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

Jan Nekovář

The main results of this article are the following two instances of the parity conjecture for Selmer groups (see [N2, §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*

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

(which is also equal to the dimension $\dim_{\mathbf{Q}_p} H^1_f(F, V_p(E))$ of the Bloch-Kato Selmer group [BK, Def. 5.1] of the Galois representation $V_p(E) = T_p(E) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$ 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 $2 \nmid [F : \mathbf{Q}]$;*
(3) *E has complex multiplication by an imaginary quadratic field K' and p splits in $K'/\mathbf{Q}$.*

Note that potential modularity of E [Wi, Thm. A.1] implies that the L-function $L(E/F, s)$ has a meromorphic continuation to $\mathbf{C}$ and satisfies the expected functional equation ([T2, proof of Cor. 2.2]; [N2, 12.11.6]). As a result, the integer $\mathrm{ord}_{s=1} L(E/F, s) \in \mathbf{Z}$ is well-defined.

Various special cases of Theorem A (for $F \neq \mathbf{Q}$) were proved in [N2], [Ki] and [N6].

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

Theorem B. *Let $g = \sum_{n=1}^{\infty} a_n q^n \in S_{2r}(\Gamma_0(N))$ ($r \geq 1$) be a normalised ($a_1 = 1$) newform, let $L = \mathbf{Q}(a_1, a_2, \ldots)$ 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 $G_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $L_{\mathfrak{p}}$ attached to g:*

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

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

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

If g is (the newform associated to) a twist of a p-ordinary eigenform, Theorem B was proved in [N2, Thm. 12.2.3], even for $p = 2$ and without the assumption on the residual representation.

The proofs of Theorem A and B combine the techniques developed in [N1-6] and [AN] (namely, a combination of suitable relative parity results involving two Selmer groups with an Euler system argument [N3] applied to a non-trivial Euler system [CV], [AN]) with a formula of Mazur and Rubin [MR2, Thm. 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 which 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 Sect. 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 "bi-relative" 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 [Ka], [N7]), 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 programme is carried out for Hilbert modular forms in Sect. 3; the results for abelian varieties with real multiplication are deduced in Sect. 4. The assumptions on E in Theorem A come from an application of [N7, Cor. Thm. B'].

This work owes its origin to the author's stay at the Centre de Recerca Matemàtica at Universitat Autònoma de Barcelona in December 2009. He is grateful to the organisers of the programme "Arithmetic Geometry" for invitation and to the CRM for its hospitality. He would also like to thank the referee for helpful comments.

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_∞ (resp. by S_p) the set of all archimedean primes (resp. of all primes above a rational prime p) of F. For any $R[G]$-module M and a character $\chi : G \longrightarrow R^\times$ we denote by $M^{(\chi)} = \{m \in M \mid \forall g \in G \;\; g(m) = \chi(g)m\}$ the χ-eigenspace for the action of G on M.

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

1.1. Theorem (An abstract cohomological version of the case $\mathfrak{S} = \emptyset$ of [MR2, Thm. 7.1]). *Let F be a number field, 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 $\mathbf{Q}_p$, where $p \neq 2$. Assume that:*
(1) *There exists a non-degenerate skew-symmetric G_F-equivariant bilinear pairing $\langle\ ,\ \rangle : V \times V \longrightarrow \mathcal{K}(1)$.*
(2) *After possibly multiplying $\langle\ ,\ \rangle$ by an element of $\mathcal{K}^\times$, there exists a G_F-stable $\mathcal{O}_\mathcal{K}$-lattice $T \subset V$ which is self-dual (i.e., 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, 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 $\chi : \mathrm{Gal}(K'/K) \longrightarrow \mathcal{K}^\times$,

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

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 $t \in \mathcal{O} = \mathcal{O}_\mathcal{K}$ and denote by $k = \mathcal{O}/t\mathcal{O}$ the residue field of $\mathcal{K}$. The $\mathcal{K}$-subspaces $H^1_f(F_v, V) \subset H^1(F_v, V)$ ($v \notin S_\infty$) define, by propagation [MR1, Ex. 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 $\{T/t^nT\}_{n \leq \infty}$ [MR1, Lemma 3.7.1]. The exact sequences

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

imply that

$$\dim_k H^1_f(F, V/T)[t] - \dim_\mathcal{K} H^0(F, V) = \dim_k H^1_f(F, \overline{T}) - \dim_k H^0(F, \overline{T}), \tag{1.1.1}$$
$$\dim_k \left(H^1_f(F_v, \overline{T}) = H^1_f(F_v, T) \otimes_\mathcal{O} k\right) = \dim_k H^0(F_v, \overline{T}) + \dim_\mathcal{K} H^1_f(F_v, V) - \dim_\mathcal{K} H^0(F_v, V). \tag{1.1.2}$$

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 non-degenerate skew-symmetric bilinear pairing on $H^1_f(F,V/T)/\left(H^1_f(F,T)\otimes_{\mathcal{O}}\mathcal{K}/\mathcal{O}\right)$ with values in $\mathcal{K}/\mathcal{O}$ constructed in [Fl] (taking into account [BK, Prop. 3.8]) implies that

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

we deduce from (1.1.1) that

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

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

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

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

The discussion leading to the formulas (1.1.1-3) applies to $V\otimes I[\chi]$ and the self-dual lattice $T\otimes_{\mathcal{O}} I[\chi]$. Note that 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 1.1 and 1.2, should not to be confused with the Tate twist "(1)"). However, the Selmer structures $H^1_{f,\chi}(F_v,-)$ (resp. $H^1_{f,1}(F_v,-)$) on the G_F-module $\overline{T}\otimes I[\chi] = \overline{T}\otimes I[1]$ obtained by propagation of the subspaces $H^1_f(F_v,V\otimes I[\chi])\subset H^1(F_v,V\otimes I[\chi])$ (resp. $H^1_f(F_v,V\otimes I[1])\subset H^1(F_v,V\otimes I[1])$) are not necessarily the same. The formula [MR2, Thm. 1.4] applies in our case, since both Selmer structures $H^1_{f,\chi}$ and $H^1_{f,1}$ are self-dual, thanks to [BK, Prop. 3.8]; it yields

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

where

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

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

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

where we have put

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

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

1.2. Lemma. *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 (= the restriction of χ to G_{K_w}) is unramified by assumption, and therefore trivial [MR2, 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

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

we must show that

$$\dim_k(Y \cap Z_+) \stackrel{?}{\equiv} \dim_k(Y \cap Z_-) \pmod 2.$$

Firstly, the local duality

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

is a non-degenerate symmetric bilinear pairing under which $Y^\perp = Y$ and $Z_\pm^\perp = Z_\mp$, by [BK, Prop. 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 R.H.S. is equal to zero. If $v \mid p$, then the R.H.S. is equal, by [BK, Cor. 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. 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 $V_p(A) \otimes_{\mathbf{Q}_p} \mathcal{K}$, where A is an abelian variety over F.

1.4. Theorem (Generalisation of [N6, Thm. 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:*

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

Assume that at least one of the following three conditions is satisfied:
(a) $2 \nmid [F : \mathbf{Q}]$;
(b) *there exists a non-archimedean prime of F at which the local component of the automorphic representation $\pi(g)$ of $PGL_2(\mathbf{A}_F)$ attached to g is a twist of the Steinberg representation;*
(c) *there exists a non-archimedean 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. (a), (b) In the case when g corresponds to an elliptic curve defined over F this result was proved in [N6]. The argument of [loc. cit.] 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 [MR2, Thm. 7.1]. As $V_{\mathfrak{p}}(g)(1)$ arises as a subrepresentation of $V_p(A)\otimes_{\mathbf{Q}_p} L_{\mathfrak{p}}$, where A is the Jacobian of a suitable Shimura curve, (1.3.1) applies in this case.
(c) Thanks to (a) we can assume that $2 \mid [F:\mathbf{Q}]$. In addition, we can assume, as in [N6, Step 3] (after replacing F by a suitable cyclic extension of odd degree), that there exists a prime $P \mid p$ in F, $P \neq v_0$. Let K be any totally imaginary quadratic extension of F in which P splits and which satisfies the properties of Lemma 1.5 below (and such that g does not have CM by K). As in [N5, 1.2-1.5] (for $\chi = 1$, $\Sigma = \{P\}$, $c = 1$), the generalisation of [CV, Thm. 4.1] proved in [AN, Thm. 4.3.1] combined with [N3, Thm. 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 [N1]:

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 [Wa, Thm. 4] and [FH, Thm. 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 [N7, Thm. 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 $2 \mid \dim_{L_{\mathfrak{p}}} H^1_f(F, V_{\mathfrak{p}}(g)(1))$.

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

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

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 [N7, Prop. 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 non-archimedean prime v of F we write, as in [N4, Prop. 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 non-trivial additive character of F_v and dx_ψ the corresponding self-dual Haar measure on F_v, and $WD(V_v)$ is the representation of the Weil-Deligne group of F_v attached to V_v if $v \nmid p$, resp. to $D_{pst}(V_v)$ if $v \mid p$ (see [D, 8.4], [Fo], [FoPR, I.1.3.2]).

2.2. Theorem. *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 $\mathcal{K}$ which satisfy the assumptions (1) and (2) of Theorem 1.1. Let $T \subset V$ and $T' \subset V'$ be G_F-stable $\mathcal{O}$-lattices, self-dual with respect to the corresponding pairings $\langle\ ,\ \rangle : T \times T \longrightarrow \mathcal{O}(1)$ and $\langle\ ,\ \rangle' : T' \times T' \longrightarrow \mathcal{O}(1)$. Assume that there exists an isomorphism of $k[G_F]$-modules $u : \overline{T}' = T' \otimes_{\mathcal{O}} k \xrightarrow{\sim} \overline{T} = T \otimes_{\mathcal{O}} k$ compatible with the pairings induced by $\langle\ ,\ \rangle$ (resp. $\langle\ ,\ \rangle'$) on $\overline{T}$ (resp. 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 $\alpha : G_F \longrightarrow \{\pm 1\}$ is a character such that $\alpha_v = 1$ for all $v \in S - S_\infty$, then (using the notation from (1.1.6)):*

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

Proof. As remarked in the course of the proof of Theorem 1.1, the Selmer structure $H^1_f(F_v, \overline{T})$ (resp. $H^1_{f'}(F_v, \overline{T})$) obtained by propagation of $H^1_f(F_v, V) \subset H^1(F_v, V)$ (resp. 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) is self-dual. Combining [MR2, Thm. 1.4] with (1.1.3) we obtain

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

where

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

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

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

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, $H^1(F_v, \overline{T} \otimes \alpha) = 0$ by the local Euler characteristic formula.

The pairings $\langle\ ,\ \rangle$, $\langle\ ,\ \rangle'$ 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 (resp. the third) congruence follows from (2.2.2) (resp. 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 $(W \otimes \alpha)_v = W_v$ ($W = V, V'$), 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 [D, Thm. 6.5], the isomorphism $\overline{T}' \otimes \alpha \xrightarrow{\sim} \overline{T} \otimes \alpha$ implies that $\varepsilon_v(V \otimes \alpha), \varepsilon_v(V' \otimes \alpha) \in \{\pm 1\}$ are congruent modulo p, therefore they are equal to each other.

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

2.3.1. representations V and V' which satisfy the assumption (1) of Theorem 1.1;
2.3.2. a G_F-stable $\mathcal{O}$-lattice $T \subset V$ which is self-dual with respect to $\langle\ ,\ \rangle : T \times T \longrightarrow \mathcal{O}(1)$,
2.3.3. and for which $\overline{T} = T \otimes_{\mathcal{O}} k$ is an absolutely irreducible representation of G_F;
2.3.4. a dense set of elements $g \in G_F$ for which $\mathrm{Tr}(g \mid V) \equiv \mathrm{Tr}(g \mid V') \pmod{t\mathcal{O}}$.

The condition 2.3.4 implies that, for any G_F-stable $\mathcal{O}$-lattice $T' \subset V'$, the semi-simplification $\overline{T}'^{ss}$ of $\overline{T}'$ is isomorphic to $\overline{T}^{ss}$, which is in turn equal to $\overline{T}$, by 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 2.3.3). Irreducibility of $\overline{T}'$ implies that any G_F-stable $\mathcal{O}$-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 $\langle\ ,\ \rangle$ (resp. by $\langle\ ,\ \rangle'$ and u) coincide up to a multiplicative factor $b \in k^\times$ (by 2.3.3). After multiplying $\langle\ ,\ \rangle'$ by a suitable element of $\mathcal{O}^\times$, 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 $\mathfrak{n}$, 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 $PGL_2(\mathbf{A}_F)$ associated to g:

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

As 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:

$$L(\pi(g),s) = \varepsilon(\pi(g),s)\, L(\pi(g),1-s), \qquad (-1)^{r_{\mathrm{an}}(F,g)} = \varepsilon(\pi(g),\tfrac{1}{2}) = \prod_v \varepsilon_v(\pi(g)_v,\tfrac{1}{2}).$$

If L, $L_{\mathfrak{p}}$ and $V_{\mathfrak{p}}(g)$ are as in Theorem B (with an appropriate modification if $F \neq \mathbf{Q}$; 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 ([BK], [FoPR]) predict that

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

We are interested in this conjecture modulo 2:

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

3.2. Let $g \in S_k(\mathfrak{n},1)$ be as in 3.1. If F'/F is a quadratic extension and $\alpha : \mathrm{Gal}(F'/F) \stackrel{\sim}{\longrightarrow} \{\pm 1\}$ 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

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

where we have denoted, somewhat abusively, by $g' = g\otimes F'$ the base change of g to an automorphic form on $PGL_2(\mathbf{A}_{F'})$ 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 $PGL_2(\mathbf{A}_{F'})$ attached to g' which is the base change of $\pi(g)$).

3.3. Proof of Theorem B. The statement for $r=1$ is a special case of Theorem 1.4(a). If $r>1$, then it follows from [R, Thm. 2.1, Thm. 2.2, Cor. 3.2] (the author would like to thank F. Diamond for pointing out this reference) and 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 which satisfies, for a suitable prime $\mathfrak{p}' \mid \mathfrak{p}$ of L',

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

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 $\mathcal{K} = L'_{\mathfrak{p}'}$, $\mathcal{O} = \mathcal{O}_{\mathcal{K}}$, $V = V_{\mathfrak{p}}(g)(r)\otimes_{L_{\mathfrak{p}}}\mathcal{K}$ and $V' = V_{\mathfrak{p}'}(g')(1) = V_{\mathfrak{p}'}(g_1)(1)\otimes\omega^{r-1}$.

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

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

whenever $\alpha : G_{\mathbf{Q}} \longrightarrow \{\pm 1\}$ is a character satisfying

$$\forall l \mid pN \qquad \alpha_l = 1. \tag{3.3.2}$$

According to Theorem 1.4(a),

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

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

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

It follows from the non-vanishing results of [Wa, Thm. 4] and [FH, Thm. B.1] that there exists a character α satisfying (3.3.2) for which $r_{\mathrm{an}}(\mathbf{Q}, g \otimes \alpha) = 0$. A fundamental result of Kato [Ka, Thm. 14.2(2)] then implies that $H^1_f(\mathbf{Q}, V \otimes \alpha) = 0$. The congruence (3.3.4) for this particular α becomes

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

which proves Theorem B.

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

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

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

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

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

$$\varepsilon_l(g) = \mu(-1) = 1 = \mu'(-1) = \varepsilon_l(g'), \qquad \varepsilon_l(g \otimes \alpha) = (\mu\alpha_l)(-1) = \alpha_l(-1) = (\mu'\alpha_l)(-1) = \varepsilon_l(g' \otimes \alpha),$$

which completes the proof of (3.4.1).

3.5. Theorem. *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 $2 \mid [F : \mathbf{Q}]$, 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 3.6 below);*
(2) *g has complex multiplication: g is the theta series attached to an algebraic Hecke character $\mathbf{A}^\times_{K(g)} \longrightarrow L'^\times$, where $K(g)$ (resp. L') is a totally imaginary quadratic extension of F (resp. of L), $\mathfrak{p}$ splits in L'/L and $V_{\mathfrak{p}}(g)|_{G_{K(g)}} = \psi_1 \oplus \psi_2$, where $\psi_i : G_{K(g)} \longrightarrow L^\times_{\mathfrak{p}}$ 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 2.3.1–2.3.3. The level raising machinery [T1] together with [DS, 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

$$\forall v \nmid p\mathfrak{n}\mathfrak{q} \qquad \lambda_v(g') \equiv \lambda_v(g) \pmod{\mathfrak{p}'},$$

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

$$\forall v \mid p\mathfrak{n}\mathfrak{q} \qquad \alpha_v = 1, \tag{3.5.1}$$

that

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

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

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

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

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

for any quadratic character α satisfying (3.5.1). As in 3.3, it follows from [Wa, Thm. 4] and [FH, Thm. B.1] that there exists α satisfying (3.5.1) such that $r_{\mathrm{an}}(F,g\otimes\alpha) = 0$. A generalisation of [L, Thm. C] proved in [N7, Thm. B] implies that $H^1_f(F,V\otimes\alpha) = 0$ (this is where the assumptions (1) and (2) come in, by [N7, B.5.5(2)] and [N7, 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 [N7, App. B.3] that there exists a finite abelian group $\Gamma \subset \mathrm{Aut}(L/\mathbf{Q})$ 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

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

is equal to

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

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 [N7, 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 [N7, 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, let A be an abelian variety over F satisfying

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

For each finite prime $\mathfrak{p}$ of L the two-dimensional $L_{\mathfrak{p}}$-representation $V_{\mathfrak{p}}(A) := T_p(A)\otimes_{O_L\otimes\mathbf{Z}_p} L_{\mathfrak{p}}$ 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 $\iota(L) \subset \mathbf{C}$ (for some embedding $\iota : L \hookrightarrow \mathbf{C}$) and which satisfies

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

for one ($\iff$ 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

$$\forall \sigma \in \mathrm{Aut}(\mathbf{C}) \quad L(\sigma\iota A/F, s) = L({}^{\sigma}g, s).$$

4.2. The potential automorphy results of [BLGGT] (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 which is linearly disjoint from M/F such that $A \otimes_F F'$ is modular over F'.

As in [N2, 12.11.6] and [N6, Step 4], a minor improvement (use of Solomon's induction theorem [CR, Thm. 15.10] instead of the usual Brauer theorem) of an argument of Taylor [T2, proof of Cor. 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) $V_{\mathfrak{p}}(A) = \bigoplus_i n_i \,\mathrm{Ind}_{G_{F_i}}^{G_F}\left(V_{\mathfrak{p}}(A)|_{G_{F_i}}\right) = \bigoplus_i n_i \,\mathrm{Ind}_{G_{F_i}}^{G_F}\left(V_{\mathfrak{p}}(g_i)(1)\right)$ in the Grothendieck ring of $L_{\mathfrak{p}}[G_F]$-modules.

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

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

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

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

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

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

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

4.3. Theorem. *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 $2 \nmid [F : \mathbf{Q}]$.*
(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 $C := \mathrm{End}_{\overline{F}}(A) \otimes \mathbf{Q}$ 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 $\mathbf{Z}_p^{\times} \times \mathbf{Z}_p^{\times}$.*
(e) *$A[\mathfrak{p}]$ is a reducible G_F-module, $L_{\mathfrak{p}}/\mathbf{Q}_p$ is unramified and $p > 2[L_{\mathfrak{p}} : \mathbf{Q}_p] + 1$.*
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 $\tau : L \hookrightarrow \mathbf{C}$.

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

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

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 4.2 we ensure that $A[\mathfrak{p}]$ is irreducible as a G_{F_i}-module in the case (c) or (d)). The case (b) then follows from Theorem 1.4(b) and the cases (c) and (d) from Theorem 3.5 (using [N7, B.6.5(2)]). In the 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 [AT, ch. 10, Thm. 5]) good reduction over a suitable cyclic extension. The result then follows from an $O_{L,\mathfrak{p}}$-equivariant version of the proof of [CFKS, Thm. 2.1].

4.4. Proof of Theorem A. As in the proof of Theorem 4.3, potential modularity of E [Wi, Thm. A.1] together with (4.2.2-3) 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 [Wa, Thm. 4] and [FH, Thm. B.1] that there exists a non-trivial quadratic character $\alpha : G_F \longrightarrow \{\pm 1\}$ such that $r_{\mathrm{an}}(E \otimes \alpha/F) = 0$. This implies, by [N7, Cor. of Thm. B'], that $s_2(E \otimes \alpha/F) = 0$. Let F'/F be the quadratic extension corresponding to α. As

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

by [DD2, Cor. 4.8], we conclude by the following analogue of (3.2.1-2):

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

If $p \neq 2$, we can assume that $2 \mid [F : \mathbf{Q}]$, in view of [N6, Thm. 1(a)]. Theorem 4.3(c),(d) (resp. (e)) then implies the desired result if $E[p]$ is an irreducible G_F-module (resp. 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 [DD2, Cor. 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 [MR2, Thm. 6.4, 7.1], [MR3, Thm. 1.1], [DD1, Thm. 4.3, 4.5], [DD2, Prop. 6.12], [G, §11.8] and [Ro, Thm. 2.1].

4.6. Note that 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: [AN], [N7] and [YZZ] (used in the proof of [N7, Thm. B(b)]). It would be desirable to have a more direct proof in the reducible case.

4.7. The conclusion of Theorem A also holds in the case when E has complex multiplication (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 $PGL_2(F_v)$ is a square).

References

[AN] E. Aflalo, J. Nekovář, *Non-triviality of CM points in ring class field towers*, Israel J. Math. **175** (2010), 225–284.

[AT] E. Artin, J. Tate, *Class field theory*, Second ed., Addison-Wesley, Redwood City, 1990.

[BLGGT] T. Barnet-Lamb, T. Gee, D. Geraghty, R. Taylor, *Potential automorphy and change of weight*, preprint, version of 10th October 2010.

[BK] S. Bloch, K. Kato, *L-functions and Tamagawa numbers of motives*, in: The Grothendieck Festschrift I, Progress in Mathematics **86**, Birkhäuser, Boston, Basel, Berlin, 1990, pp. 333–400.

[CFKS] J. Coates, T. Fukaya, K. Kato, R. Sujatha, *Root numbers, Selmer groups and non-commutative Iwasawa theory*, J. Alg. Geom. **19** (2010), 19–97.

[CR] C.W. Curtis, I. Reiner, *Methods of Representation Theory, Vol. I*, Wiley, New York, 1981.

[CV] C. Cornut, V. Vatsal, *Nontriviality of Rankin-Selberg L-functions and CM points*, in: L-functions and Galois representations (Durham, July 2004), LMS Lecture Note Series **320**, Cambridge Univ. Press, 2007, pp. 121–186.

[D] P. Deligne, *Les constantes des équations fonctionnelles des fonctions L*, in: Modular functions of one variable II (Antwerp, 1972), Lect. Notes in Math. **349**, Springer, Berlin, 1973, pp. 501–597.

[DS] P. Deligne, J.-P. Serre, *Formes modulaires de poids* 1, Ann. Sci. E.N.S. (4) **7** (1974), 507–530.

[DD1] T. Dokchitser, V. Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math. **178** (2009), 23–71.

[DD2] T. Dokchitser, V. Dokchitser, *Root numbers and parity of ranks of elliptic curves*, J. reine angew. Math. **658** (2011), 39-64.

[Fl] M. Flach, *A generalization of the Cassels-Tate pairing*, J. reine angew. Math. **412** (1990), 113–127.

[Fo] J.-M. Fontaine, *Représentations ℓ-adiques potentiellement semi-stables*, in: Périodes p-adiques (Bures-sur-Yvette, 1988), Astérisque **223** (1994), Soc. Math. de France, Paris, pp. 321–347.

[FoPR] J.-M. Fontaine, B. Perrin-Riou, *Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L*, in: Motives (Seattle, 1991), Proc. Symposia in Pure Math. **55/I**, American Math. Society, Providence, Rhode Island, 1994, pp. 599–706.

[FH] S. Friedberg, J. Hoffstein, *Nonvanishing theorems for automorphic L-functions on $GL(2)$*, Ann. of Math. (2) **142** (1995), 385–423.

[G] R. Greenberg, *Iwasawa theory, projective modules, and modular representations*, Memoirs Amer. Math. Soc. **211** (2011), no. 992.

[Ka] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, in: Cohomologies p-adiques et applications arithmétiques III, Astérisque **295** (2004), Soc. Math. de France, Paris, pp. 117–290.

[Ki] 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 Th. **129** (2009), 1149–1160.

[L] M. Longo, *On the Birch and Swinnerton-Dyer conjecture for modular elliptic curves over totally real fields*, Ann. Inst. Fourier **56** (2006), 689–733.

[MR1] B. Mazur, K. Rubin, *Kolyvagin Systems*, Memoirs Amer. Math. Soc. **168** (2004), no. 799.

[MR2] B. Mazur, K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Ann. of Math. (2) **166** (2007), 581–614.

[MR3] B. Mazur, K. Rubin, *Growth of Selmer rank in nonabelian extensions of number fields*, Duke Math. J. **143** (2008), 437–461.

[N1] J. Nekovář, *On the parity of ranks of Selmer groups II*, C.R.A.S. Paris, Sér. I Math. **332** (2001), no. 2, 99–104.

[N2] J. Nekovář, *Selmer complexes*, Astérisque **310** (2006), Soc. Math. de France, Paris.

[N3] J. Nekovář, *The Euler system method for CM points on Shimura curves*, in: L-functions and Galois representations (Durham, July 2004), LMS Lecture Note Series **320**, Cambridge Univ. Press, 2007, pp. 471–547.

[N4] J. Nekovář, *On the parity of ranks of Selmer groups III*, Doc. Math. **12** (2007), 243–274. Erratum: Doc. Math. **14** (2009), 191–194.

[N5] J. Nekovář, *Growth of Selmer groups of Hilbert modular forms over ring class fields*, Ann. Sci. E.N.S. (4) **41** (2008), 1003–1022.

[N6] J. Nekovář, *On the parity of ranks of Selmer groups IV*, Compositio Math. **145** (2009), 1351–1359.

[N7] J. Nekovář, *Level raising and anticyclotomic Selmer groups for Hilbert modular forms of weight two*, Canadian J. Math **64** (2012), 588–668.

[R] K. Ribet, *Report on mod l representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, in: Motives (Seattle, 1991), Proc. Symposia in Pure Math. **55/II**, American Math. Society, Providence, Rhode Island, 1994, pp. 639–676.

[Ro] T. de La Rochefoucauld, *Invariance of the parity conjecture for p-Selmer groups of elliptic curves in a D_{2p^n}-extension*, Bull. S.M.F. **139** (2011), 571–592.

[T1] R. Taylor, *On Galois representations associated to Hilbert modular forms*, Inv. Math. **98** (1989), 265–280.

[T2] R. Taylor, *Remarks on a conjecture of Fontaine and Mazur*, J. Inst. Math. Jussieu **1** (2002), 1–19.

[Wa] J.-L. Waldspurger, *Correspondances de Shimura et quaternions*, Forum Math. **3** (1991), 219–307.

[Wi] J.-P. Wintenberger, *Potential modularity of elliptic curves over totally real fields*, appendix to [N6].

[YZZ] X. Yuan, S.-W. Zhang, W. Zhang, *Heights of CM points I. Gross-Zagier formula*, preprint, 2008.

Université Pierre et Marie Curie (Paris 6)
Institut de Mathématiques de Jussieu
Théorie des Nombres, Case 247
4, place Jussieu
F-75252 Paris cedex 05
FRANCE