ISSN 0012-9593

quatrième série - tome 41 *fascicule 6* *novembre-décembre 2008*

ANNALES SCIENTIFIQUES de L'ÉCOLE NORMALE SUPÉRIEURE

Jan Nekovář

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

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Ann. Scient. Éc. Norm. Sup.
4^e série, t. 41, 2008, p. 1003 à 1022

GROWTH OF SELMER GROUPS OF HILBERT MODULAR FORMS OVER RING CLASS FIELDS

BY JAN NEKOVÁŘ

ABSTRACT. – We prove non-trivial lower bounds for the growth of ranks of Selmer groups of Hilbert modular forms over ring class fields and over certain Kummer extensions, by establishing first a suitable parity result.

RÉSUMÉ. – On donne des bornes inférieures non triviales sur la croissance des rangs des groupes de Selmer de formes modulaires de Hilbert sur les corps de classes d'anneau et sur des extensions de Kummer, en démontrant d'abord un résultat de parité.

0. Introduction

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

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 $\chi : \mathbb{A}_K^*/K^*\mathbb{A}_F^* \longrightarrow \mathbb{C}^*$ a (continuous) character of finite order. Fix a number field $L \subset \overline{\mathbb{Q}}$ 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 $G_F = \mathrm{Gal}(\overline{\mathbb{Q}}/F)$ 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 $\eta = \eta_{K/F} : \mathbb{A}_F^*/F^*N_{K/F}\mathbb{A}_K^* \xrightarrow{\sim} \{\pm 1\}$ the quadratic character corresponding to the extension K/F.

0012-9593/06/

0.2. – Normalising the reciprocity map $\mathrm{rec}_K : \mathbb{A}_K^*/K^* \longrightarrow \mathrm{Gal}(K^{\mathrm{ab}}/K)$ so that the local uniformisers correspond to geometric Frobenius elements, we identify χ with the corespond-ing Galois character $\chi : G_K = \mathrm{Gal}(\overline{\mathbb{Q}}/K) \longrightarrow O_L^* \subset L_{\mathfrak{p}}^*$; put $K_\chi = \overline{\mathbb{Q}}^{\mathrm{Ker}(\chi)}$. 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 $GL_2(\mathbb{A}_F)$ generated by g, and by θ_χ the automorphic representation of $GL_2(\mathbb{A}_F)$ 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. [13, 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 $\mathbb{C}$ and a functional equation of the form

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

Put

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

(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 ([2], [8]) predict that

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

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 $\varphi : \mathbb{A}_F^*/F^* \longrightarrow \overline{\mathbb{Q}}^*$ such that the newform associated to $g \otimes \varphi$ is p-ordinary; see* [13, 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 $2 \nmid r_{\mathrm{an}}(K, g, \chi)$, then $2 \nmid h_f^1(K, V \otimes \chi)$.*
2. *If $2 \mid r_{\mathrm{an}}(K, g, \chi)$ and if there exists a prime $v \mid p$ of F which does not split in K/F and for which $\pi(g)_v = \mathrm{St} \otimes \mu$, $\mu : F_v^* \longrightarrow \{\pm 1\}$, $\chi_w = \mu \circ N_{K_w/F_v}$, where w is the unique prime of K above v (as g is potentially ordinary, this can occur only if $k = 2$; see* [13, 12.5.4]*), then $2 \mid h_f^1(K, V \otimes \chi)$.*

(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. [13, 12.6.3.10] *and* [13, 12.6.4.3]*.)*

0.5. Corollary. – *Let $K[\infty] \subset K^{\mathrm{ab}}$ be the union of all ring class fields of K in the sense of* [1, 1.1] *(the Galois group $\mathrm{Gal}(K[\infty]/K)$ is the quotient of $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ by $\mathrm{rec}_K(\mathbb{A}_F^*)$). 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*

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

where

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

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 $\mathbb{Q}(\sqrt{-D})$, assume, in addition, that $p \neq 2$ and $F(\sqrt{-D}) \not\subset K_\chi$. Theorem 0.4 then implies the following:

1. If $2 \nmid \mathrm{ord}_{s=1} L(E/K, \chi, s)$, then
$$2 \nmid \left(\dim_L (E(K_\chi) \otimes L)^{(\chi^{-1})} + \mathrm{cork}_{O_{L,\mathfrak{p}}} (\text{Ш}(E/K_\chi) \otimes O_{L,\mathfrak{p}})^{(\chi^{-1})}\right).$$
2. If $2 \mid \mathrm{ord}_{s=1} L(E/K, \chi, s)$ and if there exist a prime $v \mid p$ of F which does not split in K/F and a character $\mu : F_v^* \longrightarrow \{\pm 1\}$ 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
$$2 \mid \left(\dim_L (E(K_\chi) \otimes L)^{(\chi^{-1})} + \mathrm{cork}_{O_{L,\mathfrak{p}}} (\text{Ш}(E/K_\chi) \otimes O_{L,\mathfrak{p}})^{(\chi^{-1})}\right).$$

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

0.7. Example [7]. – Let $q \neq 2$ be a prime number and F_0 a totally real number field such that $F_0 \cap \mathbb{Q}(\mu_{q^\infty}) = \mathbb{Q}$. 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 each $r \geq 1$, put $F_r = F_0\mathbb{Q}(\mu_{q^r})^+$, $K_r = F_0(\mu_{q^r})$; then $\mathrm{Gal}(K_r/F_0) \xrightarrow{\sim} (\mathbb{Z}/q^r\mathbb{Z})^*$ and $\mathrm{Gal}(K_r(\sqrt[q^r]{a})/K_r) \xrightarrow{\sim} \mathbb{Z}/q^r\mathbb{Z}$. Fix an injective character $\chi_r : \mathrm{Gal}(K_r(\sqrt[q^r]{a})/K_r) \longrightarrow \overline{\mathbb{Q}}^*$; then χ_r (more precisely, $\chi_r \circ \mathrm{rec}_{K_r}$) factors through $\mathbb{A}_{K_r}^*/K_r^*\mathbb{A}_{F_r}^*$.

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* $d = (-1)^{[F_0:\mathbb{Q}]} N(\mathfrak{n}_0^{(aq)}) \in \mathbb{Z} - \{0\}$. *Then:*

1. *For each* $r \geq 1$, $\varepsilon(\pi(g_r) \times \chi_r, \frac{1}{2}) = \left(\frac{d}{q}\right)$. *(See* [7, 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* $2 \nmid [F_0 : \mathbb{Q}]$*). If* $\left(\frac{d}{q}\right) = -1$, *then*

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

0.9. Corollaire. – *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* $F_0 \otimes \mathrm{End}_{\overline{\mathbb{Q}}}(E) \neq F_0(\sqrt{-q}))$ *(the latter condition is automatically satisfied if* $2 \nmid [F_0 : \mathbb{Q}]$*). Assume, finally, that* $\left(\frac{d}{q}\right) = -1$, *where* $d = (-1)^{[F_0:\mathbb{Q}]} N(\mathrm{cond}(E)^{(aq)})$. *Then, for each prime number* p *such that* E *has potentially ordinary reduction at all primes of* F_0 *above* p, *the ranks*

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

satisfy

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