Algebra & Number Theory

Volume 7

2013

No. 5

Some consequences of a formula of Mazur and Rubin for arithmetic local constants

Jan Nekovář

msp

ALGEBRA AND NUMBER THEORY 7:5 (2013)
dx.doi.org/10.2140/ant.2013.7.1101

Some consequences of a formula of Mazur and Rubin for arithmetic local constants

Jan Nekovář

We prove a very general case of the parity conjecture for Selmer groups of elliptic curves over totally real fields, as well as slightly less general results for classical modular forms, Hilbert modular forms of parallel weight two and for abelian varieties with real multiplication.

The main results of this article are the following two instances of the parity conjecture for Selmer groups (see [Nekovář 2006, Section 12.1] for a general discussion of this conjecture). Along the way we also prove slightly weaker results for Hilbert modular forms of parallel weight two with trivial character (Theorems 1.4 and 3.5) and for abelian varieties with real multiplication (Theorem 4.3).

Theorem A. *Let E be an elliptic curve over a totally real number field F and let p be a prime number. The p-Selmer rank of E over F*

$$s_p(E/F) := \mathrm{rk}_{\mathbb{Z}}\, E(F) + \mathrm{cork}_{\mathbb{Z}_p}\, Ш(E/F)[p^\infty]$$

(*which is also equal to the dimension* $\dim_{\mathbb{Q}_p} H^1_f(F, V_p(E))$ *of the Bloch–Kato Selmer group* [Bloch and Kato 1990, Definition 5.1] *of the Galois representation* $V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ *over* F) *and the analytic rank of E over F*

$$r_{\mathrm{an}}(E/F) := \mathrm{ord}_{s=1}\, L(E/F, s)$$

satisfy

$$s_p(E/F) \equiv r_{\mathrm{an}}(E/F) \pmod 2$$

in each of the following cases:

(1) *E does not have complex multiplication*,

(2) *E has complex multiplication and $2 \nmid [F : \mathbb{Q}]$, and*

(3) *E has complex multiplication by an imaginary quadratic field K' and p splits in $K'/\mathbb{Q}$.*

MSC2010: 11G40.
Keywords: Selmer groups, parity, elliptic curves, modular forms.

Note that potential modularity of E [Wintenberger 2009, Theorem A.1] implies that the L-function $L(E/F, s)$ has a meromorphic continuation to $\mathbb{C}$ and satisfies the expected functional equation [Taylor 2002, proof of Corollary 2.2; Nekovář 2006, 12.11.6]. As a result, the integer $\mathrm{ord}_{s=1} L(E/F, s) \in \mathbb{Z}$ is well defined.

Various special cases of Theorem A (for $F \neq \mathbb{Q}$) were proved in [Nekovář 2006; Kim 2009; Nekovář 2009].

If the p-primary part of $Ш(E/F)$ is finite for some prime number p, then $s_p(E/F) = \mathrm{rk}_{\mathbb{Z}} E(F)$ and the statement of Theorem A is the conjecture of Birch and Swinnerton-Dyer for E over F modulo 2.

Theorem B. *Let $g = \sum_{n=1}^{\infty} a_n q^n \in S_{2r}(\Gamma_0(N))$ for $r \geq 1$ be a normalised $(a_1 = 1)$ newform, and let $L = \mathbb{Q}(a_1, a_2, \ldots)$ be the (totally real) number field generated by its coefficients. For any prime $\mathfrak{p}$ of L above a rational prime $p \neq 2$, denote by $V_{\mathfrak{p}}(g)$ the two-dimensional representation of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ over $L_{\mathfrak{p}}$ attached to g:*

$$\det(1 - X\,\mathrm{Fr}_{\mathrm{geom}}(l) \mid V_{\mathfrak{p}}(g)) = 1 - a_l X + l^{2r-1} X^2, \quad \textit{for all } l \nmid pN.$$

In the case when $r > 1$, assume that the residual representation of $V_{\mathfrak{p}}(g)$ is irreducible. Then

$$\dim_{L_{\mathfrak{p}}} H^1_f(\mathbb{Q}, V_{\mathfrak{p}}(g)(r)) \equiv \mathrm{ord}_{s=r} L(g, s) \pmod 2.$$

If g is (the newform associated to) a twist of a p-ordinary eigenform, Theorem B was proved in [Nekovář 2006, Theorem 12.2.3], even for $p = 2$ and without the assumption on the residual representation.

The proofs of Theorems A and B combine the techniques developed in [Nekovář 2001; 2006; 2007a; 2007b; 2008; 2009] and [Aflalo and Nekovář 2010] — namely, a combination of suitable relative parity results involving two Selmer groups with an Euler system argument [Nekovář 2007a] applied to a nontrivial Euler system [Cornut and Vatsal 2007; Aflalo and Nekovář 2010] — with a formula of Mazur and Rubin [2007, Theorem 1.4]. This formula expresses the difference of the parities of ranks of Selmer groups corresponding to two self-dual Selmer structures on a given finite (self-dual) Galois module as a finite sum of terms depending on purely local data at a finite set of (finite) primes. In a motivic setting, when the two Selmer structures are obtained by propagation from the Bloch–Kato Selmer structures for two self-dual geometric Galois representations that are congruent modulo a prime ideal dividing p, these local terms are expected to mirror the local ε-factors of the corresponding L-functions. Unfortunately, such a relation to ε-factors remains conjectural (in the required generality) even in the fairly simple situation relevant to us, when the two Galois representations come from two congruent Hilbert modular forms of parallel weight (as in Section 3). This means that we do not have at our disposal appropriate relative parity results in the generality we desire. To get around this problem we apply the formula of Mazur and Rubin in two different global situations for which the local data agree. We obtain a "birelative" global result (Theorem 2.2) for the parities of ranks of four different Selmer groups. If we are able to control three of them (in our case, Theorem 1.4 applies to two of them and the auxiliary global situation is chosen in such a way that the third Selmer group is trivial, by an application of another Euler system argument [Kato 2004; Nekovář 2012]), the sought-for parity result for the remaining Selmer group follows. Note that the formula of Mazur and Rubin is used in the proofs of both Theorems 1.1 (on which Theorem 1.4 relies) and 2.2. This program is carried out for Hilbert modular forms in Section 3; the results for abelian varieties with real multiplication are deduced in Section 4. The assumptions on E in Theorem A come from an application of [Nekovář 2012, corollary of Theorem B′].

Notation and conventions

All representations (in particular, characters) of various Galois groups are assumed to be continuous. Given a number field F, a choice of an embedding $\overline{F} \hookrightarrow \overline{F}_v$, for each prime v of F, identifies $G_{F_v} = \mathrm{Gal}(\overline{F}_v/F_v)$ with a subgroup of $G_F = \mathrm{Gal}(\overline{F}/F)$. For each representation V of G_F, we denote by V_v its restriction to G_{F_v}. Denote by S_∞ the set of all archimedean primes of F, and by S_p the set of all primes above a rational prime p of F. For any $R[G]$-module M and a character $\chi : G \to R^\times$ we denote by $M^{(\chi)} = \{m \in M \mid g(m) = \chi(g)m \text{ for all } g \in G\}$ the χ-eigenspace for the action of G on M.

1. A parity result for Hilbert modular forms of parallel weight two

Theorem 1.1 (an abstract cohomological version of the case $\mathfrak{S} = \varnothing$ of [Mazur and Rubin 2007, Theorem 7.1]). *Let F be a number field, and let V be a geometric representation* (*in the sense of Fontaine and Mazur*) *of G_F with coefficients in a finite extension $\mathcal{K}$ of $\mathbb{Q}_p$, where $p \neq 2$. Assume that*

(1) *there exists a nondegenerate skew-symmetric G_F-equivariant bilinear pairing $\langle \cdot , \cdot \rangle : V \times V \to \mathcal{K}(1)$ and*

(2) *after possibly multiplying $\langle \cdot , \cdot \rangle$ by an element of $\mathcal{K}^\times$, there exists a G_F-stable $\mathbb{O}_{\mathcal{K}}$-lattice $T \subset V$ that is self-dual* (*that is, for which the rescaled pairing defines an isomorphism $T \xrightarrow{\sim} T^*(1)$*). (*This is automatic if* $\dim_{\mathcal{K}}(V) = 2$, *for any T.*)

Let K/F be a quadratic extension, and let K' be a cyclic extension of K of p-power order, dihedral over F. Assume that no finite prime of K stable under $\mathrm{Gal}(K/F)$

ramifies in K'/K. Then, for each character $\chi : \mathrm{Gal}(K'/K) \to \mathcal{K}^\times$,

$$\dim_{\mathcal{K}} H^1_f(K', V)^{(\chi^{\pm 1})} - \dim_{\mathcal{K}} H^0(K', V)^{(\chi^{\pm 1})} \equiv \dim_{\mathcal{K}} H^1_f(K, V) - \dim_{\mathcal{K}} H^0(K, V) \pmod 2.$$

Proof. Fix a finite set S of primes of F containing $S_\infty \cup S_p$ such that V is unramified outside S. Fix a uniformiser $t \in \mathbb{O} = \mathbb{O}_{\mathcal{K}}$ and denote by $k = \mathbb{O}/t\mathbb{O}$ the residue field of $\mathcal{K}$. The $\mathcal{K}$-subspaces $H^1_f(F_v, V) \subset H^1(F_v, V)$ for $v \notin S_\infty$ define, by propagation [Mazur and Rubin 2004, Example 1.1.2], a Selmer structure $H^1_f(F_v, X) \subset H^1(F_v, X)$ on each $X = T,\ V/T,\ T/t^nT,\ \overline{T} = T/tT$, which is cartesian on $\{T/t^nT\}_{n \le \infty}$ [Mazur and Rubin 2004, Lemma 3.7.1]. The exact sequences

$$0 \to H^0(F, V/T) \otimes_{\mathbb{O}} k \to H^1_f(F, \overline{T}) \to H^1_f(F, V/T)[t] \to 0,$$
$$0 \to H^0(F_v, T) \otimes_{\mathbb{O}} k \to H^0(F_v, \overline{T}) \to H^1_f(F_v, T)[t] \to 0$$

imply that

$$\dim_k H^1_f(F, V/T)[t] - \dim_{\mathcal{K}} H^0(F, V) = \dim_k H^1_f(F, \overline{T}) - \dim_k H^0(F, \overline{T}), \quad (1.1.1)$$

and

$$\dim_k (H^1_f(F_v, \overline{T}) = H^1_f(F_v, T) \otimes_{\mathbb{O}} k) = \dim_k H^0(F_v, \overline{T}) + \dim_{\mathcal{K}} H^1_f(F_v, V) - \dim_{\mathcal{K}} H^0(F_v, V). \quad (1.1.2)$$

So far we have not used the assumptions (1) and (2) of the theorem, but we are going to do it now. The existence of a nondegenerate skew-symmetric bilinear pairing on $H^1_f(F, V/T)/(H^1_f(F, T) \otimes_{\mathbb{O}} \mathcal{K}/\mathbb{O})$ with values in $\mathcal{K}/\mathbb{O}$ constructed in [Flach 1990] (taking into account [Bloch and Kato 1990, Proposition 3.8]) implies that

$$\dim_{\mathcal{K}} H^1_f(F, V) = \mathrm{cork}_{\mathbb{O}}\,(H^1_f(F, T) \otimes_{\mathbb{O}} \mathcal{K}/\mathbb{O}) \equiv \dim_k H^1_f(F, V/T)[t] \pmod 2;$$

we deduce from (1.1.1) that

$$\dim_{\mathcal{K}} H^1_f(F, V) - \dim_{\mathcal{K}} H^0(F, V) \equiv \dim_k H^1_f(F, \overline{T}) - \dim_k H^0(F, \overline{T}) \pmod 2. \quad (1.1.3)$$

The induced representation $\mathrm{Ind}^{\mathrm{Gal}(K'/F)}_{\mathrm{Gal}(K'/K)}(\chi)$ has a natural model $I[\chi]$ (free of rank two) over $\mathbb{O}$, which is equipped with a nondegenerate symmetric G_F-equivariant pairing $I[\chi] \times I[\chi] \to \mathbb{O}$ inducing an isomorphism $I[\chi] \xrightarrow{\sim} I[\chi]^*$. By Shapiro's lemma,

$$\begin{aligned} H^1_f(F, V \otimes I[\chi]) = H^1_f(K, V \otimes \chi) &= (H^1_f(K', V) \otimes \chi)^{\mathrm{Gal}(K'/K)} \\ &= H^1_f(K', V)^{(\chi^{-1})}, \\ H^j(F, V \otimes I[\chi]) = H^j(K, V \otimes \chi) &= H^j(K', V)^{(\chi^{-1})}. \end{aligned}$$

Since $I[\chi] \xrightarrow{\sim} I[\chi^{-1}]$, these groups are respectively isomorphic to $H^1_f(K', V)^{(\chi)}$ and $H^j(K', V)^{(\chi)}$.

The discussion leading to (1.1.1)–(1.1.3) applies to $V \otimes I[\chi]$ and the self-dual lattice $T \otimes_{\mathbb{O}} I[\chi]$. Note there is a canonical identification $\overline{T} \otimes I[\chi] = \overline{T} \otimes I[1]$, where we have denoted by "1" the trivial character of $\mathrm{Gal}(K'/K)$ (this notation, which occurs only in Theorem 1.1 and Lemma 1.2, should not be confused with the Tate twist "(1)"). However, the Selmer structures $H^1_{f,\chi}(F_v, \cdot)$ and $H^1_{f,1}(F_v, \cdot)$ on the G_F-module $\overline{T} \otimes I[\chi] = \overline{T} \otimes I[1]$ obtained by propagation of the subspaces $H^1_f(F_v, V \otimes I[\chi]) \subset H^1(F_v, V \otimes I[\chi])$ and $H^1_f(F_v, V \otimes I[1]) \subset H^1(F_v, V \otimes I[1])$, respectively, are not necessarily the same. The formula [Mazur and Rubin 2007, Theorem 1.4] applies in our case, since both Selmer structures $H^1_{f,\chi}$ and $H^1_{f,1}$ are self-dual, thanks to [Bloch and Kato 1990, Proposition 3.8]; it yields

$$\dim_k H^1_{f,\chi}(F, \overline{T} \otimes I[\chi]) - \dim_k H^1_{f,1}(F, \overline{T} \otimes I[1]) \equiv \sum_{v \in S - S_\infty} \delta_v \pmod 2, \quad (1.1.4)$$

where

$$\delta_v \equiv \dim_k H^1_{f,1}(F, \overline{T} \otimes I[1]) / (H^1_{f,1}(F, \overline{T} \otimes I[1]) \cap H^1_{f,\chi}(F, \overline{T} \otimes I[\chi])) \pmod 2.$$

Combining (1.1.4) with (1.1.3) for $T \otimes_{\mathbb{O}} I[\chi]$ and $T \otimes_{\mathbb{O}} I[1]$, we obtain

$$\chi_f(K, V \otimes \chi) - \chi_f(K, V) \equiv \sum_{v \in S - S_\infty} \delta_v \pmod 2, \quad (1.1.5)$$

where we have put

$$\chi_f(K, W) := \dim_{\mathcal{K}} H^1_f(K, W) - \dim_{\mathcal{K}} H^0(K, W). \quad (1.1.6)$$

To conclude the proof, it remains to prove the following lemma.

Lemma 1.2. *Under the assumptions of Theorem 1.1, we have* $\delta_v \equiv 0 \pmod 2$ *for all* $v \in S - S_\infty$.

Proof. If there is a unique prime $w \mid v$ in K, then χ_w (that is, the restriction of χ to G_{K_w}) is unramified by assumption, and therefore trivial [Mazur and Rubin 2007, Lemma 6.5]. It follows that $I[\chi]_v = I[1]_v$; hence $H^1_{f,\chi}(F_v, \overline{T} \otimes I[\chi]) = H^1_{f,1}(F_v, \overline{T} \otimes I[1])$.

The case when v splits as $v\mathcal{O}_K = ww'$ requires a more detailed argument. In this case $K_w = F_v = K_{w'}$, $I[1]_v = 1 \oplus 1$ and $I[\chi]_v = \chi_w \oplus \chi_w^{-1}$. As

$$\delta_v \equiv \dim_k\left(\frac{Y \oplus Y}{(Y \cap Z_+) \oplus (Y \cap Z_-)}\right) \pmod 2,$$

where

$$Y = \mathrm{Im}(H^1_f(F_v, T) \otimes_{\mathcal{O}} k \hookrightarrow H^1(F_v, \overline{T})),$$
$$Z_\pm = \mathrm{Im}(H^1_f(F_v, T \otimes \chi_w^{\pm 1}) \otimes_{\mathcal{O}} k \hookrightarrow H^1(F_v, \overline{T} \otimes \chi_w^{\pm 1}) = H^1(F_v, \overline{T})),$$

we must show that

$$\dim_k(Y \cap Z_+) \equiv \dim_k(Y \cap Z_-) \pmod 2.$$

Firstly, the local duality

$$H^1(F_v, \overline{T}) \times H^1(F_v, \overline{T}) \to H^2(F_v, k(1)) \xrightarrow{\sim} k$$

is a nondegenerate symmetric bilinear pairing under which $Y^\perp = Y$ and $Z_\pm^\perp = Z_\mp$, by [Bloch and Kato 1990, Proposition 3.8]. Secondly, (1.1.2) applied to $T \otimes \chi_w^{\pm 1}$ yields (since $\overline{T} \otimes \chi_w^{\pm 1} = \overline{T}$)

$$\dim_k(Z_\pm) - \dim_k H^0(F_v, \overline{T}) = \dim_{\mathcal{K}} H^1_f(F_v, V \otimes \chi_w^{\pm 1}) - \dim_{\mathcal{K}} H^0(F_v, V \otimes \chi_w^{\pm 1}).$$

If $v \nmid p$, then the right-hand side is equal to zero, but if $v \mid p$, then it is equal, by [Bloch and Kato 1990, Corollary 3.8.4], to

$$\dim_{\mathcal{K}} D_{dR}(V_v \otimes \chi_w^{\pm 1})/Fil^0 = \dim_{\mathcal{K}} D_{dR}(V_v)/Fil^0,$$

which does not depend on the sign $\pm$. In either case,

$$\dim_k(Z_+) = \dim_k(Z_-) = \tfrac{1}{2} \dim_k H^1(F_v, \overline{T}) = \dim_k(Y)$$

and

$$\begin{aligned} \dim_k(Y \cap Z_+) &= \dim_k(Y) + \dim_k(Z_+) - \dim_k(Y + Z_+) \\ &= \dim_k H^1(F_v, \overline{T}) - \dim_k(Y + Z_+) \\ &= \dim_k(Y + Z_+)^\perp = \dim_k(Y^\perp \cap Z_+^\perp) = \dim_k(Y \cap Z_-), \end{aligned}$$

as required. The lemma (and Theorem 1.1) is proved. □

1.3. If V arises as a subquotient of $H^{2r-1}_{et}(X \otimes_F \overline{F}, \mathcal{K})(r)$ for some proper and smooth scheme X over F, then $H^0(L, V) = 0$ for all finite extensions L/F, by Deligne's proof of Weil's conjectures. Theorem 1.1 in this case states that

$$\dim_{\mathcal{K}} H^1_f(K', V)^{(\chi^{\pm 1})} \equiv \dim_{\mathcal{K}} H^1_f(K, V) \pmod 2. \tag{1.3.1}$$

This remark applies, in particular, to $V = V_{\mathfrak{p}}(g)(r)$ as in Theorem B, and to any subrepresentation of $V_p(A) \otimes_{\mathbb{Q}_p} \mathcal{K}$, where A is an abelian variety over F.

Theorem 1.4 (generalisation of [Nekovář 2009, Theorem 1]). *Let $g \in S_2(\mathfrak{n}, 1)$ be a cuspidal Hilbert modular newform of parallel weight two and trivial character over a totally real number field F. Let L be the (totally real) number field generated by its Hecke eigenvalues $\lambda_v(g)$. For any prime $\mathfrak{p}$ of L above a rational prime $p \neq 2$, denote by $V_{\mathfrak{p}}(g)$ the two-dimensional representation of G_F over $L_{\mathfrak{p}}$ attached to g:*

$$\det(1 - X\,\mathrm{Fr}_{\mathrm{geom}}(v) \mid V_{\mathfrak{p}}(g)) = 1 - \lambda_v(g)X + N(v)X^2, \quad \text{for all } v \nmid p\mathfrak{n}.$$

Assume that at least one of the following three conditions is satisfied:

(a) $2 \nmid [F : \mathbb{Q}]$,

(b) *there exists a nonarchimedean prime of F at which the local component of the automorphic representation $\pi(g)$ of $\mathrm{PGL}_2(\mathbf{A}_F)$ attached to g is a twist of the Steinberg representation, or*

(c) *there exists a nonarchimedean prime v_0 of F at which the local component of $\pi(g)$ is supercuspidal.*

Then

$$\dim_{L_{\mathfrak{p}}} H^1_f(F, V_{\mathfrak{p}}(g)(1)) \equiv r_{\mathrm{an}}(F, g) \pmod 2,$$

where $r_{\mathrm{an}}(F, g) := \mathrm{ord}_{s=1}\, L(g, s)$.

Proof. Assume either (a) or (b). In the case when g corresponds to an elliptic curve defined over F this result was proved in [Nekovář 2009]. The argument there applies in general, with the following modifications: We replace the conductor of E by $\mathfrak{n}$ (the level of g) and use Theorem 1.1 instead of [Mazur and Rubin 2007, Theorem 7.1]. As $V_{\mathfrak{p}}(g)(1)$ arises as a subrepresentation of $V_p(A) \otimes_{\mathbb{Q}_p} L_{\mathfrak{p}}$, where A is the Jacobian of a suitable Shimura curve, (1.3.1) applies in this case.

Now assume (c). Thanks to (a) we can assume that $2 \mid [F : \mathbb{Q}]$. In addition, we can assume, as in [Nekovář 2009, Step 3] (after replacing F by a suitable cyclic extension of odd degree), that there exists a prime $P \mid p$ in F, with $P \neq v_0$. Let K be any totally imaginary quadratic extension of F in which P splits and that satisfies the properties of Lemma 1.5 below (and such that g does not have CM by K). As in [Nekovář 2008, 1.2–1.5] (for $\chi = 1$, $\Sigma = \{P\}$, and $c = 1$), the generalisation of [Cornut and Vatsal 2007, Theorem 4.1] proved in [Aflalo and Nekovář 2010, Theorem 4.3.1] combined with [Nekovář 2007a, Theorem 3.2] implies that there is a finite cyclic subextension K'/K of the ring class field extension $K[P^\infty]/K$ and a character χ of $\mathrm{Gal}(K'/K)$ for which $2 \nmid \dim_{\mathcal{K}} H^1_f(K', V_{\mathfrak{p}}(g)(1))^{(\chi)}$, where

$\mathcal{K} = L_{\mathfrak{p}}(\chi)$. Theorem 1.1 then yields

$$2 \nmid \dim_{L_{\mathfrak{p}}} H^1_f(K, V_{\mathfrak{p}}(g)(1)) \\ = \dim_{L_{\mathfrak{p}}} H^1_f(F, V_{\mathfrak{p}}(g)(1)) + \dim_{L_{\mathfrak{p}}} H^1_f(F, V_{\mathfrak{p}}(g \otimes \alpha)(1)), \qquad (\star)$$

where α is the quadratic character associated to K/F. We can now vary K as in the endgame of [Nekovář 2001]:

If $2 \nmid r_{\mathrm{an}}(F, g)$, then $2 \mid r_{\mathrm{an}}(F, g \otimes \alpha)$ for any α as in Lemma 1.5 below. According to [Waldspurger 1991, Theorem 4] and [Friedberg and Hoffstein 1995, Theorem B.1] there exists such an α satisfying $r_{\mathrm{an}}(F, g \otimes \alpha) = 0$, which implies that $H^1_f(F, V_{\mathfrak{p}}(g \otimes \alpha)(1)) = 0$, by [Nekovář 2012, Theorem B(b)]; thus $2 \nmid \dim_{L_{\mathfrak{p}}} H^1_f(F, V_{\mathfrak{p}}(g)(1))$, by $(\star)$.

If $2 \mid r_{\mathrm{an}}(F, g)$, then $2 \nmid r_{\mathrm{an}}(F, g \otimes \alpha)$ for any α as in Lemma 1.5. The previous argument applies to $g \otimes \alpha$, yielding $2 \nmid \dim_{L_{\mathfrak{p}}} H^1_f(F, V_{\mathfrak{p}}(g \otimes \alpha)(1))$. Applying $(\star)$ again, we obtain $2 \mid \dim_{L_{\mathfrak{p}}} H^1_f(F, V_{\mathfrak{p}}(g)(1))$. □

Lemma 1.5. *Let g be as in Theorem 1.4(c). If $2 \mid [F : \mathbb{Q}]$, then there exists a character $\mu : G_{F_{v_0}} \to \{\pm 1\}$ such that, for any character $\alpha : G_F \to \{\pm 1\}$ satisfying*

$$\alpha_{v_0} = \mu, \qquad \alpha_v = 1 \text{ for all } v \mid \mathfrak{n} \text{ with } v \neq v_0, \quad \alpha_v(-1) = -1 \text{ for all } v \in S_\infty,$$

the corresponding quadratic extension $K = \overline{F}^{\mathrm{Ker}(\alpha)}$ of F is totally imaginary and $2 \nmid r_{\mathrm{an}}(F, g) + r_{\mathrm{an}}(F, g \otimes \alpha)$.

Proof. See [Nekovář 2012, Proposition 2.10.2]. □

2. A relative parity result with a twist

2.1. Assume that V satisfies the assumption (1) of Theorem 1.1. For each nonarchimedean prime v of F we write, as in [Nekovář 2007b, Proposition 2.2.1(1)],

$$\varepsilon_v(V) = \varepsilon_v(V_v) = \varepsilon(WD(V_v), \psi, dx_\psi) \in \{\pm 1\},$$

where ψ is any nontrivial additive character of F_v, where dx_ψ is the corresponding self-dual Haar measure on F_v, and where $WD(V_v)$ is the representation of the Weil–Deligne group of F_v attached to V_v if $v \nmid p$, or to $D_{pst}(V_v)$ if $v \mid p$ (see [Deligne 1973, 8.4; Fontaine 1994; Fontaine and Perrin-Riou 1994, I.1.3.2]).

Theorem 2.2. *Let F and $\mathcal{K}$ be as in Theorem 1.1 (in particular, $p \neq 2$). Let V and V' be geometric representations of G_F with coefficients in $\mathcal{K}$ that satisfy assumptions (1) and (2) of Theorem 1.1. Let $T \subset V$ and $T' \subset V'$ be G_F-stable $\mathbb{O}$-lattices, self-dual with respect to the corresponding pairings $\langle\,\cdot\,,\cdot\,\rangle : T \times T \to \mathbb{O}(1)$ and $\langle\,\cdot\,,\cdot\,\rangle' : T' \times T' \to \mathbb{O}(1)$. Assume that there exists an isomorphism of $k[G_F]$-modules $u : \overline{T}' = T' \otimes_{\mathbb{O}} k \xrightarrow{\sim} \overline{T} = T \otimes_{\mathbb{O}} k$ compatible with the pairings induced by $\langle\,\cdot\,,\cdot\,\rangle$ on $\overline{T}$ and by $\langle\,\cdot\,,\cdot\,\rangle'$ on $\overline{T}'$. Let S be a finite set of primes of F containing $S_\infty \cup S_p$ and* *all primes at which V or V' is ramified. If $\alpha : G_F \to \{\pm 1\}$ is a character such that $\alpha_v = 1$ for all $v \in S - S_\infty$, then* (*using the notation from* (1.1.6)):

$$\chi_f(F, V) - \chi_f(F, V') \equiv \chi_f(F, V \otimes \alpha) - \chi_f(F, V' \otimes \alpha) \pmod 2,$$
$$\varepsilon_v(V)/\varepsilon_v(V') = \varepsilon_v(V \otimes \alpha)/\varepsilon_v(V' \otimes \alpha) \quad \textit{for all } v \notin S_\infty.$$

Proof. As remarked in the course of the proof of Theorem 1.1, the Selmer structure $H^1_f(F_v, \overline{T})$ obtained by propagation of $H^1_f(F_v, V) \subset H^1(F_v, V)$ is self-dual; so is the structure $H^1_{f'}(F_v, \overline{T})$ obtained by propagation of $H^1_f(F_v, V') \subset H^1(F_v, V')$, composed with the isomorphism $H^1(F_v, \overline{T}') \xrightarrow{\sim} H^1(F_v, \overline{T})$ induced by u. Combining [Mazur and Rubin 2007, Theorem 1.4] with (1.1.3) we obtain

$$\begin{aligned} \chi_f(F, V) - \chi_f(F, V') &\equiv \dim_k H^1_f(F, \overline{T}) - \dim_k H^1_{f'}(F, \overline{T}) \\ &\equiv \sum_{v \in S - S_\infty} \delta_v(T_v, T'_v) \pmod 2, \end{aligned} \tag{2.2.1}$$

where

$$\delta_v(T_v, T'_v) \equiv \dim_k H^1_f(F_v, \overline{T})/(H^1_f(F_v, \overline{T}) \cap H^1_{f'}(F, \overline{T})) \pmod 2.$$

Set $S(\alpha) = S \cup \{v \mid \alpha_v \text{ is ramified}\}$. We claim that

$$H^j(F_v, \overline{T} \otimes \alpha) = 0 \quad \text{for all } v \in S(\alpha) - S \text{ and } j = 0, 1, 2. \tag{2.2.2}$$

Indeed, $H^0(F_v, \overline{T} \otimes \alpha) \subset (\overline{T} \otimes \alpha)^{I_v} = 0$ (since $p \neq 2$) and $H^2(F_v, \overline{T} \otimes \alpha) = H^0(F_v, (\overline{T} \otimes \alpha)^*(1))^* = H^0(F_v, \overline{T} \otimes \alpha)^* = 0$, by local duality. Finally, by the local Euler characteristic formula, $H^1(F_v, \overline{T} \otimes \alpha) = 0$.

The pairings $\langle \cdot, \cdot \rangle$ and $\langle \cdot, \cdot \rangle'$ and the isomorphism u induce the same data for $T \otimes \alpha$ and $T' \otimes \alpha$. Applying (2.2.1) to these twisted modules, we obtain

$$\begin{aligned} \chi_f(F, V \otimes \alpha) - \chi_f(F, V' \otimes \alpha) &\equiv \sum_{v \in S(\alpha) - S_\infty} \delta_v((T \otimes \alpha)_v, (T' \otimes \alpha)_v) \\ &\equiv \sum_{v \in S - S_\infty} \delta_v((T \otimes \alpha)_v, (T' \otimes \alpha)_v) \\ &\equiv \sum_{v \in S - S_\infty} \delta_v(T_v, T'_v) \\ &\equiv \chi_f(F, V) - \chi_f(F, V') \pmod 2, \end{aligned}$$

where the second congruence follows from (2.2.2) and the third from the fact that $\alpha_v = 1$ for all $v \in S - S_\infty$.

Let us now prove the statement about local ε-constants. For $v \in S - S_\infty$ there is nothing to prove, as $(W \otimes \alpha)_v = W_v$ (here $W = V, V'$); hence $\varepsilon_v(W \otimes \alpha) = \varepsilon_v(W)$. For $v \notin S(\alpha)$ all four ε-constants are equal to 1. Finally, for $v \in S(\alpha) - S$, $\varepsilon_v(W) = 1$ ($W = V, V'$). It follows from (2.2.2) that $(W \otimes \alpha)^{I_v} = 0$, which implies that

$\varepsilon_v(W\otimes\alpha)=\varepsilon_{0,v}(W\otimes\alpha)$. As the local ε_0-constants at primes not dividing p are compatible with congruences modulo p [Deligne 1973, Theorem 6.5], the isomorphism $\overline{T}'\otimes\alpha \xrightarrow{\sim} \overline{T}\otimes\alpha$ implies that $\varepsilon_v(V\otimes\alpha), \varepsilon_v(V'\otimes\alpha)\in\{\pm1\}$ are congruent modulo p; therefore they are equal to each other. $\square$

2.3. In practice, we are often given a slightly different set of data:

2.3.1 representations V and V' that satisfy the assumption (1) of Theorem 1.1;

2.3.2 a G_F-stable $\mathbb{O}$-lattice $T\subset V$, self-dual with respect to $\langle\,\cdot\,,\cdot\,\rangle : T\times T\to\mathbb{O}(1)$,

2.3.3 for which $\overline{T}=T\otimes_{\mathbb{O}}k$ is an absolutely irreducible representation of G_F, and

2.3.4 a dense set of elements $g\in G_F$ for which $\mathrm{Tr}(g\mid V)\equiv\mathrm{Tr}(g\mid V')\pmod{t\mathbb{O}}$.

The condition 2.3.4 implies that, for any G_F-stable $\mathbb{O}$-lattice $T'\subset V'$, the semisimplification $\overline{T}'^{ss}$ of $\overline{T}'$ is isomorphic to $\overline{T}^{ss}$, which is in turn equal to $\overline{T}$, by condition 2.3.3. It follows that there is an isomorphism $u:\overline{T}'\xrightarrow{\sim}\overline{T}$ of $k[G_F]$-modules, which is unique up to a scalar in $k^\times$ (again by condition 2.3.3). Irreducibility of $\overline{T}'$ implies that any G_F-stable $\mathbb{O}$-lattice in V' is of the form aT' for some $a\in\mathcal{K}^\times$; as a result, T' satisfies the assumption (2) of Theorem 1.1. Finally, the pairings induced on $\overline{T}$ by $\langle\,\cdot\,,\cdot\,\rangle$ (and respectively by $\langle\,\cdot\,,\cdot\,\rangle'$ and u) coincide up to a multiplicative factor $b\in k^\times$ (by condition 2.3.3). After multiplying $\langle\,\cdot\,,\cdot\,\rangle'$ by a suitable element of $\mathbb{O}^\times$, we obtain $b=1$. In other words, the conditions 2.3.1–2.3.4 give rise to the data required in Theorem 2.2.

3. Two applications of Theorem 2.2 to modular forms

3.1. Let F be a totally real number field. If $g\in S_k(\mathfrak{n},1)$ is a cuspidal Hilbert newform over F of level $\mathfrak{n}$, of trivial character and parallel weight k (necessarily even), then its completed L-function coincides, up to a shift, with the L-function of the automorphic representation $\pi(g)$ of $\mathrm{PGL}_2(\mathbf{A}_F)$ associated to g:

$$(L_\infty\cdot L)(g,s)=L(\pi(g),s-(k-1)/2),\qquad L_\infty(g,s)=\Gamma_{\mathbb{C}}(s)^{[F:\mathbb{Q}]}.$$

Since the Γ-factor $L_\infty(g,s)$ has no zero nor pole at the central point $s=k/2$ of the functional equation, the parity of the analytic rank of g over F,

$$r_{\mathrm{an}}(F,g):=\mathrm{ord}_{s=k/2}\,L(g,s),$$

can be read off from the corresponding ε-constant in the functional equation

$$L(\pi(g),s)=\varepsilon(\pi(g),s)\,L(\pi(g),1-s),$$
$$(-1)^{r_{\mathrm{an}}(F,g)}=\varepsilon\big(\pi(g),\tfrac12\big)=\prod_v\varepsilon_v\big(\pi(g)_v,\tfrac12\big).$$

If L, $L_{\mathfrak{p}}$, and $V_{\mathfrak{p}}(g)$ are as in Theorem B (with an appropriate modification if $F\neq\mathbb{Q}$; see Theorem 1.4 in the case $k=2$), then the Galois representation $V=V_{\mathfrak{p}}(g)(k/2)$

satisfies the assumption (1) of Theorem 1.1. The conjectures of Bloch and Kato [1990; Fontaine and Perrin-Riou 1994] predict that

$$\dim_{L_\mathfrak{p}} H^1_f(F, V) = r_{\mathrm{an}}(F, g).$$

We are interested in this conjecture modulo 2:

$$\dim_{L_\mathfrak{p}} H^1_f(F, V) \equiv r_{\mathrm{an}}(F, g) \pmod 2.$$

3.2. Let $g \in S_k(\mathfrak{n}, 1)$ be as in Section 3.1. If F'/F is a quadratic extension and $\alpha : \mathrm{Gal}(F'/F) \xrightarrow{\sim} \{\pm 1\}$ the corresponding quadratic character, then we have

$$H^1_f(F', V) = H^1_f(F, V) \oplus H^1_f(F, V \otimes \alpha) \tag{3.2.1}$$

and

$$\begin{aligned} L(g \otimes F', s) &= L(g, s)L(g \otimes \alpha, s), \\ r_{\mathrm{an}}(F', g) &= r_{\mathrm{an}}(F, g) + r_{\mathrm{an}}(F, g \otimes \alpha), \end{aligned} \tag{3.2.2}$$

where we have denoted, somewhat abusively, by $g' = g \otimes F'$ the base change of g to an automorphic form on $\mathrm{PGL}_2(\mathbf{A}_{F'})$ and by $r_{\mathrm{an}}(F', g)$ the analytic rank $r_{\mathrm{an}}(F', g \otimes F')$ (strictly speaking, it is the automorphic representation of $\mathrm{PGL}_2(\mathbf{A}_{F'})$ attached to g' that is the base change of $\pi(g)$).

3.3. ***Proof of Theorem B.*** The claim for $r = 1$ is a special case of Theorem 1.4(a). If $r > 1$, then it follows from [Ribet 1994, Theorems 2.1 and 2.2, Corollary 3.2] (the author would like to thank F. Diamond for pointing out this reference) and from our assumption about the residual representation of $V_\mathfrak{p}(g)$ that there exists a normalised newform $g_1 \in S_2(N_1, \omega^{2-2r})$ of level N_1 dividing pN whose coefficients lie in a number field $L' \supset L$ and that satisfies, for a suitable prime $\mathfrak{p}' \mid \mathfrak{p}$ of L',

$$\mathrm{Tr}(g \mid V_{\mathfrak{p}'}(g_1)) \equiv \mathrm{Tr}(g \mid V_\mathfrak{p}(g) \otimes_{L_\mathfrak{p}} L'_{\mathfrak{p}'}) \pmod{\mathfrak{p}'} \quad \text{for all } g \in G_\mathbb{Q}.$$

Let $g' \in S_2(N', 1)$ be the newform associated to $g_1 \otimes \omega^{r-1}$ (of level dividing N multiplied by a suitable power of p); set $\mathcal{K} = L'_{\mathfrak{p}'}$, $\mathbb{O} = \mathbb{O}_\mathcal{K}$, $V = V_\mathfrak{p}(g)(r) \otimes_{L_\mathfrak{p}} \mathcal{K}$ and $V' = V_{\mathfrak{p}'}(g')(1) = V_{\mathfrak{p}'}(g_1)(1) \otimes \omega^{r-1}$.

The representations V and V' satisfy conditions 2.3.1 and 2.3.4 (note that $\mathbb{Z}_p(r)$ and $\mathbb{Z}_p(1) \otimes \omega^{r-1}$ have the same residual representation $\mathbf{F}_p(r)$). Fix any $G_\mathbb{Q}$-stable $\mathbb{O}$-lattice $T \subset V$. It satisfies condition 2.3.3 (irreducibility implies absolute irreducibility, as the action of the complex conjugation on $\overline{T}$ has two distinct eigenvalues ± 1 contained in $k = \mathbb{O}/t\mathbb{O}$) and, after rescaling the symplectic form $\langle \cdot, \cdot \rangle : V \times V \to \mathcal{K}(1)$, also condition 2.3.2. The discussion in Section 2.3 implies that the assumptions of Theorem 2.2 are satisfied. Using, in addition, Section 1.3, we deduce that

$$\dim_{\mathcal{K}} H^1_f(\mathbb{Q}, V) - \dim_{\mathcal{K}} H^1_f(\mathbb{Q}, V') \equiv \dim_{\mathcal{K}} H^1_f(\mathbb{Q}, V\otimes\alpha) - \dim_{\mathcal{K}} H^1_f(\mathbb{Q}, V'\otimes\alpha) \pmod 2, \tag{3.3.1}$$

whenever $\alpha : G_{\mathbb{Q}} \to \{\pm 1\}$ is a character satisfying

$$\alpha_l = 1 \quad \text{for all } l \mid pN. \tag{3.3.2}$$

According to Theorem 1.4(a),

$$\begin{aligned} \dim_{\mathcal{K}} H^1_f(\mathbb{Q}, V') &\equiv r_{\mathrm{an}}(\mathbb{Q}, g') \pmod 2, \\ \dim_{\mathcal{K}} H^1_f(\mathbb{Q}, V'\otimes\alpha) &\equiv r_{\mathrm{an}}(\mathbb{Q}, g'\otimes\alpha) \pmod 2. \end{aligned} \tag{3.3.3}$$

Combining (3.3.1) and (3.3.3) with Lemma 3.4 below, we obtain

$$\dim_{\mathcal{K}} H^1_f(\mathbb{Q}, V) - r_{\mathrm{an}}(\mathbb{Q}, g) \equiv \dim_{\mathcal{K}} H^1_f(\mathbb{Q}, V\otimes\alpha) - r_{\mathrm{an}}(\mathbb{Q}, g\otimes\alpha) \pmod 2. \tag{3.3.4}$$

It follows from the nonvanishing results of [Waldspurger 1991, Theorem 4; Friedberg and Hoffstein 1995, Theorem B.1] that there exists a character α satisfying (3.3.2) for which $r_{\mathrm{an}}(\mathbb{Q}, g\otimes\alpha) = 0$. A fundamental result of Kato [2004, Theorem 14.2(2)] then implies that $H^1_f(\mathbb{Q}, V\otimes\alpha) = 0$. The congruence (3.3.4) for this particular α becomes

$$\dim_{\mathcal{K}} H^1_f(\mathbb{Q}, V) \equiv r_{\mathrm{an}}(\mathbb{Q}, g) \pmod 2,$$

which proves Theorem B.

Lemma 3.4. *For any character α satisfying* (3.3.2) *we have*

$$r_{\mathrm{an}}(\mathbb{Q}, g) - r_{\mathrm{an}}(\mathbb{Q}, g') \equiv r_{\mathrm{an}}(\mathbb{Q}, g\otimes\alpha) - r_{\mathrm{an}}(\mathbb{Q}, g'\otimes\alpha) \pmod 2.$$

Proof. To simplify the notation we write $\varepsilon_v(h) = \varepsilon_v\big(\pi(h)_v, \tfrac{1}{2}\big)$ for the corresponding local ε-constants. It is enough to show that, for any prime v of $\mathbb{Q}$,

$$\varepsilon_v(g)/\varepsilon_v(g') = \varepsilon_v(g\otimes\alpha)/\varepsilon_v(g'\otimes\alpha). \tag{3.4.1}$$

Firstly, $\varepsilon_\infty(h) = \varepsilon_\infty(h\otimes\alpha)$ $(h = g, g')$, since the twist by α does not change the weight. Secondly, if l is a prime number dividing pN, then (3.3.2) implies that $\pi(h\otimes\alpha)_l = \pi(h)_l$ $(h = g, g')$; hence $\varepsilon_l(h\otimes\alpha) = \varepsilon_l(h)$. Finally, if l does not divide pN, then $\pi(g)_l = \pi(\mu, \mu^{-1})$ and $\pi(g')_l = \pi(\mu', \mu'^{-1})$ are unramified principal series representations with trivial central characters; it follows that $\pi(g\otimes\alpha) = \pi(\mu\alpha_l, \mu^{-1}\alpha_l)$, $\pi(g'\otimes\alpha) = \pi(\mu'\alpha_l, \mu'^{-1}\alpha_l)$ and

$$\begin{aligned} \varepsilon_l(g) = \mu(-1) = 1 = \mu'(-1) = \varepsilon_l(g'), \\ \varepsilon_l(g\otimes\alpha) = (\mu\alpha_l)(-1) = \alpha_l(-1) = (\mu'\alpha_l)(-1) = \varepsilon_l(g'\otimes\alpha), \end{aligned}$$

which completes the proof of (3.4.1). □

Theorem 3.5. *Let $g \in S_2(\mathfrak{n}, 1)$, L and $\mathfrak{p} \mid p$ ($p \neq 2$) be as in Theorem 1.4. Assume that $2 \mid [F : \mathbb{Q}]$, that the residual representation $T_\mathfrak{p}(g)/\mathfrak{p}T_\mathfrak{p}(g)$ (where $T_\mathfrak{p}(g) \subset V_\mathfrak{p}(g)$ is a G_F-stable $O_{L,\mathfrak{p}}$-lattice) is an irreducible G_F-module and that one of the following two conditions holds*:

(1) *g has no complex multiplication and $V_\mathfrak{p}(g)$ is not quaternionic (in the sense of Section 3.6 below)*;

(2) *g has complex multiplication: g is the theta series attached to an algebraic Hecke character $\mathbf{A}^\times_{K(g)} \to L'^\times$, where $K(g)$ and L' are totally imaginary quadratic extensions of F and L, respectively, $\mathfrak{p}$ splits in L'/L and $V_\mathfrak{p}(g)|_{G_{K(g)}} = \psi_1 \oplus \psi_2$, where $\psi_i : G_{K(g)} \to L_\mathfrak{p}^\times$ are characters for which $\psi_2(\mathrm{Ker}(\psi_1))$ is infinite.*

Then

$$\dim_{L_\mathfrak{p}} H^1_f(F, V_\mathfrak{p}(g)(1)) \equiv r_{\mathrm{an}}(F, g) \pmod 2.$$

Proof. As in the proof of Theorem B, the G_F-modules $V_\mathfrak{p}(g)(1) \supset T_\mathfrak{p}(g)(1)$ satisfy conditions 2.3.1–2.3.3. The level raising machinery [Taylor 1989] together with [Deligne and Serre 1974, Lemme 6.11] imply that there exists a newform $g' \in S_2(\mathfrak{n}', 1)$ of level $\mathfrak{n}'$ satisfying $\mathfrak{q} \mid \mathfrak{n}' \mid \mathfrak{n}\mathfrak{q}$ (for a suitable prime $\mathfrak{q} \nmid \mathfrak{n}$) whose Hecke eigenvalues lie in a number field $L' \supset L$ and satisfy

$$\lambda_v(g') \equiv \lambda_v(g) \pmod{\mathfrak{p}'} \quad \text{for all } v \nmid p\mathfrak{n}\mathfrak{q}$$

for a suitable prime $\mathfrak{p}' \mid \mathfrak{p}$ of L'. It follows from the Čebotarev density theorem that the representations $V = V_\mathfrak{p}(g)(1) \otimes_{L_\mathfrak{p}} \mathcal{K}$, $T = T_\mathfrak{p}(g)(1) \otimes_{O_{L,\mathfrak{p}}} \mathbb{O}_\mathcal{K}$ (where $\mathcal{K} = L'_{\mathfrak{p}'}$), and $V' = V_{\mathfrak{p}'}(g')(1)$ satisfy conditions 2.3.1–2.3.4. Applying Theorem 2.2 and taking into account Section 1.3, we obtain, for any character $\alpha : G_F \to \{\pm 1\}$ satisfying

$$\alpha_v = 1 \quad \text{for all } v \mid p\mathfrak{n}\mathfrak{q}, \tag{3.5.1}$$

that

$$\begin{aligned}\dim_\mathcal{K} H^1_f(F, V) - \dim_\mathcal{K} H^1_f(F, V') \\ \equiv \dim_\mathcal{K} H^1_f(F, V \otimes \alpha) - \dim_\mathcal{K} H^1_f(F, V' \otimes \alpha) \pmod 2. \end{aligned}\tag{3.5.2}$$

Since $\mathrm{ord}_\mathfrak{q}(\mathfrak{n}') = 1$, the local representation $\pi(g')_\mathfrak{q}$ is the twist of the Steinberg representation by an unramified character of order one or two. Then Theorem 1.4(b) applies to g' and its quadratic twists:

$$\begin{aligned}\dim_\mathcal{K} H^1_f(F, V') &\equiv r_{\mathrm{an}}(F, g') \pmod 2, \\ \dim_\mathcal{K} H^1_f(F, V' \otimes \alpha) &\equiv r_{\mathrm{an}}(F, g' \otimes \alpha) \pmod 2.\end{aligned}\tag{3.5.3}$$

The argument used in the proof of Lemma 3.4 applies, yielding

$$r_{\mathrm{an}}(F, g) - r_{\mathrm{an}}(F, g') \equiv r_{\mathrm{an}}(F, g \otimes \alpha) - r_{\mathrm{an}}(F, g' \otimes \alpha) \pmod 2. \tag{3.5.4}$$

Combining (3.5.2)–(3.5.4), we obtain

$$\begin{aligned} &\dim_{\mathcal{K}} H^1_f(F, V) - r_{\mathrm{an}}(F, g) \\ &\qquad \equiv \dim_{\mathcal{K}} H^1_f(F, V \otimes \alpha) - r_{\mathrm{an}}(F, g \otimes \alpha) \pmod 2, \end{aligned} \tag{3.5.5}$$

for any quadratic character α satisfying (3.5.1). As in the proof 3.3, it follows from [Waldspurger 1991, Theorem 4; Friedberg and Hoffstein 1995, Theorem B.1] that there exists α satisfying (3.5.1) such that $r_{\mathrm{an}}(F, g \otimes \alpha) = 0$. A generalisation of [Longo 2006, Theorem C] proved in [Nekovář 2012, Theorem B] implies that $H^1_f(F, V \otimes \alpha) = 0$ (this is where the assumptions (1) and (2) come in, by [Nekovář 2012, B.5.5(2) and B.6.5(2)], respectively). The congruence (3.5.5) for this α yields the desired result. □

3.6. ***(Non)quaternionic representations.*** If g from Theorem 3.5 does not have complex multiplication, recall from [Nekovář 2012, Appendix B.3] that there exists a finite abelian group $\Gamma \subset \mathrm{Aut}(L/\mathbb{Q})$ of exponent at most two and a quaternion algebra D over L^Γ such that, for each finite prime $\mathfrak{p}$ of L, the Lie algebra of the Galois image

$$\mathrm{Im}(G_F \to \mathrm{Aut}_{L_\mathfrak{p}}(V_\mathfrak{p}(g)) \xrightarrow{\sim} GL_2(L_\mathfrak{p}))$$

is equal to

$$\{x \in D_{\mathfrak{p}_\Gamma} \subset M_2(L_\mathfrak{p}) \mid \mathrm{Trd}(x) \in \mathbb{Q}_p\},$$

where $\mathfrak{p}_\Gamma$ is the prime of $L^\Gamma \subset L$ below $\mathfrak{p}$ and $D_{\mathfrak{p}_\Gamma} = D \otimes_{L^\Gamma} (L^\Gamma)_{\mathfrak{p}_\Gamma}$.

As in [Nekovář 2012, B.4.7] we say that $V_\mathfrak{p}(g)$ is *quaternionic* if $D_{\mathfrak{p}_\Gamma}$ is a division algebra (which can happen only for finitely many $\mathfrak{p}$).

According to [Nekovář 2012, B.4.8(1)], if the extension $L_\mathfrak{p}/(L^\Gamma)_{\mathfrak{p}_\Gamma}$ is unramified and the residual representation $T_\mathfrak{p}(g)/\mathfrak{p}T_\mathfrak{p}(g)$ is an irreducible G_F-module, then $V_\mathfrak{p}(g)$ is not quaternionic. In particular, the condition "$V_\mathfrak{p}(g)$ is not quaternionic" can be omitted in Theorem 3.5(1) if $L_\mathfrak{p}/(L^\Gamma)_{\mathfrak{p}_\Gamma}$ is unramified.

4. Parity results for abelian varieties with real multiplication

4.1. Let F and L be totally real number fields, and let A be an abelian variety over F satisfying

$$\dim(A) = [L : \mathbb{Q}], \qquad O_L = \mathrm{End}_F(A). \tag{4.1.1}$$

For each finite prime $\mathfrak{p}$ of L the two-dimensional $L_\mathfrak{p}$-representation $V_\mathfrak{p}(A) := T_p(A) \otimes_{O_L \otimes \mathbb{Z}_p} L_\mathfrak{p}$ of G_F satisfies the assumptions of Theorem 1.1 (with $\mathcal{K} = L_\mathfrak{p}$).

Recall that A is *modular* (over F) if there exists a cuspidal Hilbert modular newform $g \in S_2(\mathfrak{n}, 1)$ whose field of Hecke eigenvalues is equal to $\iota(L) \subset \mathbb{C}$ (for some embedding $\iota : L \hookrightarrow \mathbb{C}$) and that satisfies

$$V_{\mathfrak{p}}(A) \xrightarrow{\sim} V_{\mathfrak{p}}(g)(1)$$

for one (equivalently, for each) finite prime $\mathfrak{p}$ of L. This is, in turn, equivalent to an equality of L-functions,

$$L(\iota A/F, s) = L(g, s)$$

(Euler factor by Euler factor), which implies that

$$L(\sigma\iota A/F, s) = L({}^{\sigma}g, s) \quad \text{for all } \sigma \in \mathrm{Aut}(\mathbb{C}).$$

4.2. The potential automorphy results of [Barnet-Lamb et al. 2010, Theorems 4.5.1 and 5.3.1] imply that every abelian variety A satisfying (4.1.1) is potentially modular in the following sense: For each finite extension M/F there exists a totally real finite extension F'/F that is linearly disjoint from M/F such that $A \otimes_F F'$ is modular over F'.

As in [Nekovář 2006, 12.11.6; 2009, Step 4], a minor improvement (use of Solomon's induction theorem [Curtis and Reiner 1981, Theorem 15.10] instead of the usual Brauer theorem) of an argument of Taylor [2002, proof of Corollary 2.2] implies that there exist intermediate fields $F \subset F_i \subset F'$ and integers n_i with the following properties:

4.2.1 A is modular over each F_i: there exists a Hilbert modular newform g_i of parallel weight 2 over F_i such that $L(\iota A/F_i, s) = L(g_i, s)$ and $V_{\mathfrak{p}}(A)|_{G_{F_i}} \xrightarrow{\sim} V_{\mathfrak{p}}(g_i)(1)$ for each finite prime $\mathfrak{p}$ of L.

4.2.2 $L(\iota A/F, s) = \prod_i L(\iota A/F_i, s)^{n_i} = \prod_i L(g_i, s)^{n_i}$.

4.2.3 $V_{\mathfrak{p}}(A) = \bigoplus_i n_i \operatorname{Ind}_{G_{F_i}}^{G_F}(V_{\mathfrak{p}}(A)|_{G_{F_i}}) = \bigoplus_i n_i \operatorname{Ind}_{G_{F_i}}^{G_F}(V_{\mathfrak{p}}(g_i)(1))$ in the Grothendieck ring of $L_{\mathfrak{p}}[G_F]$-modules.

It follows that, for each $\sigma \in \mathrm{Aut}(\mathbb{C})$, the L-function

$$L(\sigma\iota A/F, s) = \prod_i L({}^{\sigma}g_i, s)^{n_i}$$

has a meromorphic continuation to $\mathbb{C}$ and satisfies the expected functional equation. In particular, the analytic rank

$$r_{\mathrm{an}}(\sigma\iota A/F) := \operatorname{ord}_{s=1} L(\sigma\iota A/F, s) \in \mathbb{Z}$$

is defined. Since the ε-constant in the functional equation of $L({}^{\sigma}g_i, s)$ does not depend on σ, the parity

$$r_{\mathrm{an}}(\tau A/F) \pmod 2 \in \mathbb{Z}/2\mathbb{Z}$$

of the analytic rank $r_{\mathrm{an}}(\tau A/F)$ does not depend on the embedding $\tau : L \hookrightarrow \mathbb{C}$.

Theorem 4.3. *Let A, F and L be as in* (4.1.1). *Let $\mathfrak{p}$ be a prime of L above a rational prime $p \neq 2$. Assume that at least one of the following conditions holds*:

(a) *A is modular over F and $2 \nmid [F : \mathbb{Q}]$.*

(b) *A does not have potentially good reduction everywhere.*

(c) *A does not have complex multiplication, $A[\mathfrak{p}]$ is an irreducible G_F-module, and the simple algebra $C := \mathrm{End}_{\overline{F}}(A) \otimes \mathbb{Q}$ satisfies $C \otimes_{Z(C)} Z(C)_{\mathfrak{p}_C} \xrightarrow{\sim} M_n(Z(C)_{\mathfrak{p}_C})$, where $\mathfrak{p}_C$ is the prime of $Z(C) \subset L$ below $\mathfrak{p}$ (the latter condition follows from the irreducibility of $A[\mathfrak{p}]$ if $L_{\mathfrak{p}}/Z(C)_{\mathfrak{p}_C}$ is unramified).*

(d) *A has complex multiplication by a totally imaginary quadratic extension L' of L (defined over a totally imaginary quadratic extension $K(A)$ of F), $A[\mathfrak{p}]$ is an irreducible G_F-module, $\mathfrak{p}$ splits in L'/L, and the image of $G_{K(A)}$ in $\mathrm{Aut}_{L'\otimes_L L_{\mathfrak{p}}}(V_{\mathfrak{p}}(A)) = L_{\mathfrak{p}}^\times \times L_{\mathfrak{p}}^\times$ contains an open subgroup of $\mathbb{Z}_p^\times \times \mathbb{Z}_p^\times$.*

(e) *$A[\mathfrak{p}]$ is a reducible G_F-module, $L_{\mathfrak{p}}/\mathbb{Q}_p$ is unramified and $p > 2[L_{\mathfrak{p}} : \mathbb{Q}_p] + 1$.*

Then the Selmer rank

$$\dim_{L_{\mathfrak{p}}} H^1_f(F, V_{\mathfrak{p}}(A)) = \mathrm{rk}_{O_L} A(F) + \mathrm{cork}_{O_{L,\mathfrak{p}}} Ш(A/F)[\mathfrak{p}^\infty]$$

satisfies

$$\dim_{L_{\mathfrak{p}}} H^1_f(F, V_{\mathfrak{p}}(A)) \equiv r_{\mathrm{an}}(\tau A/F) \pmod 2,$$

for each embedding $\tau : L \hookrightarrow \mathbb{C}$.

Proof. The case (a) follows from Theorem 1.4(a). In the cases (b)–(e) we have, thanks to Section 4.2,

$$\begin{aligned}\dim_{L_{\mathfrak{p}}} H^1_f(F, V_{\mathfrak{p}}(A)) - r_{\mathrm{an}}(\tau A/F)& \\ \equiv \sum_i n_i\big(\dim_{L_{\mathfrak{p}}} H^1_f(F_i, V_{\mathfrak{p}}(g_i)(1)) - r_{\mathrm{an}}(F_i, g_i)\big) &\pmod 2,\end{aligned}$$

which means that we can replace F by F_i and assume that A is modular over F (taking $M = F(A[\mathfrak{p}])$ in Section 4.2 we ensure that $A[\mathfrak{p}]$ is irreducible as a G_{F_i}-module in cases (c) or (d)). The case (b) then follows from Theorem 1.4(b) and the cases (c) and (d) from Theorem 3.5 (using [Nekovář 2012, B.6.5(2)]). In case (e) we can assume, thanks to Theorem 1.4(c), that $\pi(g)$ is a principal series representation at each finite prime of F, which implies that A acquires locally at each completion of F (hence also globally, by [Artin and Tate 1990, Chapter 10, Theorem 5]) good reduction over a suitable cyclic extension. The result then follows from an $O_{L,\mathfrak{p}}$-equivariant version of the proof of [Coates et al. 2010, Theorem 2.1]. ∎

4.4. ***Proof of Theorem A.*** As in the proof of Theorem 4.3, potential modularity of E [Wintenberger 2009, Theorem A.1] together with properties 4.2.2 and 4.2.3 imply that we can write $s_p(E/F) - r_{\mathrm{an}}(E/F)$ as an integral linear combination of $s_p(E/F_i) - r_{\mathrm{an}}(E/F_i)$, for suitable totally real extensions F_i/F over which E is modular. It is enough, therefore, to replace F by F_i and consider only the case when E is modular over F (which is automatic if E has complex multiplication).

Assume first that $p = 2$. It follows from [Waldspurger 1991, Theorem 4; Friedberg and Hoffstein 1995, Theorem B.1] that there exists a nontrivial quadratic character $\alpha : G_F \to \{\pm 1\}$ such that $r_{\mathrm{an}}(E \otimes \alpha/F) = 0$. This implies, by [Nekovář 2012, corollary of Theorem B′], that $s_2(E \otimes \alpha/F) = 0$. Let F'/F be the quadratic extension corresponding to α. Since

$$s_2(E/F') \equiv r_{\mathrm{an}}(E/F') \pmod 2$$

by [Dokchitser and Dokchitser 2011, Corollary 4.8], we conclude by the following analogue of (3.2.1) and (3.2.2):

$$s_p(E/F') = s_p(E/F) + s_p(E \otimes \alpha/F), \quad r_{\mathrm{an}}(E/F') = r_{\mathrm{an}}(E/F) + r_{\mathrm{an}}(E \otimes \alpha/F).$$

If $p \neq 2$, we can assume that $2 \mid [F : \mathbb{Q}]$, in view of [Nekovář 2009, Theorem 1(a)]. Theorem 4.3(c),(d) (respectively (e)) then implies the desired result if $E[p]$ is an irreducible G_F-module (respectively when $E[p]$ is reducible and $p > 3$). The remaining case when $p = 3$ and $E[3]$ is a reducible G_F-module is treated in [Dokchitser and Dokchitser 2011, Corollary 5.8].

4.5. Further absolute parity results (it would be too cumbersome to list them all here) follow from a combination of Theorem A with the relative parity results proved in [Mazur and Rubin 2007, Theorems 6.4 and 7.1; 2008, Theorem 1.1; Dokchitser and Dokchitser 2009, Theorems 4.3 and 4.5; 2011, Proposition 6.12; Greenberg 2011, Section 11.8; de La Rochefoucauld 2011, Theorem 2.1].

4.6. Our proof of Theorem A in the case when $E[p]$ is a reducible G_F-module uses Theorem 1.4(c), which relies on several very recent technical advances: [Aflalo and Nekovář 2010; Nekovář 2012] and [Yuan et al. 2008] (used in the proof of [Nekovář 2012, Theorem B(b)]). It would be desirable to have a more direct proof in the reducible case.[1]

4.7. The conclusion of Theorem A also holds in the case when E has complex multiplication (and hence is modular over F), $p \neq 2$ and the conductor of E is not a square, by Theorem 1.4(c) (conductors are preserved under the local Langlands correspondence and the conductor of any principal series representation of $\mathrm{PGL}_2(F_v)$ is a square).

[1] Added in proof: This is done in [Česnavičius 2012].

Acknowledgements

This work owes its origin to my stay at the Centre de Recerca Matemàtica at Universitat Autònoma de Barcelona in December 2009. I am grateful to the organisers of the program "Arithmetic Geometry" for their invitation and to the CRM for its hospitality. I thank the referee for helpful comments.

References

[Aflalo and Nekovář 2010] E. Aflalo and J. Nekovář, "Non-triviality of CM points in ring class field towers", *Israel J. Math.* **175** (2010), 225–284. MR 2011j:11108 Zbl 05789726

[Artin and Tate 1990] E. Artin and J. Tate, *Class field theory*, 2nd ed., Addison-Wesley, Redwood City, CA, 1990. MR 91b:11129 Zbl 0681.12003

[Barnet-Lamb et al. 2010] T. Barnet-Lamb, T. Gee, D. Geraghty, and R. Taylor, "Potential automorphy and change of weight", preprint, 2010. arXiv 1010.2561v1

[Bloch and Kato 1990] S. Bloch and K. Kato, "L–functions and Tamagawa numbers of motives", pp. 333–400 in *The Grothendieck Festschrift, I*, edited by P. Cartier et al., Progr. Math. **86**, Birkhäuser, Boston, MA, 1990. MR 92g:11063 Zbl 0768.14001

[Česnavičius 2012] K. Česnavičius, "The p-parity conjecture for elliptic curves with a p-isogeny", preprint, 2012. arXiv 1207.0431

[Coates et al. 2010] J. Coates, T. Fukaya, K. Kato, and R. Sujatha, "Root numbers, Selmer groups, and non-commutative Iwasawa theory", *J. Algebraic Geom.* **19**:1 (2010), 19–97. MR 2011a:11127 Zbl 1213.11135

[Cornut and Vatsal 2007] C. Cornut and V. Vatsal, "Nontriviality of Rankin–Selberg L–functions and CM points", pp. 121–186 in *L–functions and Galois representations* (Durham, 2004), edited by D. Burns et al., London Math. Soc. Lecture Note Ser. **320**, Cambridge Univ. Press, 2007. MR 2009m:11088 Zbl 1153.11025

[Curtis and Reiner 1981] C. W. Curtis and I. Reiner, *Methods of representation theory, I: With applications to finite groups and orders*, Wiley, New York, 1981. MR 82i:20001 Zbl 0469.20001

[Deligne 1973] P. Deligne, "Les constantes des équations fonctionnelles des fonctions L", pp. 501–597 in *Modular functions of one variable, II* (Antwerp, 1972), edited by P. Deligne and W. Kuyk, Lecture Notes in Math. **349**, Springer, Berlin, 1973. MR 50 #2128 Zbl 0271.14011

[Deligne and Serre 1974] P. Deligne and J.-P. Serre, "Formes modulaires de poids 1", *Ann. Sci. École Norm. Sup.* (4) **7** (1974), 507–530. MR 52 #284 Zbl 0321.10026

[Dokchitser and Dokchitser 2009] T. Dokchitser and V. Dokchitser, "Regulator constants and the parity conjecture", *Invent. Math.* **178**:1 (2009), 23–71. MR 2010j:11089 Zbl 1219.11083

[Dokchitser and Dokchitser 2011] T. Dokchitser and V. Dokchitser, "Root numbers and parity of ranks of elliptic curves", *Crelle's Journal* **658** (2011), 39–64. MR 2012h:11084 Zbl 05962772

[Flach 1990] M. Flach, "A generalisation of the Cassels–Tate pairing", *Crelle's Journal* **412** (1990), 113–127. MR 92b:11037 Zbl 0711.14001

[Fontaine 1994] J.-M. Fontaine, "Représentations l–adiques potentiellement semi-stables", pp. 321–347 in *Périodes p–adiques* (Bures-sur-Yvette, 1988), Astérisque **223**, Société Mathématique de France, Paris, 1994. MR 95k:14031 Zbl 0873.14020

[Fontaine and Perrin-Riou 1994] J.-M. Fontaine and B. Perrin-Riou, "Autour des conjectures de Bloch et Kato: Cohomologie galoisienne et valeurs de fonctions L", pp. 599–706 in *Motives* (Seattle, 1991), vol. 1, edited by U. Jannsen et al., Proc. Sympos. Pure Math. **55**, Amer. Math. Soc., 1994. MR 95j:11046 Zbl 0821.14013

[Friedberg and Hoffstein 1995] S. Friedberg and J. Hoffstein, "Nonvanishing theorems for automorphic L–functions on GL(2)", *Ann. of Math.* **142**:2 (1995), 385–423. MR 96e:11072 Zbl 0847.11026

[Greenberg 2011] R. Greenberg, *Iwasawa theory, projective modules, and modular representations*, Mem. Amer. Math. Soc. **992**, Amer. Math. Soc., 2011. MR 2807791 Zbl 1247.11085

[Kato 2004] K. Kato, "p–adic Hodge theory and values of zeta functions of modular forms", pp. 117–290 in *Cohomologies p–adiques et applications arithmétiques, III*, Astérisque **295**, Société Mathématique de France, Paris, 2004. MR 2006b:11051 Zbl 1142.11336

[Kim 2009] B. D. Kim, "The symmetric structure of the plus/minus Selmer groups of elliptic curves over totally real fields and the parity conjecture", *J. Number Theory* **129**:5 (2009), 1149–1160. MR 2010f:11089 Zbl 1170.11011

[de La Rochefoucauld 2011] T. de La Rochefoucauld, "Invariance of the parity conjecture for p–Selmer groups of elliptic curves in a D_{2p^n}–extension", *Bull. Soc. Math. France* **139**:4 (2011), 571–592. MR 2869306 Zbl 1244.11062 arXiv 1002.0554

[Longo 2006] M. Longo, "On the Birch and Swinnerton–Dyer conjecture for modular elliptic curves over totally real fields", *Ann. Inst. Fourier* (*Grenoble*) **56**:3 (2006), 689–733. MR 2008f:11071 Zbl 1152.11028

[Mazur and Rubin 2004] B. Mazur and K. Rubin, *Kolyvagin systems*, Mem. Amer. Math. Soc. **799**, Amer. Math. Soc., 2004. MR 2005b:11179 Zbl 1055.11041

[Mazur and Rubin 2007] B. Mazur and K. Rubin, "Finding large Selmer rank via an arithmetic theory of local constants", *Ann. of Math.* **166**:2 (2007), 579–612. MR 2009a:11127 Zbl 1219.11084

[Mazur and Rubin 2008] B. Mazur and K. Rubin, "Growth of Selmer rank in nonabelian extensions of number fields", *Duke Math. J.* **143**:3 (2008), 437–461. MR 2009g:11070 Zbl 1151.11023

[Nekovář 2001] J. Nekovář, "On the parity of ranks of Selmer groups, II", *C. R. Acad. Sci. Paris Sér. I Math.* **332**:2 (2001), 99–104. MR 2002e:11060 Zbl 1090.11037

[Nekovář 2006] J. Nekovář, *Selmer complexes*, Astérisque **310**, Société Mathématique de France, Paris, 2006. MR 2009c:11176 Zbl 1211.11120

[Nekovář 2007a] J. Nekovář, "The Euler system method for CM points on Shimura curves", pp. 471–547 in *L–functions and Galois representations* (Durham, 2004), edited by D. Burns et al., London Math. Soc. Lecture Note Ser. **320**, Cambridge University Press, 2007. MR 2010a:11110 Zbl 1152.11023

[Nekovář 2007b] J. Nekovář, "On the parity of ranks of Selmer groups, III", *Doc. Math.* **12** (2007), 243–274. Corrected in *Doc. Math.* **14** (2009), 191–194. MR 2009k:11109 Zbl 1201.11067

[Nekovář 2008] J. Nekovář, "Growth of Selmer groups of Hilbert modular forms over ring class fields", *Ann. Sci. Éc. Norm. Supér.* (4) **41**:6 (2008), 1003–1022. MR 2010g:11084 Zbl 1236.11047

[Nekovář 2009] J. Nekovář, "On the parity of ranks of Selmer groups, IV", *Compos. Math.* **145**:6 (2009), 1351–1359. MR 2010j:11106 Zbl 1221.11150

[Nekovář 2012] J. Nekovář, "Level raising and anticyclotomic Selmer groups for Hilbert modular forms of weight two", *Canad. J. Math.* **64**:3 (2012), 588–668. MR 2962318 Zbl 06042742

[Ribet 1994] K. A. Ribet, "Report on mod l representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$", pp. 639–676 in *Motives* (Seattle, 1991), vol. 2, edited by U. Jannsen et al., Proc. Sympos. Pure Math. **55**, Amer. Math. Soc., 1994. MR 95d:11056 Zbl 0822.11034

[Taylor 1989] R. Taylor, "On Galois representations associated to Hilbert modular forms", *Invent. Math.* **98**:2 (1989), 265–280. MR 90m:11176 Zbl 0705.11031

[Taylor 2002] R. Taylor, "Remarks on a conjecture of Fontaine and Mazur", *J. Inst. Math. Jussieu* **1**:1 (2002), 125–143. MR 2004c:11082 Zbl 1047.11051

[Waldspurger 1991] J.-L. Waldspurger, "Correspondances de Shimura et quaternions", *Forum Math.* **3**:3 (1991), 219–307. MR 92g:11054 Zbl 0724.11026

[Wintenberger 2009] J.-P. Wintenberger, "Potential modularity of elliptic curves over totally real fields", 2009, available at http://www-irma.u-strasbg.fr/~wintenb/potmodcomp.pdf. Appendix to [Nekovář 2009].

[Yuan et al. 2008] X. Yuan, S.-w. Zhang, and W. Zhang, "Heights of CM points, I: Gross–Zagier formula", preprint, 2008, available at http://www.math.columbia.edu/~szhang/papers/HCMI.pdf.

Communicated by Brian Conrad
Received 2011-10-03 Revised 2012-05-18 Accepted 2012-05-18

nekovar@math.jussieu.fr *Institut de Mathématiques de Jussieu, Université Pierre et Marie Curie (Paris 6), Théorie des Nombres, Case 247, 4, place Jussieu, F-75252 Paris cedex 05, France*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2013 is US $200/year for the electronic version, and $350/year (+$40, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
http://msp.org/

Algebra & Number Theory

Volume 7 No. 5 2013

1937-0652(2013)7:5;1-8