Growth of Selmer groups of Hilbert modular forms over ring class fields

Jan Nekovář

0. Introduction

0.1. Fix an algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$, a prime number p and embeddings $i_\infty : \overline{\mathbf{Q}} \hookrightarrow \mathbf{C}$ and $i_p : \overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$.

Let F be a totally real number field and $g \in S_k(\mathfrak{n}, 1)$ a cuspidal Hilbert modular newform over F of parallel weight k, trivial character (which implies that k is even) and (exact) level $\mathfrak{n}$.

Let K be a totally imaginary quadratic extension of F and $\chi : \mathbf{A}_K^*/K^*\mathbf{A}_F^* \longrightarrow \mathbf{C}^*$ a (continuous) character of finite order. Fix a number field $L \subset \overline{\mathbf{Q}}$ such that $i_\infty(L)$ contains all Hecke eigenvalues $\lambda_g(v)$ of g and all values of χ; denote by $\mathfrak{p}$ the prime of L above p induced by i_p.

Let $V(g) = V_{\mathfrak{p}}(g)$ be the two-dimensional representation of $G_F = \mathrm{Gal}(\overline{\mathbf{Q}}/F)$ with coefficients in $L_{\mathfrak{p}}$ attached to g: if $v \nmid \infty p\mathfrak{n}$ is a prime of F, then $V(g)$ is unramified at v and

$$\det\left(1 - \mathrm{Fr}(v)_{\mathrm{geom}}\, X \mid V(g)\right) = 1 - i_p(\lambda_g(v))X + (Nv)^{k-1}X^2.$$

The Tate twist $V = V(g)(k/2)$ is self-dual in the sense that there exists a skew-symmetric isomorphism $V \xrightarrow{\sim} V^*(1) = \mathrm{Hom}_{L_{\mathfrak{p}}}(V, L_{\mathfrak{p}})(1)$.

Denote by $\eta = \eta_{K/F} : \mathbf{A}_F^*/F^* N_{K/F}\mathbf{A}_K^* \xrightarrow{\sim} \{\pm 1\}$ the quadratic character corresponding to the extension K/F.

0.2. Normalising the reciprocity map $\mathrm{rec}_K : \mathbf{A}_K^*/K^* \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$ so that the local uniformisers correspond to geometric Frobenius elements, we identify χ with the coresponding Galois character $\chi : G_K = \mathrm{Gal}(\overline{\mathbf{Q}}/K) \longrightarrow O_L^* \subset L_{\mathfrak{p}}^*$; put $K_\chi = \overline{\mathbf{Q}}^{\mathrm{Ker}(\chi)}$. There are canonical isomorphisms

$$H^1_f(K, V \otimes \chi^{\pm 1}) \xrightarrow{\sim} (H^1_f(K_\chi, V) \otimes \chi^{\pm 1})^{\mathrm{Gal}(K_\chi/K)} = H^1_f(K_\chi, V)^{(\chi^{\mp 1})},$$

where $H^1_f(-)$ are the Bloch-Kato Selmer groups and

$$M^{(\chi)} = \{m \in M \mid \forall \sigma \in \mathrm{Gal}(K_\chi/K) \quad \sigma(m) = \chi(\sigma)m\},$$

for any $O_L[\mathrm{Gal}(K_\chi/K)]$-module M. The action of the complex conjugation $\rho \in \mathrm{Gal}(K_\chi/F)$ on $H^1_f(K_\chi, V)$ interchanges the eigenspaces $H^1_f(K_\chi, V)^{(\chi^{\pm 1})}$, which implies that their dimensions

$$h^1_f(K, V \otimes \chi^{\pm 1}) := \dim_{L_{\mathfrak{p}}} H^1_f(K, V \otimes \chi^{\pm 1})$$

are equal to each other: $h^1_f(K, V \otimes \chi) = h^1_f(K, V \otimes \chi^{-1})$.

0.3. Denote by $\pi = \pi(g)$ the (irreducible, cuspidal) automorphic representation of $GL_2(\mathbf{A}_F)$ generated by g, and by θ_χ the automorphic representation of $GL_2(\mathbf{A}_F)$ generated by the theta series of χ. They are both self-dual, as the central character of π (resp., of θ_χ) is trivial (resp., is equal to $\eta = \eta_{K/F}$, and $\theta_\chi \otimes \eta = \theta_\chi$).

The Rankin-Selberg L-function $L(\pi \times \theta_\chi, s)$ has Euler factors

$$L_v(\pi \times \theta_\chi, s) = \prod_{w \mid v} \det(1 - \mathrm{Fr}(w)_{\mathrm{geom}}\, (Nw)^{1/2-s} \mid (V \otimes \chi)^{I_w})^{-1},$$

where $v \nmid \infty p$ is a prime of F and w a prime of K (cf. [N 1, 12.6.2.2]). We shall abuse the notation and write $L_v(\pi \times \chi, s)$ instead of $L_v(\pi \times \theta_\chi, s)$. The complete L-function $L(\pi \times \chi, s) = \prod_v L_v(\pi \times \chi, s)$ is equal to $L(\pi \times \chi^{-1}, s)$, has holomorphic continuation to $\mathbf{C}$ and a functional equation of the form

$$L(\pi \times \chi, s) = \varepsilon(\pi \times \chi, s)\, L(\pi \times \chi, 1 - s),$$
$$\varepsilon(\pi \times \chi, s) = c(\pi \times \chi)^{1/2-s}\, \varepsilon(\pi \times \chi, \tfrac{1}{2}), \qquad \varepsilon(\pi \times \chi, \tfrac{1}{2}) \in \{\pm 1\}.$$

Put

$$r_{\rm an}(K,g,\chi) := {\rm ord}_{s=1/2}\, L(\pi\times\chi,s) = {\rm ord}_{s=1/2} \prod_{v\nmid\infty} L_v(\pi\times\chi,s)$$

(the Γ-factors $L_v(\pi\times\chi,s)$ for $v \mid \infty$ take finite non-zero values at $s=1/2$).

The conjectures of Bloch and Kato ([B-K], [F-PR]) predict that

$$r_{\rm an}(K,g,\chi) \stackrel{?}{=} h^1_f(K, V\otimes\chi). \tag{0.3.1}$$

The main result of the present article is the following theorem.

0.4. Theorem. *Assume that $g\in S_k(\mathfrak{n},1)$ is potentially p-ordinary, i.e., that there exists a finite solvable extension of totally real number fields F'/F such that the base change $BC_{F'/F}(\pi(g))$ is equal to $\pi(g')$, where g' is a p-ordinary (cuspidal) Hilbert eigenform over F' (equivalently, that there exists a character of finite order $\varphi : \mathbf{A}_F^*/F^* \longrightarrow \overline{\mathbf{Q}}^*$ such that the newform associated to $g\otimes\varphi$ is p-ordinary; see [N 1, 12.5.10]). If g has complex multiplication by a totally imaginary quadratic extension K' of F, assume, in addition, that $p\neq 2$ and that $K'\not\subset K_\chi$. Then:*
(1) If $2\nmid r_{\rm an}(K,g,\chi)$, then $2\nmid h^1_f(K,V\otimes\chi)$.
(2) If $2\mid r_{\rm an}(K,g,\chi)$ and if there exists a prime $v\mid p$ of F which does not split in K/F and for which $\pi(g)_v = {\rm St}\otimes\mu$, $\mu : F_v^* \longrightarrow \{\pm1\}$, $\chi_w = \mu\circ N_{K_w/F_v}$, where w is the unique prime of K above v (as g is potentially ordinary, this can occur only if $k=2$; see [N 1, 12.5.4]), then $2\mid h^1_f(K,V\otimes\chi)$.
[The hypothesis in (2) can be interpreted as saying that the Euler factor at v of the p-adic counterpart of $L(\pi\times\chi,s)$ has a trivial zero of odd order at the central point; cf. [N 1, 12.6.3.10] and [N 1, 12.6.4.3].]

0.5. Corollary. *Let $K[\infty]\subset K^{\rm ab}$ be the union of all ring class fields of K in the sense of [A-N, 1.1] (the Galois group ${\rm Gal}(K[\infty]/K)$ is the quotient of ${\rm Gal}(K^{\rm ab}/K)$ by ${\rm rec}_K(\mathbf{A}_F^*)$). Let K_0/K be a finite subextension of $K[\infty]/K$. Assume that $g\in S_k(\mathfrak{n},1)$ is potentially p-ordinary; if g has complex multiplication by a totally imaginary quadratic extension K' of F, assume, in addition, that $p\neq 2$ and that $K'\not\subset K_0$. Then*

$$h^1_f(K_0,V) := \dim_{L_\mathfrak{p}}\, H^1_f(K_0,V) \geq |X^-(g,K_0)|,$$

where

$$X^\pm(g,K_0) = \{\chi : {\rm Gal}(K_0/K) \longrightarrow \mathbf{C}^* \mid \varepsilon(\pi(g)\times\chi,\tfrac{1}{2}) = \pm1\}.$$

0.6. Example. Let E be an elliptic curve over F. It is expected that E is modular in the sense that there exists $g\in S_2(\mathfrak{n},1)$ such that $L_v(E/F,s) = L_v(\pi(g),s+1/2)$, for all primes v of F. If this is the case, assume that E has potentially ordinary reduction (= potentially good ordinary or potentially multiplicative reduction) at all primes of F above p. If E has complex multiplication by $\mathbf{Q}(\sqrt{-D})$, assume, in addition, that $p\neq 2$ and $F(\sqrt{-D})\not\subset K_\chi$. Theorem 0.4 then implies the following:

(1) If $2\nmid {\rm ord}_{s=1}\, L(E/K,\chi,s)$, then $2\nmid \Big(\dim_L(E(K_\chi)\otimes L)^{(\chi^{-1})} + {\rm cork}_{O_{L,\mathfrak{p}}}(Ш(E/K_\chi)\otimes O_{L,\mathfrak{p}})^{(\chi^{-1})}\Big)$.
(2) If $2\mid {\rm ord}_{s=1}\, L(E/K,\chi,s)$ and if there exists a prime $v\mid p$ of F which does not split in K/F and a character $\mu : F_v^*\longrightarrow\{\pm1\}$ such that $\chi_w = \mu\circ N_{K_w/F_v}$ and the quadratic twist $E\otimes\mu$ has split multiplicative reduction at v, then $2\mid \Big(\dim_L(E(K_\chi)\otimes L)^{(\chi^{-1})} + {\rm cork}_{O_{L,\mathfrak{p}}}(Ш(E/K_\chi)\otimes O_{L,\mathfrak{p}})^{(\chi^{-1})}\Big)$.

There is an obvious variant of this statement when E is replaced by an abelian variety A_0 with $O_{L_0}\hookrightarrow {\rm End}_F(A_0)$, where L_0 is a totally real number field of degree $[L_0:\mathbf{Q}] = \dim(A_0)$.

0.7. Example [D]. Let $q\neq 2$ be a prime number and F_0 a totally real number field such that $F_0\cap\mathbf{Q}(\mu_{q^\infty}) = \mathbf{Q}$. Let $a\in O_{F_0} - \{0\}$ be an element satisfying $a\notin F_0^{*q}$ and, for each finite prime v_0 of F_0 not dividing q, ${\rm ord}_{v_0}(a) < q$. For each $r\geq 1$, put $F_r = F_0\mathbf{Q}(\mu_{q^r})^+$, $K_r = F_0(\mu_{q^r})$; then ${\rm Gal}(K_r/F_0) \xrightarrow{\sim} (\mathbf{Z}/q^r\mathbf{Z})^*$ and ${\rm Gal}(K_r(\sqrt[q^r]{a})/K_r) \xrightarrow{\sim} \mathbf{Z}/q^r\mathbf{Z}$. Fix an injective character $\chi_r : {\rm Gal}(K_r(\sqrt[q^r]{a})/K_r) \longrightarrow \overline{\mathbf{Q}}^*$; then χ_r (more precisely, $\chi_r\circ{\rm rec}_{K_r}$) factors through $\mathbf{A}_{K_r}^*/K_r^*\mathbf{A}_{F_r}^*$.

Let $g_0\in S_k(\mathfrak{n}_0,1)$ be a cuspidal Hilbert newform over F_0 of parallel weight k, trivial character and level $\mathfrak{n}_0$; put $V = V_\mathfrak{p}(g_0)(k/2)$. For $r\geq 1$, denote by g_r the corresponding base change newform over F_r (i.e., $BC_{F_r/F}(\pi(g_0)) = \pi(g_r)$). An easy exercise in group theory (see §3.1 below) shows that, for each $r\geq 1$,

$$H^1_f(F_0(\sqrt[q^r]{a}), V) = H^1_f(F_0, V) \oplus \bigoplus_{s=1}^{r} H^1_f(K_s, V \otimes \chi_s).$$

0.8. Theorem. *In the notation of 0.7, assume that* $(\forall v_0 | q)$ $\pi(g_0)_{v_0}$ *is a principal series representation and that* $(\forall v_0 | a)$ $\pi(g_0)_{v_0}$ *is not supercuspidal. Put* $\mathfrak{n}_0^{(aq)} = \mathfrak{n}_0/(\mathfrak{n}_0, (aq)^\infty)$ *and* $d = (-1)^{[F_0:\mathbf{Q}]} N(\mathfrak{n}_0^{(aq)}) \in \mathbf{Z} - \{0\}$. *Then:*
(1) *For each* $r \geq 1$, $\varepsilon(\pi(g_r) \times \chi_r, \frac{1}{2}) = \left(\frac{d}{q}\right)$. *[See [D, Thm. 6] for a special case.]*
(2) *Assume that* g_0 *is potentially* p*-ordinary. If* g_0 *has complex multiplication by a totally imaginary quadratic extension* K'_0 *of* F_0*, assume that* $p \neq 2$ *and that* ($q \equiv 1 \pmod 4$ *or* $K'_0 \neq F_0(\sqrt{-q})$) *[the latter condition is automatically satisfied if* $2 \nmid [F_0 : \mathbf{Q}]$*]. If* $\left(\frac{d}{q}\right) = -1$, *then*

$$\forall r \geq 0 \qquad h^1_f(F_0(\sqrt[q^r]{a}), V) - h^1_f(F_0, V) \geq r, \qquad h^1_f(F_0(\sqrt[q^r]{a}), V) - h^1_f(F_0, V) \equiv r \pmod 2,$$
$$h^1_f(F_0(\mu_{q^r}, \sqrt[q^r]{a}), V) - h^1_f(F_0, V) \geq q^r - 1.$$

0.9. Corollary. *In the notation of 0.7, assume that* E *is a modular elliptic curve over* F_0 *such that for each prime* v_0 *of* F_0 *above* q *(resp., dividing* a*) there exists a quadratic twist of* E *with good reduction (resp., semistable reduction) at* v_0*. If* E *has complex multiplication, assume that* $p \neq 2$ *and that* ($q \equiv 1 \pmod 4$ *or* $F_0 \otimes \mathrm{End}_{\overline{\mathbf{Q}}}(E) \neq F_0(\sqrt{-q})$) *[the latter condition is automatically satisfied if* $2 \nmid [F_0 : \mathbf{Q}]$*]. Assume, finally, that* $\left(\frac{d}{q}\right) = -1$, *where* $d = (-1)^{[F_0:\mathbf{Q}]} N(\mathrm{cond}(E)^{(aq)})$*. Then, for each prime number* p *such that* E *has potentially ordinary reduction at all primes of* F_0 *above* p*, the ranks*

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

satisfy

$$\forall r \geq 0 \qquad s_p(E/F_0(\sqrt[q^r]{a})) - s_p(E/F_0) \geq r, \qquad s_p(E/F_0(\sqrt[q^r]{a})) - s_p(E/F_0) \equiv r \pmod 2,$$
$$s_p(E/F_0(\mu_{q^r}, \sqrt[q^r]{a})) - s_p(E/F_0) \geq q^r - 1.$$

0.10. Remarks. (1) The proof of Theorem 0.4 does not use any explicit formula for the global root number $\varepsilon(\pi(g) \times \chi, \frac{1}{2})$ (in fact, such a formula is not available in general). Instead, the local root numbers enter the picture indirectly, through their representation-theoretical characterisation ([T], [W, Thm. 2], [S]) that appears in a refinement of the method of Cornut and Vatsal ([A-N]).
(2) A suitable strenghtening of the methods of [M-R] or [D-D2] would allow us to drop the assumption of potentially ordinary reduction at p in Example 0.6 (if the order of χ is a power of p, this can be done, in many cases, by combining [M-R, Thm. 6.4], [D-D2, Thm. 4.3] and [N 4, Thm. 1]).
(3) In the special case $p = q$ there are more elementary approaches to Corollary 0.9 ([M-R, Thm. 7.1], [D-D1, Prop. 4.13], [C-F-K-S, Thm. 4.2, 4.6]), which do not require E to be modular but instead assume that $s_p(E/F_0(\mu_p)) \equiv \mathrm{ord}_{s=1} L(E/F_0(\mu_p), s) \pmod 2$, which under fairly general circumstances follows from [N 4, Thm. 1].
(4) If $\chi^2 = 1$, then $\chi = \varphi \circ N_{K/F}$, where $\varphi : \mathbf{A}_F^*/F^* \longrightarrow \{\pm 1\}$, and

$$H^1_f(K, V \otimes \chi) = H^1_f(F, V \otimes \varphi) \oplus H^1_f(F, V \otimes \varphi\eta_{K/F}).$$

In many cases [N 1, Thm. 12.2.3] applies to $g \otimes \varphi$ and $g \otimes \varphi\eta_{K/F}$, yielding

$$r_{\mathrm{an}}(K, g, \chi) \equiv h^1_f(K, V \otimes \chi) \pmod 2.$$

1. Proof of Theorem 0.4

In this section we prove Theorem 0.4., following closely the arguments in [N 1, §12.9]. The main difference is that the non-vanishing results of [C-V, §4] are replaced by their strenghtening proved in [A-N]. We are going to use the notation from [A-N] and [N 1, ch. 12].

Assume that $g \in S_k(\mathfrak{n}, 1)$ is potentially p-ordinary and, if g has complex multiplication by a totally imaginary quadratic extension K' of F, that $p \neq 2$ and $K' \not\subset K_\chi$. Put $\pi = \pi(g)$, $\eta = \eta_{K/F}$, $\varepsilon_v = \varepsilon(\pi_v \times \chi_v, \frac{1}{2}) \in \{\pm 1\}$ and $\varepsilon = \varepsilon(\pi \times \chi, \frac{1}{2}) = \prod_v \varepsilon_v$. Note that ε_v does not depend on the choice of an additive character, by the self-duality of $V \otimes \mathrm{Ind}_{K/F}(\chi)$ ([N 3, 2.2.1(1)]).

1.1. Reduction steps

1.1.1. Let Σ_p (resp., $\Sigma_\infty = \{\tau_1, \ldots, \tau_d\}$, $d = [F : \mathbf{Q}]$) be the set of all primes of F above p (resp., above ∞). Put

$$\Sigma_\chi = \Sigma_\chi(g) = \{v \in \Sigma_p \mid v \text{ does not split in } K/F,\ \pi_v = \mathrm{St} \otimes \mu,\ \mu : F_v^* \longrightarrow \{\pm 1\},\ \chi_w = \mu \circ N_{K_w/F_v}\}$$

(where w is the unique prime of K above v). As g is potentially p-ordinary, π_v is not supercuspidal for any $v \in \Sigma_p$, which implies that

$$\forall v \in \Sigma_p \qquad \eta_v(-1)\,\varepsilon_v = \begin{cases} -1, & v \in \Sigma_\chi \\ 1, & v \notin \Sigma_\chi \end{cases} \tag{1.1.1.1}$$

(see [N 1, 12.6.2.4]). At the archimedean primes,

$$\forall v \in \Sigma_\infty \qquad \eta_v(-1) = -1, \qquad \varepsilon_v = 1. \tag{1.1.1.2}$$

1.1.2. Reduction to the case $k = 2$. Assume that $k > 2$ and that Theorem 0.4 has been proved for $k = 2$. As in [N 1, 12.9.5.1], let $g' \in S_2(\mathfrak{n}', 1)$ be a weight 2 specialisation of the twisted Hida family containing a twist of the p-stabilisation of a p-ordinary twist of g; put $\pi' = \pi(g')$, $V' = V_{\mathfrak{p}}(g')(1)$. As $k > 2$, we have $\Sigma_\chi(g) = \emptyset$ ([N 1, Lemma 12.5.4]). According to [N 1, 12.7.14.5(v),(ii),(iii)] (combined with (2.2.3.1) below),

1.1.2.1. g has complex multiplication by K' $\iff$ g' has complex multiplication by K';
1.1.2.2. $r_{\mathrm{an}}(K, g, \chi) = r_{\mathrm{an}}(K, g, \chi) + |\Sigma_\chi(g)| \equiv r_{\mathrm{an}}(K, g', \chi) + |\Sigma_\chi(g')| \pmod 2$.
1.1.2.3. $h^1_f(K, V \otimes \chi) = h^1_f(K, V \otimes \chi) + |\Sigma_\chi(g)| \equiv h^1_f(K, V' \otimes \chi) + |\Sigma_\chi(g')| \pmod 2$.

As Theorem 0.4 holds for g' by assumption, the statements 1.1.2.1-3 imply that it also holds for g (in fact, one can always choose g' satisfying $\Sigma_\chi(g') = \emptyset$, by [N 1, 12.7.10]).

1.1.3. Further reduction in the case $k = 2$ (cf. [N 1, 12.10.1]). From now on, until the end of §1, $k = 2$. Assume that Theorem 0.4 has been proved for $k = 2$ under the following additional assumption:

$$\exists\, \Sigma \subseteq \Sigma_p,\ \Sigma \neq \emptyset \qquad (-1)^{|\Sigma \cap \Sigma_\chi| - 1} = \varepsilon(\pi \times \chi, \tfrac{1}{2}) = \varepsilon. \tag{1.1.3.1}$$

There is precisely one case in which the assumptions of Theorem 0.4 ($\varepsilon = -1$ or $|\Sigma_\chi| \neq 0$) are satisfied, but (1.1.3.1) is not:

$$|\Sigma_\chi| = |\Sigma_p| = 1, \qquad \varepsilon = -1.$$

In this case fix a totally real cyclic extension F_1/F of odd order $n > 1$ in which the unique prime $v \in \Sigma_p$ splits completely and put $K_1 = F_1 K$, $\chi_1 = \chi \circ N_{K_1/K} : \mathbf{A}^*_{K_1}/K_1^* \mathbf{A}^*_{F_1} \longrightarrow \mathbf{C}^*$ (thus $(K_1)_{\chi_1} = F_1 K_\chi$), $\pi_1 = BC_{F_1/F}(\pi) = \pi(g_1)$, $\Delta = \mathrm{Gal}(F_1/F) = \mathrm{Gal}(K_1/K)$, $\widehat{\Delta} = \mathrm{Hom}(\Delta, \mathbf{C}^*)$. As g is potentially p-ordinary, so is the base change form g_1 over F_1. Furthermore, if g has complex multiplication by K' ($[K' : F] = 2$), then g_1 has complex multiplication by $F_1 K'$, and

$$K' \not\subset K_\chi \iff F_1 K' \not\subset F_1 K_\chi = (K_1)_{\chi_1}. \tag{1.1.3.2}$$

We have

$$\varepsilon(\pi_1 \times \chi_1, \tfrac{1}{2}) = \prod_{\alpha \in \widehat{\Delta}} \varepsilon(\pi \times (\theta_\chi \otimes \alpha), \tfrac{1}{2}), \qquad h^1_f(K_1, V \otimes \chi_1) = \sum_{\alpha \in \widehat{\Delta}} h^1_f(K, V \otimes \chi\alpha).$$

As

$$\varepsilon(\pi \times (\theta_\chi \otimes \alpha^{-1}), \tfrac{1}{2}) = \varepsilon(\pi \times (\theta_\chi \otimes \alpha), \tfrac{1}{2})^{-1}$$

by the functional equation, it follows that

$$\text{(1.1.3.3)} \qquad r_{\mathrm{an}}(K, g_1, \chi_1) \equiv r_{\mathrm{an}}(K, g, \chi) \pmod 2.$$

Similarly,

$$\begin{aligned} h^1_f(K, V \otimes \chi\alpha) &= h^1_f(K, V^*(1) \otimes \chi^{-1}\alpha^{-1}) = h^1_f(K, V \otimes \chi^{-1}\alpha^{-1}) \qquad ([\mathrm{N1}, 12.5.9.5(\mathrm{iv})]) \\ &= h^1_f(K, V \otimes \chi\alpha^{-1}) \end{aligned}$$

(the last equality follows from the fact that the action of the complex conjugation $\rho \in \mathrm{Gal}(F_1K_\chi/F)$ interchanges the $\chi\alpha$- and $\chi^{-1}\alpha$-eigenspaces for the action of $\mathrm{Gal}(F_1K_\chi/K)$ on $H^1_f(F_1K_\chi, V)$), which implies that

$$\text{(1.1.3.4)} \qquad h^1_f(K_1, V \otimes \chi_1) \equiv h^1_f(K, V \otimes \chi) \pmod 2.$$

Finally,

$$\text{(1.1.3.5)} \qquad \Sigma_{\chi_1}(g_1) = \{v_1 \mid v,\ v \in \Sigma_\chi(g)\}.$$

Putting (1.1.3.2-5) together, we obtain that Theorem 0.4 holds for g iff it holds for g_1. However, g_1 satisfies (1.1.3.1), as there are $n > 1$ primes above p in F_1. This concludes the proof of the reduction step to the case when (1.1.3.1) holds.

1.2. Passage to a Shimura curve

1.2.1. Thanks to 1.1, we can (and will) assume that $k = 2$ and that there exists a non-empty subset $\Sigma = \{P_1, \ldots, P_s\} \subseteq \Sigma_p$ for which (1.1.3.1) holds; fix such Σ (in fact, we can always take $s = 1$ or $s = 2$). Our goal is to show that $r_{\mathrm{an}}(K, g, \chi) \equiv h^1_f(K, V \otimes \chi) \pmod 2$.

1.2.2. Choice of a quaternion algebra. As

$$\varepsilon = \prod_v \varepsilon_v = \prod_v \eta_v(-1)\,\varepsilon_v = \prod_{v \in \Sigma_\infty} \prod_{v \in \Sigma} \prod_{v \notin \Sigma \cup \Sigma_\infty} \eta_v(-1)\,\varepsilon_v = (-1)^{[F:\mathbf{Q}]}(-1)^{|\Sigma \cap \Sigma_\chi|} \prod_{v \notin \Sigma \cup \Sigma_\infty} \eta_v(-1)\,\varepsilon_v$$

(by (1.1.1.1-2)), the condition (1.1.3.1) implies that

$$\prod_{v \notin \Sigma \cup \Sigma_\infty} \eta_v(-1)\,\varepsilon_v = (-1)^{[F:\mathbf{Q}]-1}.$$

This means that there exists a (unique) quaternion algebra B over F with local invariants

$$\mathrm{inv}_v(B) = \begin{cases} 1, & v \in \Sigma \cup \{\tau_1\} \\ -1, & v \in \Sigma_\infty - \{\tau_1\} \\ \eta_v(-1)\,\varepsilon_v, & v \notin \Sigma \cup \Sigma_\infty. \end{cases}$$

1.2.3. Proposition. (1) *There exists a (unique) irreducible (cuspidal) automorphic representation* π' *of* $B^*_{\mathbf{A}}$ *such that* $\pi = JL(\pi')$ *is associated to* π' *by the Jacquet-Langlands correspondence. The representation* π' *has trivial central character,* $\pi'_v = 1$ *if* $v \in \Sigma_\infty - \{\tau_1\}$*, and* π'_{τ_1} *is the weight 2 holomorphic discrete series.*
(2) *There exists an* F*-embedding* $t : K \hookrightarrow B$*; fix such* t*.*
(3) $\forall v \notin \Sigma \cup \Sigma_\infty$ *there exists a non-zero* $t_v(K_v^*)$*-invariant linear form* $\ell_v : \pi'_v \longrightarrow \mathbf{C}(\chi_v^{-1})$*.*

Proof. (1) At each finite prime v of F at which π_v is a principal series representation we have $\eta_v(-1)\,\varepsilon_v = 1$ ([N 1, 12.6.2.4(i)]), hence B is unramified at v, by construction. This implies that π lies in the image of the Jacquet-Langlands correspondence. The central characters of π and π' coincide and the archimedean behaviour of π' follows from the coresponding local correspondence.
(2) At each finite prime v of F which splits in K/F we have $\eta_v(-1)\,\varepsilon_v = 1$ ([N 1, 12.6.2.4]); thus B is ramified only at primes of F that do not split in K/F, which implies the existence of t.
(3) By construction, $\mathrm{inv}_v(B) = \eta_v(-1)\,\varepsilon_v$ for each $v \notin \Sigma \cup \Sigma_\infty$; we apply the fundamental results of [T] and [W, Thm. 2] (see also [S]) (note that, if $\mathrm{inv}_v(B) = 1$, then $\dim(\pi'_v) = \dim(\pi_v) = \infty$).

1.2.4. Proposition (choice of an order). *There exists an* O_F*-order* $R \subset B$ *such that* $\forall v \notin \Sigma\cup\Sigma_\infty \quad \ell_v((\pi'_v)^{R_v^*}) \neq 0$*;* $\forall v \in \Sigma \quad R_v$ *is an Eichler order of level* $o(\pi'_v) = o(\pi_v)$ *(hence* $\dim(\pi'_v)^{R_v^*} = 1$*).*

Proof. Fix any O_F-order $R_0 \subset B$. There exists a finite set $S_0 \supset \Sigma_\infty$ of primes of F such that, for each $v \notin S_0$, the following conditions hold: $R_{0,v}$ is a maximal $O_{F,v}$-order in $B_v \xrightarrow{\sim} M_2(F_v)$, $t_v^{-1}(R_{0,v}) = O_{K,v}$, χ_v is unramified and $o(\pi'_v) = o(\pi_v) = 0$ ($\iff$ π_v is an unramified principal series representation). This implies, by [G-P, 2.3], that $\ell_v((\pi'_v)^{R_v^*}) \neq 0$ for all $v \notin S_0$. On the other hand, for each $v \in S_0 - (\Sigma \cup \Sigma_\infty)$, there exists a vector $x_v \in \pi'_v$ such that $\ell_v(x_v) \neq 0$. As the central character of π'_v is trivial, there exists an $O_{F,v}$-order $R(v) \subset B_v$ such that $x_v \in (\pi'_v)^{R(v)^*}$. For $v \in \Sigma$, let $R(v) \subset B_v$ be any Eichler order of level $o(\pi_v)$. The O_F-order $R \subset B$ given by its localisations

$$R_v = \begin{cases} R_{0,v}, & v \notin S_0 \\ R(v), & v \in S_0 - \Sigma_\infty \end{cases}$$

has the required properties.

1.2.5. Shimura curve. Fix an O_F-order $R \subset B$ satisfying Proposition 1.2.4 and put $H = \widehat{R}^*$. From now on, we shall work with the Shimura curve N_H^* (in the notation of [N 2, 1.4] and [A-N, 2.1.2]). By construction,

$$\pi'^H = \pi'_\infty \otimes {\bigotimes_{v\nmid\infty}}' (\pi'_v)^{R_v^*} \neq 0.$$

1.3. CM points

1.3.1. As in [A-N, 2.2], fix an isomorphism $B_{\tau_1} \xrightarrow{\sim} M_2(\mathbf{R})$ and denote by $z \in \mathbf{C}$, $\mathrm{Im}(z) > 0$ the unique point fixed by $t(K^*) \subset B^* \subset B^*_{\tau_1} \xrightarrow{\sim} GL_2(\mathbf{R})$. Let

$$\mathcal{C} = \{[z, b_1 \cdots b_s]_H \mid b_i \in B^*_{P_i}\} \subset CM(N_H, K)$$

be the $(P_1 \cdots P_s)$-isogeny class of the CM point $[z, 1]_H$ on the curve N_H^*.

Recall that the conductor of a CM point $x = [z, b]_H \in CM(N_H, K)$ is the non-zero ideal $c(x) \subset O_F$ satisfying

$$\forall v \notin \Sigma_\infty \qquad t_v^{-1}(b_v R_v b_v^{-1}) = O_{F,v} + c(x)O_{K,v}.$$

Similarly, the conductor of χ is the smallest non-zero ideal $c(\chi) \subset O_F$ (w.r.t. divisibility) such that

$$\forall v \notin \Sigma_\infty \qquad \chi_v((O_{F,v} + c(\chi)O_{K,v})^*) = 1.$$

1.3.2. Lemma. $\forall v \notin \Sigma \cup \Sigma_\infty \; \forall x \in \mathcal{C} \;\; \mathrm{ord}_v(c(\chi)) \leq \mathrm{ord}_v(c(x))$ *(the R.H.S. depends only on* $\mathcal{C}$*, by [A-N, (2.2.4.1)]).*

Proof. There exists $x_v \in (\pi'_v)^{R_v^*}$ such that $\ell_v(x_v) \neq 0$. As

$$\forall a \in K_v^* \qquad \ell_v(\pi'_v(t_v(a))\, x_v) = \chi_v^{-1}(a)\, \ell_v(x_v),$$

it follows that $\chi_v(t_v^{-1}(R_v^*)) = 1$; but $t_v^{-1}(R_v) = O_{F,v} + c(x) O_{K,v}$, by definition.

1.3.3. Corollary-Definition. *Put $c_0 = c(\chi)/(c(\chi), (P_1 \cdots P_s)^\infty)$ and $c = c(x)/(c(x), (P_1 \cdots P_s)^\infty)$ (which is independent of the choice of $x \in \mathcal{C}$). Then $c_0 \mid c$ and $c(\chi) = c_0 P_1^{n_1} \cdots P_s^{n_s}$ ($n_i \in \mathbf{N}$). As $c_0 \mid c$, χ is a character of $G^{(c)} = \mathrm{Gal}(K[cP^\infty]/K)$, in the notation of [A-N, 1.2.2]; let $\chi_0 : G_0^{(c)} \longrightarrow \mathbf{C}^*$ be the restriction of χ to the torsion subgroup $G_0^{(c)} = (G^{(c)})_{\mathrm{tors}}$ of $G^{(c)}$.*

1.3.4. Lemma. *For each $m \in \mathbf{N}$ there exists a CM point $x_m \in \mathcal{C}$ which is good in the sense of [A-N, 4.2.3] and satisfies $(P_1 \cdots P_s)^m \mid c(x_m)$.*

Proof. Let

$$X : \prod_{i=1}^{s} \mathcal{P}_{a_i}(\mathcal{T}_i) \twoheadrightarrow \mathcal{C}$$

be the $\prod_{i=1}^s K_{P_i}^*$-equivariant surjection from [A-N, (4.2.2.3)]. For each $i = 1, \ldots, s$ choose a path $\gamma_i = (y_0 \to \cdots \to y_{a_i}) \in \mathcal{P}_{a_i}(\mathcal{T}_i)$ such that $\mathscr{L}_i(y_0) = m$ and $\mathscr{L}_i(y_{a_i}) = m + a_i$; the CM point $x_m = X(\gamma_1, \ldots, \gamma_s)$ has the required properties.

1.4. Quotient of the Jacobian of the Shimura curve

1.4.1. As in [N 2, 1.16], denote by $J(N_H^*)$ the Jacobian of the curve N_H^*. As recalled in [A-N, 2.1.7] and [N 2, 1.18], there exists an isogeny $J(N_H^*) \longrightarrow A_0^a \times A_1$ (defined over F), where: A_0 is an F-simple abelian variety with $\mathrm{End}_F(A_0) = O_{L_0}$, L_0 is a totally real number field of degree $[L_0 : \mathbf{Q}] = \dim(A_0)$, there is a unique embedding $\sigma_0 : L_0 \hookrightarrow \mathbf{R}$ such that the L-function $L(\sigma_0\, A_0/F, s) = L(\sigma_0\, h^1(A_0), s)$ (in the notation of [N 3, 0.0]) is equal (Euler factor by Euler factor) to $L(\pi', s - 1/2) = L(\pi, s - 1/2)$, $a = \dim \bigotimes'_{v\nmid\infty} (\pi'_v)^{R_v^*} \geq 1$ and $\mathrm{Hom}_F(A_0, A_1) = 0$ (in the notation of [A-N, 2.1.7], $\pi' = \pi(\sigma_0)$). As $\sigma_0(L_0)$ is the field generated over $\mathbf{Q}$ by the Hecke eigenvalues of g, there is a unique embedding $i : L_0 \hookrightarrow L$ satisfying $i_\infty|_L \circ i = \sigma_0$.

For $j = 1, \ldots, a$, denote by $\mathrm{pr}_j : A_0^a \longrightarrow A_0$ the projection on the j-th factor.

1.4.2. Put $S = \{v \mid c d_{K/F}, v \neq P_1, \ldots, P_s\}$. According to Proposition 1.2.4,

$$\text{(1.4.2.1)} \qquad \forall v \in S \qquad \ell_v((\pi'_v)^{R_v^*}) \neq 0.$$

Denote by

$$\ell_S = \bigotimes_{v\in S} \ell_v : \bigotimes_{v\in S} \pi'_v \longrightarrow \mathbf{C}(\chi_S^{-1})$$

the tensor product of the linear forms ℓ_v ($v \in S$); above, $\chi_S = \prod_{v\in S} \chi_v : \prod_{v\in S} K_v^* \longrightarrow \mathbf{C}^*$.

1.4.3. As in [A-N, 2.4.3], put $A = O_L \otimes_{O_{L_0}} A_0$. As explained in [A-N, 2.1.7], $\Gamma(A, \Omega^1_{A/F})$ is a free $L \otimes_{\mathbf{Q}} F$-module of rank one and the projection $J(N_H^*) \longrightarrow A_0^a \times A_1 \longrightarrow A_0^a$ induces an isomorphism

$$\Gamma(A, \Omega^1_{A/F})^a \otimes_{F,\tau_1} \mathbf{C} \overset{\sim}{\longrightarrow} \bigoplus_{\sigma: L\hookrightarrow \mathbf{C}} \bigotimes{}'_{v\nmid\infty} ({}^\sigma\pi'_v)^{R_v^*}.$$

In particular, there is a natural $\widehat{B}^*$-equivariant projection on the term corresponding to $\sigma = i_\infty|_L$:

$$r : \Gamma(A, \Omega^1_{A/F})^a \otimes_{F,\tau_1} \mathbf{C} \twoheadrightarrow \bigotimes{}'_{v\nmid\infty} (\pi'_v)^{R_v^*}.$$

The linear form ℓ_S induces a linear map

$$\ell_S \otimes \mathrm{id} : \bigotimes{}'_{v\nmid\infty} \pi'_v \longrightarrow \Big(\bigotimes{}'_{v\notin \Sigma_\infty \cup S} \pi'_v\Big) \otimes \chi_S^{-1}$$

and it follows from (1.4.2.1) that there exists $j \in \{1, \ldots, a\}$ such that

$$(1.4.3.1) \qquad (\ell_S \otimes \mathrm{id}) \circ r \circ \mathrm{pr}_j^* \left(\Gamma(A, \Omega^1_{A/F}) \otimes_{F,\tau_1} \mathbf{C}\right) \neq 0.$$

In the notation of [A-N, 2.1.3], let $\alpha : N_H^* \longrightarrow A_0$ be the morphism (defined over F) given by

$$\alpha : N_H^* \xrightarrow{\iota_H} J(N_H^*) \longrightarrow A_0^a \times A_1 \longrightarrow A_0^a \xrightarrow{\mathrm{pr}_j} A_0.$$

1.5. End of the proof

1.5.1. Using Lemma 1.3.4, choose a sequence of good CM points $\{x_m\} \subseteq \mathcal{C}$ satisfying $(P_1 \cdots P_s)^m \mid c(x_m)$ for all $m \in \mathbf{N}$. By (1.4.3.1), the main non-vanishing result from [A-N] (Theorem 4.3.1) applies to the sequence of points $\{\alpha(x_m)\} \subset A_0(K[cP^\infty])$ and the character χ_0: if $m \in \mathbf{N}$ is large enough, then there exists a character $\chi_m : G^{(c)} \longrightarrow \overline{\mathbf{Q}}^*$ of finite order with the following properties:

1.5.1.1. the restriction of χ_m to $G_0^{(c)}$ is equal to χ_0;
1.5.1.2. $c(\chi_m)c_0^{-1} = c(x_m)c^{-1}$ (hence $(P_1 \cdots P_s)^m \mid c(\chi_m)$);
1.5.1.3. $e_{\overline{\chi}_m}(1 \otimes \alpha(x_m)) \neq 0 \in \overline{\mathbf{Q}} \otimes_{O_{L_0}} A_0(K[cP^\infty])$.

The assumptions in Theorem 0.4 imply that g does not have complex multiplication by any totally imaginary quadratic extension of F contained in K_{χ_m}, which means that the main result of [N 2] (Thm 3.2) applies to the non-torsion point $e_{\overline{\chi}_m}(1 \otimes \alpha(x_m))$, yielding

$$(1.5.1.4) \qquad h_f^1(K, V \otimes \chi_m^{\pm 1}) = 1.$$

As m is large enough, we also have

$$(1.5.1.5) \qquad \varepsilon(\pi \times \chi_m, \tfrac{1}{2}) = -1,$$

by [A-N, 2.4.12(3)], hence

$$r_{\mathrm{an}}(K, g, \chi_m) \equiv 1 \equiv h_f^1(K, V \otimes \chi_m) \pmod 2.$$

Finally, as the restrictions of χ and χ_m to the torsion subgroup of $G^{(c)}$ coincide, we have

$$r_{\mathrm{an}}(K, g, \chi) - h_f^1(K, V \otimes \chi) \equiv r_{\mathrm{an}}(K, g, \chi_m) - h_f^1(K, V \otimes \chi_m) \equiv 0 \pmod 2,$$

by Proposition 2.1.2(5) below (which was earlier proved in [N 1, 12.6.4.7(v)] in the special case when $(c, (p)) = (1)$). This finishes the proof of Theorem 0.4.

1.5.2. In fact, it is enough to appeal to a weaker non-vanishing result [A-N, Thm. 2.5.1], which does not require the CM points x_m to be good and which yields, for m large enough, a character $\chi_m : G^{(c)} \longrightarrow \overline{\mathbf{Q}}^*$ satisfying 1.5.1.1 and 1.5.1.3, but not necessarily 1.5.1.2. The equality (1.5.1.5) in this case follows from [A-N, Prop. 2.6.2(2)].

2. Iwasawa theory

Throughout this section we assume that $g \in S_k(\mathfrak{n}(g), 1)$ is a potentially p-ordinary Hilbert modular newform of level $\mathfrak{n}(g)$; let $\pi = \pi(g)$. We also fix K as in 0.1 and put $\eta = \eta_{K/F}$. Fix a non-empty subset $\Sigma = \{P_1, \ldots, P_s\} \subseteq \Sigma_p$ and an ideal $c \subset O_F$ relatively prime to $P_1 \cdots P_s$. As in [A-N, 1.2.2], set $K[cP^\infty] = \bigcup_{m \geq 1} K[cP_1^m \cdots P_s^m]$, $G^{(c)} = \mathrm{Gal}(K[cP^\infty]/K)$ and $G_0^{(c)} = \left(G^{(c)}\right)_{\mathrm{tors}}$.

2.1. ε-factors

2.1.1. For a character $\chi : G^{(c)} \longrightarrow \mathbf{C}^*$ of finite order, let

$$\varepsilon_v = \varepsilon(\pi_v \times \chi_v, \tfrac{1}{2}) \in \{\pm 1\}, \qquad \widetilde{\varepsilon}_v = \widetilde{\varepsilon}(\pi_v \times \chi_v, \tfrac{1}{2}) \in \{\pm 1\},$$

where

$$\widetilde{\varepsilon}_v = \varepsilon_v \times \begin{cases} -1, & v \in \Sigma_\chi(g) \\ 1, & v \notin \Sigma_\chi(g) \end{cases}$$

is the modified local ε-factor defined in [N 1, 12.6.3.10] (if $k > 2$, then $\Sigma_\chi(g) = \emptyset$ and $\widetilde{\varepsilon}_v = \varepsilon_v$ for all v). If $\chi' : G^{(c)} \longrightarrow \mathbf{C}^*$ is another character of finite order, denote the corresponding local ε-factors by ε'_v and $\widetilde{\varepsilon}'_v$.

2.1.2. Proposition. *Let $\chi, \chi' : G^{(c)} \longrightarrow \mathbf{C}^*$ be characters of finite order such that $\chi|_{G_0^{(c)}} = \chi'|_{G_0^{(c)}}$. If v is a prime of F, then:*
(1) *If $v \mid \infty$ or if $v \nmid \infty$ splits in K/F, then $\varepsilon_v = \varepsilon'_v = \widetilde{\varepsilon}_v = \widetilde{\varepsilon}'_v = 1$.*
(2) *If $v = P_i$ $(i = 1, \ldots, s)$, then $\widetilde{\varepsilon}_v = \widetilde{\varepsilon}'_v = \eta_v(-1)$.*
(3) *If $v \mid cd_{K/F}$, $v \neq P_1, \ldots, P_s$, then $\varepsilon_v = \varepsilon'_v$ and $\widetilde{\varepsilon}_v = \widetilde{\varepsilon}'_v$.*
(4) *If $v \nmid \infty cd_{K/F}$, then $\varepsilon_v = \varepsilon'_v$ (more precisely, $\chi_v = \chi'_v = 1$ if v does not split in K/F) and*

$$\widetilde{\varepsilon}_v = \widetilde{\varepsilon}'_v = \begin{cases} 1, & \text{if } \pi_v \text{ is not supercuspidal} \\ \eta_v(v)^{o(\pi_v)}, & \text{if } \pi_v \text{ is supercuspidal.} \end{cases}$$

(5) $r_{\rm an}(K, g, \chi) - h^1_f(K, V \otimes \chi) \equiv r_{\rm an}(K, g, \chi') - h^1_f(K, V \otimes \chi') \pmod 2$.

Proof. (1) [N 1, 12.6.2.2.1, 12.6.2.4]. (2) As $v \mid p$ and g is potentially p-ordinary, π_v is not supercuspidal; apply [N 1, 12.6.2.4(i),(ii)]. (3) Let $S = \{v \mid cd_{K/F}, v \neq P_1, \ldots, P_s\}$. By [A-N, 1.2.7], $G_0^{(c)}$ has a subgroup $G_1^{(c)} \xrightarrow{\sim} U'(c, P_1 \cdots P_s) = \prod_{v \in S} U'_v$, where each U'_v is isomorphic to a quotient of $(K_v^*)^\circ / F_v^*$, via the reciprocity map ${\rm rec}_K$. If $v \in S$ does not split in K/F, then $(K_v^*)^\circ = K_v^*$, which means that χ_v depends only on $\chi|_{G_1^{(c)}}$; thus $\chi_v = \chi'_v$, which implies that $\varepsilon_v = \varepsilon'_v$ and $\widetilde{\varepsilon}_v = \widetilde{\varepsilon}'_v$. If $v \in S$ splits in K/F, we conclude by (1).
(4) If π_v is not supercuspidal, then $\widetilde{\varepsilon}_v = \widetilde{\varepsilon}'_v = \eta_v(-1) = 1$ (recall that v is unramified in K/F, by assumption), by [N 1, 12.6.2.4(i),(ii)]. If π_v is supercuspidal, then $\varepsilon_v = \widetilde{\varepsilon}_v = \varepsilon'_v = \widetilde{\varepsilon}'_v = \eta_v(v)^{o(\pi_v)}$, by [N 1, 12.6.2.4(iii)]. If v is inert in K/F, then $\chi_v = \chi'_v = 1$, as both χ_v and χ'_v are unramified and $K_v^* = O_{K,v}^* F_v^*$. If v splits in K/F, then $\varepsilon_v = \varepsilon'_v$, by (1).
(5) As $\widetilde{\varepsilon} := \prod_v \widetilde{\varepsilon}_v$ is equal to $\widetilde{\varepsilon}' := \prod_v \widetilde{\varepsilon}'_v$, by (1)–(4), we deduce from [N 1, 12.6.4.3] that

$$\widetilde{h}^1_f(K, V \otimes \chi) - h^1_f(K, V \otimes \chi) + r_{\rm an}(K, g, \chi) \equiv \widetilde{h}^1_f(K, V \otimes \chi') - h^1_f(K, V \otimes \chi') + r_{\rm an}(K, g, \chi') \pmod 2,$$

where $\widetilde{h}^1_f(K, V \otimes \chi)$ denotes the dimension of the "extended Selmer group" $\widetilde{H}^1_f(K, V \otimes \chi)$ defined in [N 1, 12.5.9.2]. On the other hand, [N 1, Thm. 10.7.17] implies that

$$\widetilde{h}^1_f(K, V \otimes \chi) \equiv \widetilde{h}^1_f(K, V \otimes \chi') \pmod 2,$$

as explained in the proof of [N 1, 12.6.4.7(v)]. Combining the two congruences, we obtain the desired result.

2.1.3. Proposition-Definition. (1) $\varepsilon_{\rm lim}(\pi \times \chi_0, \frac{1}{2}) := \varepsilon(\pi \times \chi, \frac{1}{2}) \prod_{i=1}^s \eta_{P_i}(-1)\, \varepsilon_{P_i} \in \{\pm 1\}$ *depends only on π and $\chi_0 = \chi|_{G_0^{(c)}}$.*
(2) *If $k > 2$, then $\varepsilon_{\rm lim}(\pi \times \chi_0, \frac{1}{2}) = \varepsilon(\pi \times \chi, \frac{1}{2})$ for any χ satisfying $\chi|_{G_0^{(c)}} = \chi_0$.*
(3) *If $n \in \mathbf{N}$ is large enough and $(P_1 \cdots P_s)^n \mid c(\chi)$, then $\varepsilon(\pi \times \chi, \frac{1}{2}) = \varepsilon_{\rm lim}(\pi \times \chi_0, \frac{1}{2})$.*

Proof. (1) By Proposition 2.1.2, the individual terms in

$$\varepsilon(\pi\times\chi,\tfrac{1}{2})\prod_{i=1}^{s}\eta_{P_i}(-1)\,\varepsilon_{P_i}=\prod_{v\nmid P_1\cdots P_s}\eta_v(-1)\,\varepsilon_v$$

are the same for χ and χ'.
(2) If $k>2$, then each π_{P_i} is a principal series representation [N 2, 12.5.4], hence $\eta_{P_i}(-1)\,\varepsilon_{P_i}=1$ ([N 2, 12.6.2.4(i)]).
(3) If n is large enough, then each term $\eta_{P_i}(-1)\,\varepsilon_{P_i}$ is equal to 1, by [J-L, Prop. 3.8] and [J, Thm. 20.6].

2.2. Ranks

2.2.1. Fix a character $\chi_0 : G_0^{(c)} \longrightarrow O_L^*$, where L is a number field such that $i_\infty(L)$ contains all Hecke eigenvalues of g. Let $\mathfrak{p}\mid p$ be as in 0.1; put $O=O_{L,\mathfrak{p}}$, and $\Lambda=O[[G^{(c)}]]$. For any $O[G_0^{(c)}]$-module M, define

$$M_{(\chi_0)} := M\otimes_{O[G_0^{(c)}],\chi_0} O;$$

then

$$\Lambda_{(\chi_0)} \xrightarrow{\sim} O[[G^{(c)}/G_0^{(c)}]] \xrightarrow{\sim} O[[X_1,\ldots,X_r]],\qquad r=\sum_{i=1}^{s}[F_{P_i}:\mathbf{Q}_p].$$

2.2.2. We say that a prime v of F is **exceptional** if $v\mid p$, $v\nmid P_1\cdots P_s$ and $\pi_v=\mathrm{St}\otimes\mu$ ($\mu^2=1$). Denote by $\mathcal{M}(g,K;c,P_1,\ldots,P_s;\chi_0)$ the set of all exceptional primes of F that do not split in K/F and satisfy

$$\begin{cases}(\chi_0)_w=\mu\circ N_{K_w/F_v}, & \text{if } v\mid cd_{K/F}\\ \mathrm{ord}_v(\mathfrak{n}(g))=1, & \text{if } v\nmid cd_{K/F}\end{cases}$$

(where w is the unique prime of K above v). If $k>2$, then there are no exceptional primes.

2.2.3. Let $\chi : G^{(c)}\longrightarrow O'^*$ be a character of finite order, where O' is the ring of integers in a finite extension of $L_\mathfrak{p}$. The extended Selmer group of $V\otimes\chi$ ([N 1, 12.5.9.2]) sits in an exact sequence

$$0\longrightarrow\bigoplus_{w\mid v\mid p}H^0(K_w,V_v^-\otimes\chi_w)\longrightarrow\widetilde{H}^1_f(K,V\otimes\chi)\longrightarrow H^1_f(K,V\otimes\chi)\longrightarrow 0,$$

where v (resp., w) is a prime of F (resp., of K) and

$$0\longrightarrow V_v^+\longrightarrow V\longrightarrow V_v^-\longrightarrow 0$$

is an exact sequence of $L_\mathfrak{p}[\mathrm{Gal}(\overline{F}_v/F_v)]$-modules arising from the potential p-ordinarity of g. Denote by h^0, $\widetilde{h}^1_f$ and h^1_f the dimensions of the respective cohomology groups over the fraction field of O'; then

$$\widetilde{h}^1_f(K,V\otimes\chi)-h^1_f(K,V\otimes\chi)=\sum_{w\mid v\mid p}h^0(K_w,V_v^-\otimes\chi_w),\tag{2.2.3.1}$$

where

$$h^0(K_w,V_v^-\otimes\chi_w)=\begin{cases}1, & \pi_v=\mathrm{St}\otimes\mu\ (\mu^2=1),\ \chi_w=\mu\circ N_{K_w/F_v}\\ 0, & \text{otherwise}\end{cases}$$

([N 1, 12.5.8]). In particular, $h^0(K_w,V_v^-\otimes\chi_w)=0$ and $\widetilde{h}^1_f(K,V\otimes\chi)=h^1_f(K,V\otimes\chi)$ if $k>2$.

2.2.4. Proposition. *Asume that $k = 2$. Let $\chi : G^{(c)} \longrightarrow O'^*$ be a character of finite order satisfying $\chi|_{G_0^{(c)}} = \chi_0$ and such that $(P_1 \cdots P_s)^n \mid c(\chi)$, for large enough $n \in \mathbf{N}$. Then:*

(1) $\widetilde{h}^1_f(K, V \otimes \chi) - h^1_f(K, V \otimes \chi) \equiv |\mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0)| \pmod 2$.

(2) *If there exists an exceptional prime of F that splits in K/F, assume, in addition, that there is $i \in \{1, \ldots, s\}$ such that $F_{P_i} = \mathbf{Q}_p$. Then*

$$\widetilde{h}^1_f(K, V \otimes \chi) - h^1_f(K, V \otimes \chi) = |\mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0)|.$$

Proof. If w is a prime of K dividing $P_1 \cdots P_s$, then $\chi_w^2 \neq 1$ if n is large enough, which means that w does not contribute to the R.H.S. of (2.2.3.1).

Let v be an exceptional prime of F. If v does not split in K/F and $v \mid cd_{K/F}$, then $\chi_w = (\chi_0)_w$ (note that the decomposition group of v in $G^{(c)}$ is finite, as v does not split in K/F) and

$$h^0(K_w, V_v^- \otimes \chi_w) = h^0(K_w, V_v^- \otimes (\chi_0)_w) = \begin{cases} 1, & v \in \mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0) \\ 0, & v \notin \mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0). \end{cases}$$

If v does not split in K/F and $v \nmid cd_{K/F}$, then v is inert in K/F ($vO_K = w$) and χ_w is unramified; thus $\chi_w = 1$ and (using [N 1, (12.3.9.1)])

$$h^0(K_w, V_v^- \otimes \chi_w) = \begin{cases} 1, & \mu \text{ is unramified} \iff \mathrm{ord}_v(\mathfrak{n}(g)) = 1 \\ 0, & \text{otherwise} \end{cases} = \begin{cases} 1, & v \in \mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0) \\ 0, & v \notin \mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0). \end{cases}$$

If v splits in K/F ($vO_K = ww'$), then the h^0-terms in (2.2.3.1) for w and w' are the same; this proves (1). Under the assumptions of (2), there is i such that $\mathrm{Gal}(K[P_i^\infty]/K)$ is isomorphic to a product of $\mathbf{Z}_p$ by a finite abelian group. As the decomposition groups of w and w' in $\mathrm{Gal}(K[P_i^\infty]/K)$ are infinite, it follows that $\chi_w^2, \chi_{w'}^2 \neq 1$ if n is large enough; thus w and w' do not contribute to the R.H.S. of (2.2.3.1).

2.2.5. Proposition. *Fix a G_F-stable O-lattice $T \subset V$. Let $w|v|p$ be as in 2.2.3. Define*

$$Z_w = \varinjlim_{\alpha} \bigoplus_{w_\alpha | w} H^0((K_\alpha)_{w_\alpha}, (V/T)_v^-),$$

where and K_α/K runs through all finite subextensions of $K[cP_1^\infty \cdots P_s^\infty]/K$ and $(V/T)_v^-$ is the image of V_v^- in V/T. Then

$$\mathrm{cork}_{\Lambda_{(\chi_0)}} \bigoplus_{w|v} (Z_w)_{(\chi_0)} = \begin{cases} 1, & v \in \mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0) \\ 0, & v \notin \mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0). \end{cases}$$

Proof. If the decomposition group of w in $K[cP_1^\infty \cdots P_s^\infty]/K$ is infinite, then the L.H.S. is equal to zero ([N 1, 12.6.4.10]). We can assume, therefore, that v is exceptional and does not split in K/F. Choose an isomorphism $G^{(c)} \xrightarrow{\sim} G_0^{(c)} \times \left(G^{(c)}/G_0^{(c)}\right)$; then χ_0 becomes a character of $G^{(c)}$ and $D\left((Z_w)_{(\chi_0)}\right) = D\left(H^0(K_w, (V/T)_v^- \otimes (\chi_0^{-1})_w)\right) \otimes_O \Lambda_{(\chi_0)}$, where $D(-)$ denotes the Pontrjagin dual (cf. [N 1, 9.6.5]); thus

$$\mathrm{cork}_{\Lambda_{(\chi_0)}} (Z_w)_{(\chi_0)} = h^0(K_w, V_v^- \otimes (\chi_0^{-1})_w) = \begin{cases} 1, & v \in \mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0) \\ 0, & v \notin \mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0), \end{cases}$$

by the proof of Proposition 2.2.4.

2.2.6. Fix a finite set S of primes of F containing $\Sigma_p \cup \Sigma_\infty$ and all primes dividing $\mathfrak{n}(g)$, and a subset $\Sigma' \subseteq S - (\Sigma_p \cup \Sigma_\infty)$. As in [N 1, 12.5.9.1], consider the corresponding Greenberg's local conditions for T and V/T. In order to simplify the notation, put $K_\infty = K[cP_1^\infty \cdots P_s^\infty]$.

2.2.7. Proposition. (1) *The (co)-ranks*

$$\forall j = 1,2 \qquad \mathrm{rk}_{\Lambda_{(\chi_0)}}\, \widetilde{H}^j_{f,\mathrm{Iw}}(K_\infty/K, T)_{(\chi_0^{\pm 1})} = \mathrm{cork}_{\Lambda_{(\chi_0)}}\, \widetilde{H}^j_f(K_S/K_\infty, V/T)_{(\chi_0^{\pm 1})} = r(g)$$

(where $\widetilde{H}^j_{f,\mathrm{Iw}}(K_\infty/K,T)$ is the Λ-module defined in [N 1, 8.8.5]) are equal to the same integer $r(g)$ and do not depend on S and Σ'.
(2) *Assume that* $\varepsilon_{\lim}(\pi \times \chi_0, \frac{1}{2}) = -1$. *If g has CM by a totally imaginary quadratic extension K' of F, assume that $p \neq 2$ and $K' \not\subset K_\infty^{\mathrm{Ker}(\chi_0)}$. Then* $r(g) \equiv 1 + |\mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0)| \pmod 2$.

Proof. (1) See the proof of [N 1, 12.6.4.12].
(2) Let $\chi : G^{(c)} \longrightarrow O'^*$ be a character of finite order such that $\chi|_{G_0^{(c)}} = \chi_0$ and $(P_1 \cdots P_s)^n \mid c(\chi)$, for large enough $n \in \mathbf{N}$. We have

$$\begin{aligned} r(g) &\equiv \widetilde{h}^1_f(K, V\otimes\chi) \pmod 2 && \text{[N1, 10.7.17]} \\ &\equiv h^1_f(K, V\otimes\chi) + |\mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0)| \pmod 2 && \text{Proposition 2.2.4(1)} \\ &\equiv 1 + |\mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0)| \pmod 2 && \text{Theorem 0.4(1)} \end{aligned}$$

(Theorem 0.4(1) applies, as $\varepsilon(\pi \times \chi, \frac{1}{2}) = \varepsilon_{\lim}(\pi\times\chi_0, \frac{1}{2}) = -1$, by Proposition-Definition 2.1.3(3)).

2.2.8. Proposition. *Assume that $k = 2$ and* $\varepsilon_{\lim}(\pi \times \chi_0, \frac{1}{2}) = -1$. *If g has CM by a totally imaginary quadratic extension K' of F, assume that $p \neq 2$ and $K' \not\subset K_\infty^{\mathrm{Ker}(\chi_0)}$. If there exists an exceptional prime of F that splits in K/F, assume, in addition, that there is $i \in \{P_1, \ldots, P_s\}$ such that $F_{P_i} = \mathbf{Q}_p$. Then:*
(1) *The (co)-ranks in Proposition 2.2.7(1) are equal to* $r(g) = 1 + |\mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0)|$.
(2) $\mathrm{cork}_{\Lambda_{(\chi_0)}}\, S^{\mathrm{str}}_{V/T}(K_\infty)_{(\chi_0^{\pm1})} = 1$, *where $S^{\mathrm{str}}_{V/T}(K_\infty) \subset H^1(K_\infty, V/T)$ is Greenberg's strict Selmer group [N 1, 9.6.5].*
(3) *If $K \subset K'_\infty \subset K_\infty$ is an intermediate field such that χ_0 factors through $\chi'_0 : \mathrm{Gal}(K'_\infty/K)_{\mathrm{tors}} \longrightarrow O_L^*$, then the (co)-ranks*

$$\forall j = 1,2 \qquad \mathrm{rk}_{\Lambda'_{(\chi'_0)}}\, \widetilde{H}^j_{f,\mathrm{Iw}}(K'_\infty/K, T)_{(\chi_0'^{\pm 1})} = \mathrm{cork}_{\Lambda'_{(\chi'_0)}}\, \widetilde{H}^j_f(K_S/K'_\infty, V/T)_{(\chi_0'^{\pm 1})} = r'(g)$$

(where $\Lambda' = O[[\mathrm{Gal}(K'_\infty/K)]]$) are all equal, do not depend on S and Σ', and satisfy

$$r'(g) \geq r(g), \qquad r'(g) \equiv r(g) \pmod 2.$$

Proof (cf. [N 1, 12.6.4.12, 12.9.8]). (1),(2) Denote the coranks in (2) by $s_\pm(g)$. The exact sequence

$$H^0(K_\infty, V/T)_{(\chi_0^{\pm1})} \longrightarrow \bigoplus_{w|v|p} (Z_w)_{(\chi_0^{\pm1})} \longrightarrow \widetilde{H}^1_f(K_S/K_\infty, V/T)_{(\chi_0^{\pm1})} \longrightarrow S^{\mathrm{str}}_{V/T}(K_\infty)_{(\chi_0^{\pm1})} \longrightarrow 0$$

([N 1, (9.6.5.1)]) combined with Proposition 2.2.5 and 2.2.7 implies that

$$r(g) = s_\pm(g) + |\mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0)|.$$

For $m \in \mathbf{N}$ large enough, let χ_m be as in 1.5.1; then

$$h^1(K, V\otimes\chi_m) = 1, \qquad \widetilde{h}^1(K, V\otimes\chi_m) = 1 + |\mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0)|,$$

by (1.5.1.4) and Proposition 2.2.4(2). Finally,

$$\widetilde{h}^1(K, V\otimes\chi_m) \geq r(g), \qquad \widetilde{h}^1(K, V\otimes\chi_m) \equiv r(g) \pmod 2$$

by [N 1, 10.7.17], which implies that

$$s_\pm(g) = 1, \qquad r(g) = 1 + |\mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0)|.$$

(3) This follows from [N 1, 8.10.11(ii)] and [N 1, 10.7.17(iii)].

2.2.9. Proposition. *Let R be the quotient of the ordinary Hecke algebra defined in [N 1, 12.7.7]* (Spec(R) *is the branch of the cyclotomic Hida family of parallel weight passing through the p-stabilisation f^0 of a p-ordinary twist of g). Let $\overline{R} = R[[G^{(c)}]]$ and $\overline{\mathfrak{q}} = \overline{R} \cdot \mathrm{Ker}(\chi_0 : O[G_0^{(c)}] \longrightarrow O)$ ($\overline{\mathfrak{q}}$ is a minimal prime of $\overline{R}$). Let $\mathcal{T}$ be the big Galois representation defined in [N 1, 12.7.15.3] (then $\mathcal{T}_{\mathcal{P}}/\mathcal{P}\mathcal{T}_{\mathcal{P}} \xrightarrow{\sim} V$, where $\mathcal{P}$ is the arithmetic point of R corresponding to f^0). Assume that $\varepsilon_{\lim}(\pi \times \chi_0, \frac{1}{2}) = -1$. If g has CM by a totally imaginary quadratic extension K' of F, assume that $p \neq 2$ and $K' \not\subset K_\infty^{\mathrm{Ker}(\chi_0)}$. Then:*
(1) *The ranks*

$$\forall j = 1, 2 \qquad \mathrm{rk}_{\overline{R}_{\overline{\mathfrak{q}}}} \widetilde{H}^j_{f,\mathrm{Iw}}(K_\infty/K, \mathcal{T})_{\overline{\mathfrak{q}}} = \mathrm{rk}_{\overline{R}_{\overline{\mathfrak{q}}}} \left(\widetilde{H}^j_{f,\mathrm{Iw}}(K_\infty/K, \mathcal{T})^\iota\right)_{\overline{\mathfrak{q}}} = 1.$$

(2) *For all but finitely many arithmetic points $\mathcal{P}'$ of R, $r(g_{\mathcal{P}'}) = 1$, where $g_{\mathcal{P}'} \in S_{k'}(\mathfrak{n}', 1)$ satisfies $V(g_{\mathcal{P}'})(k'/2) \xrightarrow{\sim} \mathcal{T}_{\mathcal{P}'}/\mathcal{P}'\mathcal{T}_{\mathcal{P}'}$.*

Proof (cf. [N 1, 12.9.8, 12.9.11]). The four ranks in (1) are equal, by [N 1, 12.7.15.7(i), 12.7.16.8(i)]; denote their common value by h. Let $g' = g_{\mathcal{P}'}$ be as in (2). According to [N 1, 12.7.15.8(iii)],

$$h \leq r(g'), \qquad h \equiv r(g') \pmod 2.$$

Choose $\mathcal{P}'$ such that $k' = 2$ and $\pi(g')_v$ is a principal series representation for all $v \mid p$ (cf. [N 1, 12.7.10]); then $\mathcal{M}(g, K; c, P_1, \ldots, P_s; \chi_0) = \emptyset$. Applying (a slight variant of) Proposition 2.2.8(1) to g', we obtain $r(g') = 1$, hence $h = 1$. The statement (2) follows from the fact that $h = r(g')$ for almost all $\mathcal{P}'$.

3. Proof of Theorem 0.8

3.1. Kummer theory

3.1.1. As in 0.7, let $q \neq 2$ be a prime number and F_0 a totally real number field such that $F_0 \cap \mathbf{Q}(\mu_{q^\infty}) = \mathbf{Q}$. Let $a \in O_{F_0} - \{0\}$ be an element satisfying $a \notin F_0^{*q}$ and, for each finite prime v_0 of F_0 not dividing q, $\mathrm{ord}_{v_0}(a) < q$. For $r \geq 1$, put $F_r = F_0\mathbf{Q}(\mu_{q^r})^+$, $K_r = F_0(\mu_{q^r})$.

3.1.2. Let $r \geq 1$. As $F_0 \cap \mathbf{Q}(\mu_{q^\infty}) = \mathbf{Q}$,

$$\mathrm{Gal}(K_r/F_0) \xrightarrow{\sim} \mathrm{Gal}(\mathbf{Q}(\mu_{q^r})/\mathbf{Q}) \xrightarrow{\sim} (\mathbf{Z}/q^r\mathbf{Z})^*.$$

The map

$$F_0^* \otimes \mathbf{Z}/q^r\mathbf{Z} = H^1(F_0, \mu_{q^r}) \xrightarrow{\mathrm{res}} H^1(K_r, \mu_{q^r}) = K_r^* \otimes \mathbf{Z}/q^r\mathbf{Z}$$

is injective, as

$$|\mathrm{Ker}(\mathrm{res})| = |H^1(K_r/F_0, \mu_{q^r})| = |\widehat{H}^0(K_r/F_0, \mu_{q^r})| \leq |H^0(F_0, \mu_{q^r})| = 1;$$

thus $a \notin K_r^{*q}$, which yields, by Kummer theory, an isomorphism

$$\mathrm{Gal}\left(K_r(\sqrt[q^r]{a})/K_r\right) \xrightarrow{\sim} \mu_{q^r}, \qquad g \mapsto g(\sqrt[q^r]{a})/\sqrt[q^r]{a}.$$

A choice of a compatible system of roots $\sqrt[q^r]{a} \in \overline{\mathbf{Q}}$ such that $(\sqrt[q^r]{a})^q = \sqrt[q^{r-1}]{a}$ determines a compatible system of isomorphisms

$$\mathrm{Gal}\left(K_r(\sqrt[q^r]{a})/F_0\right) \xrightarrow{\sim} \mu_{q^r} \rtimes (\mathbf{Z}/q^r\mathbf{Z})^*,$$

under which $\mathrm{Gal}\left(K_r(\sqrt[q^r]{a})/F_0(\sqrt[q^r]{a})\right)$ corresponds to $(\mathbf{Z}/q^r\mathbf{Z})^*$.

3.1.3. Proposition. *Let H be a finite group acting on a finite abelian group A; let $G = A \rtimes H$. Let L be a field of characteristic zero containing all roots of unity of order equal to the exponent of A. Then the $L[G]$-module $L[G/H]$ decomposes into simple $L[G]$-modules as follows:*

$$L[G/H] = \bigoplus_{[\chi : A \longrightarrow L^*]} \mathrm{Ind}_{A \rtimes H_\chi}^{A \rtimes H} (\chi \otimes 1),$$

where χ runs through a set of representatives of $H \backslash \mathrm{Hom}(A, L^*)$ and $H_\chi \subset H$ is the stabiliser of χ.

Proof. Easy exercise.

3.1.4. For a subfield $k \subset \overline{\mathbf{Q}}$, put $G_k = \mathrm{Gal}(\overline{\mathbf{Q}}/k)$. If k'/k is a finite subextension of $\overline{\mathbf{Q}}/k$, denote by

$$\mathrm{Res}_{k'/k} : (G_k - \mathrm{Mod}) \longrightarrow (G_{k'} - \mathrm{Mod}), \qquad \mathrm{Ind}_{k'/k} : (G_{k'} - \mathrm{Mod}) \longrightarrow (G_k - \mathrm{Mod})$$

the corresponding restriction and induction functors, respectively.

In the situation of 3.1.2, apply Proposition 3.1.3 to

$$A = \mathrm{Gal}\left(K_r(\sqrt[q^r]{a})/K_r\right) \xrightarrow{\sim} \mu_{q^r}, \qquad H = \mathrm{Gal}\left(K_r(\sqrt[q^r]{a})/F_0(\sqrt[q^r]{a})\right) \xrightarrow{\sim} (\mathbf{Z}/q^r\mathbf{Z})^*;$$

we obtain, for any field $L \supset \mathbf{Q}(\mu_{q^r})$,

$$\mathrm{Ind}_{F_0(\sqrt[q^r]{a})/F_0}(\mathbf{Z}) \otimes L = L[A \rtimes H/H] = \bigoplus_{s=0}^{r} \rho_s, \qquad \rho_s = \mathrm{Ind}_{K_s/F_0}(\chi_s), \tag{3.1.4.1}$$

where $\chi_s : \mathrm{Gal}\left(K_s(\sqrt[q^s]{a})/K_s\right) \hookrightarrow L^*$ is an injective character (of order q^s) and ρ_s is an absolutely irreducible representation of G of dimension $\varphi(q^s)$. If $s \geq 1$, denote by ρ the non-trivial element of $\mathrm{Gal}(K_s/F_s) \xrightarrow{\sim} \mathrm{Gal}\left(\mathbf{Q}(\mu_{q^s})/\mathbf{Q}(\mu_{q^s})^+\right)$; then ${}^\rho\chi_s = \chi_s^{-1}$. As the order of χ_s is odd, it follows that χ_s (more precisely, $\chi_s \circ \mathrm{rec}_{K_s}$) factors through $\mathbf{A}_{K_s}^*/K_s^*\mathbf{A}_{F_s}^*$.

If M is an $L[G_{F_0}]$-module, the projection formula

$$\mathrm{Ind}_{k'/k}\left(X \otimes_L \mathrm{Res}_{k'/k}(Y)\right) = \mathrm{Ind}_{k'/k}(X) \otimes_L Y$$

together with (3.1.4.1) imply that

$$\mathrm{Ind}_{F_0(\sqrt[q^r]{a})/F_0} \circ \mathrm{Res}_{F_0(\sqrt[q^r]{a})/F_0}(M) = \bigoplus_{s=0}^{r} \mathrm{Ind}_{K_s/F_0}\left(\mathrm{Res}_{K_s/F_0}(M) \otimes \chi_s\right). \tag{3.1.4.2}$$

3.2. ε-factors

3.2.1. In the situation of 3.1.1, let $g_0 \in S_k(\mathfrak{n}_0, 1)$ be a cuspidal Hilbert modular newform over F_0 of parallel weight k, trivial central character and level $\mathfrak{n}_0$; put $V = V_{\mathfrak{p}}(g_0)(k/2)$. For $r \geq 1$, denote by g_r the base change of g_0 over F_r (i.e., $\pi(g_r) = BC_{F_r/F}(\pi(g_0))$).

3.2.2. It follows from (3.1.4.2) and Shapiro's Lemma that

$$\forall r \geq 1 \qquad H^1_f(F_0(\sqrt[q^r]{a}), V) = H^1_f(F_0, V) \oplus \bigoplus_{s=1}^{r} H^1_f(K_s, V \otimes \chi_s) \tag{3.2.2.1}$$

(taking $L \supset \mathbf{Q}(\mu_{q^r})$ in 0.1), hence

$$\forall r \geq 1 \qquad h^1_f(F_0(\sqrt[q^r]{a}), V) - h^1_f(F_0(\sqrt[q^{r-1}]{a}), V) = h^1_f(K_r, V \otimes \chi_r). \tag{3.2.2.2}$$

3.2.3. Proposition. *Assume that* $(\forall v_0|a)$ $\pi(g_0)_{v_0}$ *is not supercuspidal and that* $(\forall v_0|q)$ $\pi(g_0)_{v_0}$ *is a principal series representation. Then:*

$$\forall r \geq 1 \qquad \varepsilon(\pi(g_r) \times \chi_r, \tfrac{1}{2}) = \left(\frac{d}{q}\right), \qquad d = (-1)^{[F_0:\mathbf{Q}]} N(\mathfrak{n}_0^{(aq)}),$$

where $\mathfrak{a}^{(\mathfrak{b})} = \mathfrak{a}/(\mathfrak{a}, \mathfrak{b}^\infty)$ *is the prime-to-*$\mathfrak{b}$ *part of* $\mathfrak{a}$*, for any non-zero ideals* $\mathfrak{a}, \mathfrak{b}$ *in the ring of integers of a given number field.*

Proof. Fix $r \geq 1$. Let v be a finite prime of F_r. Our assumptions imply that

$$\begin{aligned} & v \text{ ramifies in } K_r/F_r \iff v \mid q \\ & v \mid a, v \nmid q \Longrightarrow v \mid c(\chi_r) \Longrightarrow v \mid aq. \end{aligned} \tag{3.2.3.1}$$

It follows that the condition $H(K_r, \chi_r)$ from [N 1, 12.6.3.5] is satisfied. Applying [N 1, 12.6.3.9], we obtain

$$\varepsilon(\pi(g_r) \times \chi_r, \tfrac{1}{2}) = (-1)^{[F_r:\mathbf{Q}]} \, \eta_{K_r/F_r}(\mathfrak{n}(g_r)^{(q)}) \, (-1)^{|R(1)^0 \cap \{v \nmid c(\chi_r)\}|} \, (-1)^{|R(1)^- \cap \{v | c(\chi_r)\}|},$$

where $\mathfrak{n}(g_r) \subset O_{F_r}$ is the level of g_r and $R(1)^0$ (resp., $R(1)^-$) contains those elements of $\Sigma_1(g_r)$ which are ramified (resp., inert) in K_r/F_r (see [N 1, 12.6.3.2]). By (3.2.3.1), we have $R(1)^0 = \emptyset$ and

$$\begin{aligned} R(1)^- \cap \{v \mid c(\chi_r)\} &= \{v \mid a;\ v \text{ is inert in } K_r/F_r,\ \pi(g_r) = \mathrm{St} \otimes \mu,\ \mu : F_{r,v}^* \longrightarrow \{\pm 1\} \text{ is unramified}\} \\ &= \{v \mid a;\ v \text{ is inert in } K_r/F_r,\ \pi(g_r) = \mathrm{St} \otimes \mu,\ \mu : F_{r,v}^* \longrightarrow \{\pm 1\},\ o(\pi(g_r)_v) = 1\} \\ &= \{v \mid a;\ v \text{ is inert in } K_r/F_r,\ \pi(g_r) = \mathrm{St} \otimes \mu,\ \mu : F_{r,v}^* \longrightarrow \{\pm 1\},\ 2 \nmid o(\pi(g_r)_v)\} \end{aligned}$$

(as $\pi(g_r)_v$ is not supercuspidal), hence

$$\varepsilon(\pi(g_r) \times \chi_r, \tfrac{1}{2}) = (-1)^{[F_r:\mathbf{Q}]} \, \eta_{K_r/F_r}(\mathfrak{n}(g_r)^{(aq)}).$$

As F_r/F is unramified outside q, it follows that

$$\mathfrak{n}(g_r)^{(q)} = \mathfrak{n}_0^{(q)} O_{F_r}, \qquad \mathfrak{n}(g_r)^{(aq)} = \mathfrak{n}_0^{(aq)} O_{F_r}.$$

Let $F' = \mathbf{Q}(\mu_{q^r})^+$, $K' = \mathbf{Q}(\mu_{q^r})$. If $I_0 \subset O_{F_0}$ is an ideal prime to q, let $I_r = I_0 O_{F_r}$; then

$$\eta_{K_r/F_r}(I_r) = \eta_{K'/F'}(N_{F_r/F'}(I_r)) \equiv N(I_r) \pmod{q^r} \equiv N(I_0)^{\varphi(q^r)/2} \equiv N(I_0)^{(q-1)/2} \pmod{q},$$

hence

$$\eta_{K_r/F_r}(I_0 O_{F_r}) = \left(\frac{N(I_0)}{q}\right), \qquad (-1)^{[F_r:\mathbf{Q}]} \, \eta_{K_r/F_r}(I_0 O_{F_r}) = \left(\frac{(-1)^{[F_0:\mathbf{Q}]} N(I_0)}{q}\right).$$

Taking $I_0 = \mathfrak{n}_0^{(aq)}$, we obtain the desired result.

3.2.4. The proof of Proposition 3.2.3 shows that the formula for $\varepsilon(\pi(g_r) \times \chi_r, \frac{1}{2})$ still holds if we replace the assumption "$(\forall v_0|q)$ $\pi(g_0)_{v_0}$ is a principal series representation" by "$(\forall v_0|q)$ $\pi(g_0)_{v_0}$ is not supercuspidal, and the extension $K_r(\sqrt[q^r]{a})/K_r$ is ramified at all primes above q", as $R(1)^0 \cap \{v \nmid c(\chi_r)\} = \emptyset$ in this case.

3.3. End of the proof

3.3.1. The statement of Theorem 0.8(1) follows from Proposition 3.2.3.

3.3.2. By (3.2.2.2), the first line in the statement of Theorem 0.8(2) will follow from Theorem 0.4(1) applied to each g_s and χ_s $(1 \leq s \leq r)$. As g_0 is potentially p-ordinary, so is g_s. By 3.3.1, $2 \nmid r_{\mathrm{an}}(K_s, g_s, \chi_s)$, so it remains to check that if g_s has CM by a totally imaginary quadratic extension K' of F_s, then K' is not contained in $K_s(\sqrt[q^s]{a})$. If $K' \subset K_s(\sqrt[q^s]{a})$, then $K' = K_s$ and g_0 has CM by a totally imaginary quadratic extension K'_0 of F_0 such that $F_r K'_0 = K_s$. However, the only quadratic extension of F_0 contained in K_s is $F_0(\sqrt{q^*})$, where $q^* = (-1)^{(q-1)/2} q$; thus $q \equiv 3 \pmod 4$ and $K'_0 = F_0(\sqrt{-q})$, which contradicts the assumptions.

It remains to show is that, in the case when $2 \nmid [F_0 : \mathbf{Q}]$, g_0 cannot have CM by $K'_0 = F_0(\sqrt{-q})$, $q \equiv 3 \pmod 4$. If that were the case, then each finite prime v_0 of F_0 ramified in K'_0/F_0 would divide q, hence $\pi(g_0)_{v_0}$ would not be supercuspidal; thus $\pi(g_0)_{v_0} = \pi(\mu, \mu\eta'_{v_0})$, where $\eta' = \eta_{K'_0/F_0}$ ([N 1, 12.6.1.2.3]). As the central character of g_0 is trivial, $\eta'_{v_0} = \mu^{-2}$, hence $\eta'_{v_0}(-1) = 1$. This would imply that $1 = \prod_{w_0} \eta'_{w_0}(-1) = (-1)^{[F_0:\mathbf{Q}]}$, which contradicts our assumption.

3.3.3. Let us now prove the second line in the statement of Theorem 0.8(2). For each $s = 0, \ldots, r$, $\rho_s = \mathrm{Ind}_{K_s/F_0}(\chi_s)$ is an absolutely irreducible $L[G_{F_0}]$-module of dimension $\varphi(q^s)$. If $1 \leq s \leq r$, then $\rho_s \otimes_L L_{\mathfrak{p}}$ occurs in $H^1_f(K_r(\sqrt[q^r]{a}), V)$ with odd multiplicity, by Shapiro's Lemma combined with Theorem 0.4(1) applied to each g_s and χ_s. As the trivial representation ρ_0 occurs with multiplicity $h^1_f(F_0, V)$, it follows that

$$h^1_f(K_r(\sqrt[q^r]{a}), V) - h^1_f(F_0, V) \geq \sum_{s=1}^{r} \dim(\rho_s) = \sum_{s=1}^{r} \varphi(q^s) = q^r - 1.$$

References

[A-N] E. Aflalo, J. Nekovář, *Non-triviality of CM points in ring class field towers*, preprint.

[B-K] 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.

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

[C-F-K-S] J. Coates, T. Fukaya, K. Kato, R. Sujatha, *Root numbers, Selmer groups and non-commutative Iwasawa theory*, preprint.

[D] V. Dokchitser, *Root numbers of non-abelian twists of elliptic curves*, Proc. London Math. Soc. **91** (2005), 300–324.

[D-D1] T. Dokchitser, V. Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, `http://arxiv.org/abs/0610290`

[D-D2] T. Dokchitser, V. Dokchitser, *Regulator constants and the parity conjecture*, `http://fr.arxiv.org/abs/0709.2852`

[F-PR] 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.

[G-P] B. Gross, D. Prasad, *Test vectors for linear forms*, Math. Ann. **291** (1991), 343–355.

[J-L] H. Jacquet, R.P. Langlands, *Automorphic forms on GL(2)*, Lect. Notes in Math. **114**, Springer, Berlin, 1970.

[J] H. Jacquet, *Automorphic forms on GL(2) II*, Lect. Notes in Math. **278**, Springer, Berlin, 1972.

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

[N 1] J. Nekovář, *Selmer complexes*, Astérisque **310**, S.M.F., Paris, 2006.

[N 2] J. Nekovář, *The Euler system method for CM points on Shimura curves*, L-functions and Galois representations (Durham, July 2004), LMS Lecture Note Series **320**, Cambridge Univ. Press, 2007, pp. 471–547.

[N 3] J. Nekovář, *On the parity of ranks of Selmer groups III*, Doc. Math. **12** (2007), 243–274.

[N 4] J. Nekovář, *On the parity of ranks of Selmer groups IV*, preprint.

[S] H. Saito, *On Tunnell's formula for characters of GL(2)*, Compos. Math. **85** (1993), 99–108.

[T] J. Tunnell, *Local ε-factors and characters of GL_2*, Am. J. Math. **105** (1983), 1277–1308.

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

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