) \to \mathbb{Q}/\mathbb{Z}$$

that uses Cartier duality

$$b_{B[\lambda]}\colon B[\lambda] \times B[\lambda] \to \mathbb{G}_m.$$

Due to the naturality of the cup product, it remains to show that the diagram

$$\begin{array}{ccc} B[n] \times B[n] & \xrightarrow{\mathrm{id} \times \theta_F} & B[n] \times B^\vee[n] \\ \downarrow & & \downarrow b_F \\ B[\lambda] \times B[\lambda] & \xrightarrow{b_{B[\lambda]}} & \mathbb{G}_m \end{array}$$

commutes. For this, apply [Oda69, Cor. 1.3 (ii)] with $\alpha = \mathrm{id}_B$, $\beta = \widetilde{\theta}$, $\lambda = [n]_B$, and $\lambda' = \lambda$.

(b) This follows from [PR12, Prop. 4.9] because the inclusion

$$H^1(F_v, B[n]) \hookrightarrow H^1(F_v, B[\lambda])$$

maps the subgroup $B(F_v)/nB(F_v)$ into $B^\vee(F_v)/\lambda B(F_v)$ via the homomorphism induced by θ.

(c) By [Čes16b, 4.2 and 2.5 (d)], for every

$$x \in H^1(U, \mathcal{B}[n]) \subset H^1(F, B[\lambda])$$

and every $v \in U$ one has

$$x_v \in B(F_v)/nB(F_v) \subset B^\vee(F_v)/\lambda B(F_v).$$

Therefore, [PR12, Thm. 4.14 (a)] gives the claim.

(d) Set $n' := n$ if n is odd, and $n' := \#\Phi_v(\mathbb{F}_v)$ if n is even. By [Čes16b, 2.5 (a)],

$$n'x \in B(F_v)/nB(F_v) \quad \text{for every} \quad x \in H^1(\mathcal{O}_v, \mathcal{B}[n]).$$

Thus, (b) gives $n'^2 q_v(x) = 0$. On the other hand, $\langle\ ,\ \rangle_v$ vanishes on $H^1(\mathcal{O}_v, \mathcal{B}[n])$ due to (a) and §5.7 via Proposition 6.3, so $2q_v(x) = \langle x, x\rangle_v = 0$. Since n' is odd, we get $q_v(x) = 0$. □

We are ready for the arithmetic duality result that will be used in the proof of Theorem 1.4.

Theorem 6.6. *Fix an $n \in \mathbb{Z}_{\geqslant 1}$, let B be an abelian variety over a global field F, and let $\mathcal{B} \to S$ be its global Néron model. For $v \nmid \infty$, let Φ_v denote the component group scheme of $\mathcal{B}_{\mathbb{F}_v}$. Suppose that*

(i) *B has a self-dual isogeny $\widetilde{\theta}'$ of degree prime to n,*

(ii) *B has semiabelian reduction at every nonarchimedean place v of F with $\operatorname{char}\mathbb{F}_v \mid n$, and*

(iii) *if n is even, then $\#\Phi_v(\mathbb{F}_v)$ is odd for every nonarchimedean v.*

Let

$$H^1(S, \mathcal{B}[n])' \subset H^1(S, \mathcal{B}[n])$$

be the subgroup of the elements whose restrictions to every $H^1(F_v, B[n])$ with $v \mid \infty$ lie in $B(F_v)/nB(F_v)$ (see Remark 6.2 for some cases when $H^1(S, \mathcal{B}[n])' = H^1(S, \mathcal{B}[n])$). Then

$$\frac{\#\operatorname{Sel}_n B}{\#H^1(S, \mathcal{B}[n])'} \equiv \prod_{v \nmid \infty} \frac{\#\Phi_v(\mathbb{F}_v)}{\#(n\Phi_v)(\mathbb{F}_v)} \bmod \mathbb{Q}^{\times 2}.$$

Proof. By [Čes16b, 2.5 (a)],

$$\#\left(\frac{B(F_v)/nB(F_v)}{H^1(\mathcal{O}_v, \mathcal{B}[n]) \cap (B(F_v)/nB(F_v))}\right) = \frac{\#\Phi_v(\mathbb{F}_v)}{\#(n\Phi_v)(\mathbb{F}_v)} \qquad \text{for } v \nmid \infty.$$

Thus, the claim results from Theorem 5.9, which applies due to Propositions 6.1, 6.3 and 6.5. □

Remark 6.7. Since Theorem 5.9 is general, one would remove the assumption (iii) from Theorem 6.6 by proving Proposition 6.5 (d) without its assumption (ii). This would also remove the additional assumption in the $\ell = 2$ case from Theorem 1.4.

7. The proof of Theorem 1.4

The goal of this section is to prove the following mild generalization of Theorem 1.4.

Theorem 7.1. *Let K be a global field of positive characteristic, let $\mathbb{F}_q$ be its field of constants, let $\ell \nmid q$ be a prime, and let A be an abelian variety over K. Suppose that $A_{K\overline{\mathbb{F}}_q}$ has a polarization of degree prime to ℓ and, if $\ell = 2$, that the orders of the component groups of all the reductions of $A_{K\overline{\mathbb{F}}_q}$ are odd. Then the ℓ-parity conjecture holds for $A_{K\mathbb{F}_{q^2}}$, i.e.,*

$$(-1)^{\operatorname{rk}_\ell(A_{K\mathbb{F}_{q^2}})} = w(A_{K\mathbb{F}_{q^2}}).$$

Proof. We let S be the connected smooth proper curve over $\mathbb{F}_q$ having K as its function field, we let $\mathcal{A} \to S$ and $\mathcal{A}^\vee \to S$ be the Néron models of A and $A^\vee$, and, for a variable closed point $v \in S$ (identified with the corresponding place v of K), we let Φ_v denote the component group $\mathcal{A}_{\mathbb{F}_v}/\mathcal{A}^0_{\mathbb{F}_v}$ of the reduction $\mathcal{A}_{\mathbb{F}_v}$ of A_{K_v}.

By Corollary 4.6, for every even n we have

$$w(A_{K\mathbb{F}_{q^n}}) = w(A_{K\mathbb{F}_{q^2}}). \tag{7.1.1}$$

We claim that for every even n we also have

$$\mathrm{rk}_\ell(A_{K\mathbb{F}_{q^n}}) \equiv \mathrm{rk}_\ell(A_{K\mathbb{F}_{q^2}}) \bmod 2. \tag{7.1.2}$$

Indeed, with the notation $\mathcal{X}_\ell(-)$ of §2, Theorem 2.2 ensures that for every 1-dimensional character χ of $\mathrm{Gal}(K\mathbb{F}_{q^n}/K)$, the χ-isotypical and the χ^{-1}-isotypical components of $\mathcal{X}_\ell(A_{K\mathbb{F}_{q^n}}) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$ have the same dimension. Therefore, the sum over all χ with $\chi^2 \neq 1$ of the χ-isotypical components is even dimensional, whereas, by Lemma 2.4, the sum over all χ with $\chi^2 = 1$ of such components is $\mathcal{X}_\ell(A_{K\mathbb{F}_{q^2}}) \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell$. The claimed congruence (7.1.2) follows.

The combination of (7.1.1) and (7.1.2) allows us to replace K by any $K\mathbb{F}_{q^n}$ with n even, so we loose no generality by assuming that A has a polarization of degree prime to ℓ, that the $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$-action on $H^1_{\text{ét}}(S_{\overline{\mathbb{F}}_q}, \mathcal{A}[\ell])$ is trivial, and that $\Phi_v(\mathbb{F}_v) = \Phi_v(\overline{\mathbb{F}}_v)$ for every place v of K.

By Corollary 3.5,

$$\mathrm{rk}_\ell(A_{K\mathbb{F}_{q^2}}) \equiv \dim_{\mathbb{F}_\ell}(\mathrm{Sel}_\ell(A_{K\mathbb{F}_{q^2}})) - \dim_{\mathbb{F}_\ell}(A[\ell](K\mathbb{F}_{q^2})) \bmod 2. \tag{7.1.3}$$

By Corollary 4.6,

$$w(A_{K\mathbb{F}_{q^2}}) = (-1)^{\sum_{v \text{ inert in } K\mathbb{F}_{q^2}} a(A_{K_v})}, \tag{7.1.4}$$

so our task becomes to compare the right sides of (7.1.3) and (7.1.4). We first use Lemma 4.2 to get

$$\textstyle\sum_{v \text{ inert in } K\mathbb{F}_{q^2}} a(A_{K_v}) = \sum_{v \text{ inert in } K\mathbb{F}_{q^2}} a(A[\ell]_{K_v}) + \sum_{v \text{ inert in } K\mathbb{F}_{q^2}} \dim_{\mathbb{F}_\ell}(\Phi_v[\ell](\mathbb{F}_v)). \tag{7.1.5}$$

A place v of K splits in $K\mathbb{F}_{q^2}$ if and only if the number of closed points of $S_{\overline{\mathbb{F}}_q}$ above the closed point of S determined by v is even. Therefore, the Grothendieck–Ogg–Shafarevich formula [Ray65, Thm. 1 (with (1 ter))] applied to $\mathcal{A}[l]_{\overline{\mathbb{F}}_q}$ (which is the Néron model of its generic fiber, cf. [Čes16b, B.6]) gives the congruence

$$\textstyle\sum_{v \text{ inert in } K\mathbb{F}_{q^2}} a(A[\ell]_{K_v}) \equiv \sum_{i=0}^{2} \dim_{\mathbb{F}_\ell}(H^i_{\text{ét}}(S_{\overline{\mathbb{F}}_q}, \mathcal{A}[\ell])) \quad \bmod 2. \tag{7.1.6}$$

Let $j\colon U \hookrightarrow S_{\overline{\mathbb{F}}_q}$ be a nonempty open subscheme for which $\mathcal{A}_U$ is an abelian scheme, so that $\mathcal{A}[\ell]_U$ and $\mathcal{A}^\vee[\ell]_U$ are Cartier dual by [Oda69, Thm. 1.1]. The Néron property ensures that

$$j_*(\mathcal{A}[\ell]_U) \cong \mathcal{A}[\ell]_{S_{\overline{\mathbb{F}}_q}} \qquad \text{and} \qquad j_*(\mathcal{A}^\vee[\ell]_U) \cong \mathcal{A}^\vee[\ell]_{S_{\overline{\mathbb{F}}_q}}$$

on the small étale site of $S_{\overline{\mathbb{F}}_q}$. Therefore, [Mil80, V.2.2 (b)] supplies the duality isomorphism

$$H^2(S_{\overline{\mathbb{F}}_q}, \mathcal{A}[\ell])^* \cong A^\vee[\ell](K\overline{\mathbb{F}}_q).$$

Since, in addition, a polarization of degree prime to ℓ gives an isomorphism

$$A^\vee[\ell](K\overline{\mathbb{F}}_q) \simeq A[\ell](K\overline{\mathbb{F}}_q),$$

the congruence (7.1.6) becomes

$$\textstyle\sum_{v \text{ inert in } K\mathbb{F}_{q^2}} a(A[\ell]_{K_v}) \equiv \dim_{\mathbb{F}_\ell}(H^1_{\text{ét}}(S_{\overline{\mathbb{F}}_q}, \mathcal{A}[\ell])) \quad \bmod 2. \tag{7.1.7}$$

We wish to express $\dim_{\mathbb{F}_\ell}(H^1_{\text{ét}}(S_{\overline{\mathbb{F}}_q}, \mathcal{A}[\ell]))$ in terms of cohomology over $S_{\mathbb{F}_{q^2}}$, so we use the Hochschild–Serre spectral sequence

$$E_2^{ij} = H^i(\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^2}), H^j_{\text{ét}}(S_{\overline{\mathbb{F}}_q}, \mathcal{A}[\ell])) \Rightarrow H^{i+j}_{\text{ét}}(S_{\mathbb{F}_{q^2}}, \mathcal{A}[\ell]),$$

which degenerates on the E_2-page because $\mathbb{F}_{q^2}$ has cohomological dimension 1. The resulting short exact sequence

$$0 \to H^1(\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^2}), A[\ell](K\overline{\mathbb{F}}_q)) \to H^1_{\text{ét}}(S_{\mathbb{F}_{q^2}}, \mathcal{A}[\ell]) \to H^1_{\text{ét}}(S_{\overline{\mathbb{F}}_q}, \mathcal{A}[\ell]) \to 0$$

together with the equalities

$$\dim_{\mathbb{F}_\ell}(H^1(\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^2}), A[\ell](K\overline{\mathbb{F}}_q))) = \dim_{\mathbb{F}_\ell}(H^0(\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_{q^2}), A[\ell](K\overline{\mathbb{F}}_q))) = \dim_{\mathbb{F}_\ell}(A[\ell](K\mathbb{F}_{q^2}))$$

shows that

$$\dim_{\mathbb{F}_\ell}(H^1_{\text{ét}}(S_{\overline{\mathbb{F}}_q}, \mathcal{A}[\ell])) = \dim_{\mathbb{F}_\ell}(H^1_{\text{ét}}(S_{\mathbb{F}_{q^2}}, \mathcal{A}[\ell])) - \dim_{\mathbb{F}_\ell}(A[\ell](K\mathbb{F}_{q^2})).$$

Therefore, by combining this with (7.1.3)–(7.1.7), we find that our task is to prove that

$$\dim_{\mathbb{F}_\ell}(\mathrm{Sel}_\ell(A_{K\mathbb{F}_{q^2}})) \equiv \dim_{\mathbb{F}_\ell}(H^1_{\text{ét}}(S_{\mathbb{F}_{q^2}}, \mathcal{A}[\ell])) + \textstyle\sum_{v \text{ inert in } K\mathbb{F}_{q^2}} \dim_{\mathbb{F}_\ell}(\Phi_v[\ell](\mathbb{F}_v)) \mod 2.$$

However, given our assumptions, this congruence is a special case of Theorem 6.6. □

References

[Čes15] Kęstutis Česnavičius, *Topology on cohomology of local fields*, Forum Math. Sigma **3** (2015), e16, 55, DOI 10.1017/fms.2015.18.

[Čes16a] Kęstutis Česnavičius, *Local factors valued in normal domains*, Int. J. Number Theory **12** (2016), no. 1, 249–272, DOI 10.1142/S1793042116500159. MR3455278

[Čes16b] ———, *Selmer groups as flat cohomology groups*, J. Ramanujan Math. Soc. **31** (2016), no. 1, 31–61. MR3476233

[Čes16c] ———, *The p-parity conjecture for elliptic curves with a p-isogeny*, J. Reine Angew. Math. **719** (2016), 45–73, DOI 10.1515/crelle-2014-0040. MR3552491

[Čes17] ———, *p-Selmer growth in extensions of degree p*, J. Lond. Math. Soc. (2) **95** (2017), no. 3, 833–852, DOI 10.1112/jlms.12038.

[CFKS10] John Coates, Takako Fukaya, Kazuya Kato, and Ramdorai Sujatha, *Root numbers, Selmer groups, and non-commutative Iwasawa theory*, J. Algebraic Geom. **19** (2010), no. 1, 19–97, DOI 10.1090/S1056-3911-09-00504-9. MR2551757 (2011a:11127)

[Dav10] A. Davydov, *Twisted automorphisms of group algebras*, Noncommutative structures in mathematics and physics, K. Vlaam. Acad. Belgie Wet. Kunsten (KVAB), Brussels, 2010, pp. 131–150. MR2742735 (2012b:16085)

[Del73] P. Deligne, *Les constantes des équations fonctionnelles des fonctions L*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 501–597. Lecture Notes in Math., Vol. 349 (French). MR0349635 (50 #2128)

[DD08] Tim Dokchitser and Vladimir Dokchitser, *Parity of ranks for elliptic curves with a cyclic isogeny*, J. Number Theory **128** (2008), no. 3, 662–679, DOI 10.1016/j.jnt.2007.02.008. MR2389862 (2009c:11079)

[DD09a] ———, *Regulator constants and the parity conjecture*, Invent. Math. **178** (2009), no. 1, 23–71, DOI 10.1007/s00222-009-0193-7. MR2534092 (2010j:11089)

[DD09b] ———, *Self-duality of Selmer groups*, Math. Proc. Cambridge Philos. Soc. **146** (2009), no. 2, 257–267, DOI 10.1017/S0305004108001989. MR2475965 (2010a:11219)

[DD10] ———, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Ann. of Math. (2) **172** (2010), no. 1, 567–596, DOI 10.4007/annals.2010.172.567. MR2680426 (2011h:11069)

[DD11] ———, *Root numbers and parity of ranks of elliptic curves*, J. reine angew. Math. **658** (2011), 39–64, DOI 10.1515/CRELLE.2011.060. MR2831512

[GA09] Cristian D. González-Avilés, *Arithmetic duality theorems for 1-motives over function fields*, J. reine angew. Math. **632** (2009), 203–231, DOI 10.1515/CRELLE.2009.055. MR2544149 (2010i:11169)

[GH70] J. Gamst and K. Hoechsmann, *Products in sheaf-cohomology*, Tôhoku Math. J. (2) **22** (1970), 143–162. MR0289605 (44 #6793)

[GH71] ———, *Ext-products and edge-morphisms*, Tôhoku Math. J. (2) **23** (1971), 581–588. MR0302741 (46 #1884)

[GH81] Benedict H. Gross and Joe Harris, *Real algebraic curves*, Ann. Sci. École Norm. Sup. (4) **14** (1981), no. 2, 157–182. MR631748 (83a:14028)

[HR79] Edwin Hewitt and Kenneth A. Ross, *Abstract harmonic analysis. Vol. I*, 2nd ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 115, Springer-Verlag, Berlin, 1979. Structure of topological groups, integration theory, group representations. MR551496 (81k:43001)

[HS05] David Harari and Tamás Szamuely, *Arithmetic duality theorems for 1-motives*, J. reine angew. Math. **578** (2005), 93–128, DOI 10.1515/crll.2005.2005.578.93. MR2113891 (2006f:14053)

[HS05e] ———, *Corrigenda for: Arithmetic duality theorems for 1-motives [MR 2113891]*, J. reine angew. Math. **632** (2009), 233–236, DOI 10.1515/CRELLE.2009.056. MR2544150 (2010i:14079)

[Kim07] Byoung Du Kim, *The parity conjecture for elliptic curves at supersingular reduction primes*, Compos. Math. **143** (2007), no. 1, 47–72, DOI 10.1112/S0010437X06002569. MR2295194 (2007k:11091)

[Kis04] H. Kisilevsky, *Rank determines semi-stable conductor*, J. Number Theory **104** (2004), no. 2, 279–286, DOI 10.1016/S0022-314X(03)00157-4. MR2029506 (2005h:11137)

[KMR13] Zev Klagsbrun, Barry Mazur, and Karl Rubin, *Disparity in Selmer ranks of quadratic twists of elliptic curves*, Ann. of Math. (2) **178** (2013), no. 1, 287–320, DOI 10.4007/annals.2013.178.1.5. MR3043582

[McC86] William G. McCallum, *Duality theorems for Néron models*, Duke Math. J. **53** (1986), no. 4, 1093–1124, DOI 10.1215/S0012-7094-86-05354-8. MR874683 (88c:14062)

[Mil80] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980. MR559531 (81j:14002)

[Mil06] J. S. Milne, *Arithmetic duality theorems*, 2nd ed., BookSurge, LLC, Charleston, SC, 2006. MR2261462 (2007e:14029)

[Mon96] P. Monsky, *Generalizing the Birch-Stephens theorem. I. Modular curves*, Math. Z. **221** (1996), no. 3, 415–420, DOI 10.1007/PL00004518. MR1381589 (97a:11103)

[Mor15] Adam Morgan, 2-*Selmer parity for hyperelliptic curves in quadratic extensions*, preprint (2015). Available at http://arxiv.org/abs/1504.01960.

[MR07] Barry Mazur and Karl Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), no. 2, 579–612, DOI 10.4007/annals.2007.166.579. MR2373150 (2009a:11127)

[Nek06] Jan Nekovář, *Selmer complexes*, Astérisque **310** (2006), viii+559 (English, with English and French summaries). MR2333680 (2009c:11176)

[Nek13] ———, *Some consequences of a formula of Mazur and Rubin for arithmetic local constants*, Algebra Number Theory **7** (2013), no. 5, 1101–1120, DOI 10.2140/ant.2013.7.1101. MR3101073

[Nek15] ———, *Compatibility of arithmetic and algebraic local constants (the case $\ell \neq p$)*, Compos. Math. **151** (2015), no. 9, 1626–1646, DOI 10.1112/S0010437X14008069. MR3406439

[Nek16] ———, *Compatibility of arithmetic and algebraic local constants II. The tame abelian potentially Barsotti-Tate case.*, preprint (2016). Available at https://webusers.imj-prg.fr/~jan.nekovar/pu/tame.pdf.

[Oda69] Tadao Oda, *The first de Rham cohomology group and Dieudonné modules*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 63–135. MR0241435 (39 #2775)

[PR12] Bjorn Poonen and Eric Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), no. 1, 245–269, DOI 10.1090/S0894-0347-2011-00710-8. MR2833483

[PS99] Bjorn Poonen and Michael Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149, DOI 10.2307/121064. MR1740984 (2000m:11048)

[Ray65] Michel Raynaud, *Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, pp. Exp. No. 286, 129–147 (French). MR1608794

[Sab07] Maria Sabitova, *Root numbers of abelian varieties*, Trans. Amer. Math. Soc. **359** (2007), no. 9, 4259–4284 (electronic), DOI 10.1090/S0002-9947-07-04148-7. MR2309184 (2008c:11090)

[Ser67] J.-P. Serre, *Local class field theory*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 128–161. MR0220701 (36 #3753)

[Ser70] Jean-Pierre Serre, *Facteurs locaux des fonctions zêta des variétés algébriques (définitions et conjectures)*, Séminaire Delange-Pisot-Poitou. 11e année: 1969/70. Théorie des nombres. Fasc. 1: Exposés 1 à 15; Fasc. 2: Exposés 16 à 24, Secrétariat Mathématique, 1970, pp. 19-01–19-15. MR0401396 (53 #5224)

[Ser77] ———, *Linear representations of finite groups*, Springer-Verlag, New York, 1977. Translated from the second French edition by Leonard L. Scott; Graduate Texts in Mathematics, Vol. 42. MR0450380 (56 #8675)

[Sha64] Stephen S. Shatz, *Cohomology of artinian group schemes over local fields*, Ann. of Math. (2) **79** (1964), 411–449. MR0193093 (33 #1314)

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. MR0236190 (38 #4488)

[TW11] Fabien Trihan and Christian Wuthrich, *Parity conjectures for elliptic curves over global fields of positive characteristic*, Compos. Math. **147** (2011), no. 4, 1105–1128, DOI 10.1112/S0010437X1100532X. MR2822863 (2012j:11134)

[TY14] Fabien Trihan and Seidai Yasuda, *The ℓ-parity conjecture for abelian varieties over function fields of characteristic $p > 0$*, Compos. Math. **150** (2014), no. 4, 507–522, DOI 10.1112/S0010437X13007501. MR3200666