On the parity of ranks of Selmer groups IV

Jan Nekovář

In recent years a substantial progress has been made on the parity conjecture for Selmer groups of elliptic curves and Hilbert modular forms. It seems, however, that the authors interested exclusively in elliptic curves or in abelian varieties considered as motives with rational coefficients ([CFKS], [DD1-4], [Gr2], [K1-2], [MR1-2]) and those striving for utmost generality ([N1-4]) inhabit two separate universes. The purpose of this note is to explain that a combination of the techniques of the two schools yields the following result.

Theorem 1. *Let k be a totally real number field, k_0/k a finite abelian extension and k'/k_0 a Galois extension of odd degree. Let E be an elliptic curve over k; assume that at least one of the following conditions is satisfied:*
(a) *E is modular (over k) and $2 \nmid [k:\mathbf{Q}]$;*
(b) *$j(E) \notin \mathcal{O}_k$;*
then, for each prime number $p \neq 2$, the parity conjecture

$$C_{par}(E/k', p) \qquad \operatorname{cork}_{\mathbf{Z}_p} \operatorname{Sel}_{p^\infty}(E/k') \equiv \operatorname{ord}_{s=1} L(E/k', s) \pmod 2$$

holds. If $k = \mathbf{Q}$, then the statement also holds for $p = 2$.

Above, $\operatorname{Sel}_{p^\infty}(E/k')$ is the Selmer group for the p-power descent on E, which sits in an exact sequence

$$0 \longrightarrow E(k') \otimes \mathbf{Q}_p/\mathbf{Z}_p \longrightarrow \operatorname{Sel}_{p^\infty}(E/k') \longrightarrow Ш(E/k')[p^\infty] \longrightarrow 0.$$

By [Wn, Thm. A.1], the elliptic curve E is potentially modular (i.e., it becomes modular over a suitable finite totally real extension of k). This implies that the L-function $L(E/k', s)$ admits meromorphic continuation to $\mathbf{C}$ and satisfies the expected functional equation ([T1, proof of Cor. 2.2], [N2, 12.11.6]). In particular, $\operatorname{ord}_{s=1} L(E/k', s) \in \mathbf{Z}$ is well-defined.

One can deduce more general parity results by combining Theorem 1 with [MR1, Thm. 6.4, 7.1], [MR2, Thm. 1.1], [Gr2, §11.8] or [DD4, Thm. 4.4, 4.6] (in these articles the authors prove relative results of the form "$C_{par}(E/k', p)$ implies $C_{par}(E/L, p)$ for various extensions L/k'").

In the case when E has potentially ordinary reduction at all primes above p, Theorem 1 was proved (even for $p = 2$) in [N2, 12.9-11] (note that the proof of [N2, Cor. 12.2.10(1),(2)] (resp., of [N2, Cor. 12.2.10(3)]) works unconditionally, by [Wn, Thm. A.1] (resp., by [Wn, Prop. A.2] applied to $T = \{v \mid p\}$)). To treat the general case we are going to replace in the arguments the Iwasawa-theoretical result [N2, 10.7.17] by the following result of Mazur and Rubin (a special case of [MR1, Thm. 7.1]).

Theorem 2 (special case of [MR1, Thm. 7.1]). *Let $p \neq 2$ be a prime number, K/k a quadratic extension of number fields, F an abelian extension of K of p-power order, dihedral over k. Assume that no finite prime of K stable under $\operatorname{Gal}(K/k)$ ramifies in F/K. Then, for each elliptic curve E over k and each character χ of $\operatorname{Gal}(F/K)$,*

$$\operatorname{cork}_{\mathbf{Z}_p[\chi]} \operatorname{Sel}_{p^\infty}(E/F)^{(\chi)} \equiv \operatorname{cork}_{\mathbf{Z}_p} \operatorname{Sel}_{p^\infty}(E/K) \pmod 2,$$

where we have denoted by $\mathbf{Z}_p[\chi]$ the ring generated over $\mathbf{Z}_p$ by the values of χ and by

$$N^{(\chi)} = \{n \in N \otimes_{\mathbf{Z}_p} \mathbf{Z}_p[\chi] \mid \forall g \in \operatorname{Gal}(F/K) \quad g(n) = \chi(g)n\}$$

the χ-component of any $\mathbf{Z}_p[\operatorname{Gal}(F/K)]$-module N.

Proof of Theorem 1. **Step 1: reduction to the case $k' = k$** (cf., [N2, 12.11.2,7,8]; p is arbitrary)

This can be carried out in the following general context. Let $M \simeq M^\vee(1)$ be a self-dual pure motive over a number field K with coefficients in a number field $L \subset \overline{\mathbf{Q}}$. Fix embeddings $i_\infty : \overline{\mathbf{Q}} \hookrightarrow \mathbf{C}$ and $i_p : L \hookrightarrow \overline{\mathbf{Q}}_p$; let $\mathfrak{p}$ be the prime of L induced by i_p. The $\mathfrak{p}$-adic realization of M is a self-dual $\mathfrak{p}$-adic

geometric representation $M_{\mathfrak{p}} \simeq M_{\mathfrak{p}}^{\vee}(1)$ of $\mathrm{Gal}(\overline{K}/K)$ (pure of weight -1 at almost all finite primes). The parity conjecture for the Bloch-Kato Selmer group of $M_{\mathfrak{p}}$ predicts that the integer

$$\delta(K, M, p) := \dim_{L_{\mathfrak{p}}} H^1_f(K, M_{\mathfrak{p}}) - \mathrm{ord}_{s=0} L(i_\infty M/K, s) \in \mathbf{Z}$$

satisfies

$$C_{par}(K, M, p) \qquad \delta(K, M, p) \stackrel{?}{\equiv} 0 \pmod 2$$

(provided that $L(i_\infty M/K, s)$ admits meromorphic continuation around $s = 0$). For $K = k$, $M = h^1(E)(1)$, $L = \mathbf{Q}$ and $\mathfrak{p} = p$ this boils down to the usual parity conjecture

$$C_{par}(E/k, p) \qquad \mathrm{cork}_{\mathbf{Z}_p} \mathrm{Sel}_{p^\infty}(E/k) \stackrel{?}{\equiv} \mathrm{ord}_{s=1} L(E/k, s) \pmod 2.$$

Proposition 3. *Let K'/K be a finite Galois extension with Galois group G. Denote by $\widehat{G}$ the set of isomorphism classes of irreducible representations of G over $\overline{\mathbf{Q}}$ and by $\widehat{G}^\circ = \{\rho \in \widehat{G} \mid \rho \simeq \rho^\vee\}$ the self-dual ones. After an extension of scalars we can assume that all $\rho \in \widehat{G}$ are defined over L. If, for each $\rho \in \widehat{G}$, the L-function $L(i_\infty M \otimes \rho/K, s)$ admits meromorphic continuation around $s = 0$ and satisfies the expected functional equation, then*

$$\delta(K', M, p) \equiv \sum_{\rho \in \widehat{G}^\circ} \delta(K, M \otimes \rho, p) \cdot \dim(\rho) \pmod 2.$$

In particular, the validity of $C_{par}(K, M \otimes \rho, p)$ for all $\rho \in \widehat{G}^\circ$ implies the validity of $C_{par}(K', M, p)$. If G is abelian, then $\widehat{G}$ is the character group of G and $\widehat{G}^\circ = \{\chi \in \widehat{G} \mid \chi^2 = 1\}$; thus

$$\delta(K', M, p) \equiv \sum_{\chi \in \widehat{G}, \chi^2 = 1} \delta(K, M \otimes \chi, p) \pmod 2.$$

Proof. The following argument can be, essentially, extracted from [N2, 12.11.2,7,8]. There are standard decompositions

$$\begin{aligned} L(i_\infty M/K', s) &= \prod_{\rho \in \widehat{G}} L(i_\infty M \otimes \rho/K, s)^{\dim(\rho)}, \\ H^1_f(K', M_{\mathfrak{p}}) = H^1_f(K, M_{\mathfrak{p}} \otimes \mathbf{Z}[G]) &= \bigoplus_{\rho \in \widehat{G}} H^1_f(K, M_{\mathfrak{p}} \otimes \rho)^{\dim(\rho)}. \end{aligned} \tag{3.1}$$

If $\rho \notin \widehat{G}^\circ$, then

$$\mathrm{ord}_{s=0} L(i_\infty M \otimes \rho/K, s) = \mathrm{ord}_{s=0} L(i_\infty M \otimes \rho^\vee/K, s), \tag{3.2}$$

by the functional equation (the archimedean L-factors do not have a pole at $s = 0$ in the self-dual case) and

$$\dim_{L_{\mathfrak{p}}} H^1_f(K, M_{\mathfrak{p}} \otimes \rho) = \dim_{L_{\mathfrak{p}}} H^1_f(K, M_{\mathfrak{p}} \otimes \rho^\vee) \tag{3.3}$$

by the self-duality result [N2, 12.5.9.5(iv)] (the loc. cit. considers only the case of abelian G, but the argument works in general. A similar result for finite Galois modules is proved in [Wi, Prop. 1.6]. The ordinary case was treated earlier in [Gr1, Prop. 2]). A special case of such a self-duality (for $M = h^1(A)(1)$, $L = \mathbf{Q}$ and $\mathfrak{p} = p \neq 2$) was reproved by another method in [DD3, Thm. 1.1]. The statement of the Proposition follows from (3.1-3).

Corollary 4. *If $K \subset K_0 \subset K_1 \subset \cdots \subset K_n$ is a chain of finite extensions such that K_0/K is abelian and each K_i/K_{i-1} $(i = 1, \ldots, n)$ is abelian of odd degree, then Proposition 3 applied to K_0/K and all K_i/K_{i-1} yields*

$$\delta(K_n, M, p) \equiv \sum_{\chi \in \widehat{G}, \chi^2 = 1} \delta(K, M \otimes \chi, p) \pmod 2, \qquad G = \mathrm{Gal}(K_0/K).$$

Completion of Step 1. As k'/k_0 is a Galois extension of odd degree, it is solvable (of odd degree). Corollary 4 for $K = k$, $K_0 = k_0$, $K_n = k'$ and $M = h^1(E)(1)$ then implies that $C_{par}(E/k', p)$ follows from $C_{par}(E \otimes \chi/k, p)$ for all quadratic twists of E by $\chi : \mathrm{Gal}(k_0/k) \longrightarrow \{\pm 1\}$ (the assumptions on the L-functions in Proposition 3 are satisfied, by potential modularity of E ([T1, proof of Cor. 2.2], [N2, 12.11.6])). If $k = \mathbf{Q}$, then $C_{par}(E/\mathbf{Q}, 2)$ was proved in [Mo]; Corollary 4 then implies $C_{par}(E/k', 2)$.

Step 2: Proof of Theorem 1 in the case (a), $k' = k$, $p \neq 2$ (cf., [N2, 12.9.5.2,3])

Let B a quaternion algebra over k ramified at all infinite primes of k except one (and at no finite prime). Let $R \subset B$ be an Eichler order of level $\mathrm{cond}(E)$ and N_H^* the (smooth projective) Shimura curve over k associated to B^*/F^* and the open compact subgroup $H = (R \otimes \hat{\mathbf{Z}})^* \subset (B \otimes \hat{\mathbf{Z}})^*$ ([N3, 1.4]). Modularity of E implies that there is a non-constant k-morphism $\mathrm{Jac}(N_H^*) \longrightarrow E$; denote by $\alpha : N_H^* \longrightarrow E$ its composition with an integral multiple of the Hodge embedding ([Zh, p. 30], [CV, 3.5], [N3, 1.19]).

Fix a prime P of k above p and an imaginary quadratic extension K/k in which all primes of k dividing $P\,\mathrm{cond}(E)$ split; then

$$\mathrm{ord}_{s=1} L(E/K, s) \equiv [k : \mathbf{Q}] \equiv 1 \pmod 2$$

([MR2, Remark 1.2]). The infinite ring class field $K[P^\infty]$ in the sense of [N2, 12.6.1.4] is an abelian extension of K unramified outside the primes of K above P, is dihedral over k, and $G = \mathrm{Gal}(K[P^\infty]/K) \simeq G_{\mathrm{tors}} \times \mathbf{Z}_p^r$ with $r = [k_P : \mathbf{Q}_p]$ and G_{tors} finite. By [CV, Thm. 4.2] there exist an integer n big enough so that G_{tors} injects into $G_n = \mathrm{Gal}(K[P^n]/K)$, a CM point $x \in N_H^*(K[P^n])$ and a character $\chi : G_n \longrightarrow \mathbf{Z}_p[\chi]^*$ not factoring through G_{n-1} with $\chi(G_{\mathrm{tors}}) = \{1\}$ and such that

$$e_\chi(\alpha(x)) = \sum_{g \in G_n} \chi^{-1}(g)\, \alpha(x) \in (E(F_n) \otimes \mathbf{Z}_p)^{(\chi)} \qquad (F_n = K[P^n]^{G_{\mathrm{tors}}})$$

is not torsion. This implies, by a generalisation of [BD, Thm. 2.2] proved in [N3, Thm. 3.2] (as E does not have CM by K; see [N2, 12.9.6]), that

$$\mathrm{cork}_{\mathbf{Z}_p[\chi']} \mathrm{Sel}_{p^\infty}(E/F_n)^{(\chi')} = 1,$$

where χ' is the character of $\mathrm{Gal}(F_n/K) = G_n/G_{\mathrm{tors}}$ through which χ factors. Applying Theorem 2 to the extension F_n/K we obtain $C_{par}(E/K, p)$:

$$\mathrm{cork}_{\mathbf{Z}_p} \mathrm{Sel}_{p^\infty}(E/K) \equiv 1 \equiv \mathrm{ord}_{s=1} L(E/K, s) \pmod 2.$$

Varying K as in [N2, 12.10.9] we deduce $C_{par}(E/k, p)$.

Step 3: First reduction in the case (b), $k' = k$ (cf., [N2, 12.10.5,6])

There is a totally real quadratic extension k_2/k such that the quadratic twist $E \otimes \chi$ of E by the corresponding quadratic character $\chi : \mathrm{Gal}(k_2/k) \xrightarrow{\sim} \{\pm 1\}$ has multiplicative reduction at some prime Q of k. Applying Corollary 4 to k_2/k we see that it is enough to prove $C_{par}(E \otimes \chi/?, p)$ over $? = k, k_2$. Moreover, after possibly replacing k by a cyclic extension of odd order in which Q splits we can assume that there is a prime $P \neq Q$ above p (cf., [N2, 12.10.6]).

Step 4: Application of a variant of Brauer's theorem ($p \neq 2$) (cf., [T1], [N2, 12.11.6])

Thanks to Step 3, we can assume that there is a prime Q of k at which E has multiplicative reduction and a prime $P \neq Q$ of k above p.

By assumption there exists a totally real finite Galois extension $\widetilde{k}/k$ over which E becomes modular; set $G = \mathrm{Gal}(\widetilde{k}/k)$. By [CR, Thm. 15.10] there exist solvable subgroups $H_j \subset G$ and integers $n_j \in \mathbf{Z}$ such that there is an equality of virtual representations of G

$$1_G = \sum_j n_j \operatorname{Ind}_{H_j}^G(1_{H_j});$$

set $k_j = \widetilde{k}^{H_j}$. As

$$L(E/k,s) = \prod_j L(E/k_j,s)^{n_j}, \qquad \operatorname{cork}_{\mathbf{Z}_p} \operatorname{Sel}_{p^\infty}(E/k) = \sum_j n_j \operatorname{cork}_{\mathbf{Z}_p} \operatorname{Sel}_{p^\infty}(E/k_j),$$

it is enough to prove $C_{par}(E/k_j,p)$ for all j. Fix j; then E is modular over k_j ([T2], proof of Thm. 2.4). If $2 \nmid [k_j:\mathbf{Q}]$, then we apply Step 2. Assume that $2 \mid [k_j:\mathbf{Q}]$. There exists a prime Q_j of k_j at which $E \otimes_k k_j$ has multiplicative reduction and a prime $P_j \neq Q_j$ of k_j above p.

Fix a totally imaginary quadratic extension K_j/k_j in which Q_j is inert and all primes of k_j dividing $P_j Q_j^{-1}\mathrm{cond}(E/k_j)$ are split. Let B_j be a quaternion algebra over k_j ramified at Q_j and at all infinite primes of k_j except one. There exists a k_j-embedding of K_j into B_j and we have (again by [MR2], Remark 1.2)

$$\operatorname{ord}_{s=1} L(E/K_j,s) \equiv [k_j:\mathbf{Q}] + 1 \equiv 1 \pmod 2.$$

The argument of Step 2 then applies to the Eichler order $R_j \subset B_j$ of level $Q_j^{-1}\mathrm{cond}(E/k_j)$ and the ring class field $K_j[P_j^\infty]$, yielding $C_{par}(E/k_j,p)$ for all j. This completes the proof of Theorem 1.

Acknowledgements: The author is grateful to Jean-Pierre Wintenberger for the appendix to this article and to a referee for helpful comments and corrections.

References

[BD] M. Bertolini, H. Darmon, *Kolyvagin's descent and Mordell-Weil groups over ring class fields*, J. reine angew. Math. **412** (1990), 63–74.

[CFKS] J. Coates, T. Fukaya, K. Kato, R. Sujatha, *Root numbers, Selmer groups and non-commutative Iwasawa theory*, J. Alg. Geom., to appear.

[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*, L-functions and Galois representations (Durham, July 2004), LMS Lecture Note Series **320**, Cambridge Univ. Press, 2007, pp. 121–186.

[DD1] T. Dokchitser, V. Dokchitser, *Parity of ranks for elliptic curves with a cyclic isogeny*, J. Number Theory, **128** (2008), 662–679.

[DD2] T. Dokchitser, V. Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Ann. Math., to appear.

[DD3] T. Dokchitser, V. Dokchitser, *Self-duality of Selmer groups*, Math. Proc. Cam. Phil. Soc. **146** (2009), 257–267.

[DD4] T. Dokchitser, V. Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math., to appear.

[Gr1] R. Greenberg, *Trivial zeros of p-adic L-functions*, Contemporary Math. **165** (1994), 149–173.

[Gr2] R. Greenberg, *Iwasawa theory, projective modules, and modular representations*, preprint.

[K1] B.D. Kim, *The Parity Theorem of Elliptic Curves at Primes with Supersingular Reduction*, Compositio Math. **143** (2007), 47–72.

[K2] B.D. Kim, *The parity conjecture over totally real fields for elliptic curves at supersingular reduction primes*, preprint.

[Mo] P. Monsky, *Generalizing the Birch-Stephens theorem. I. Modular curves*, Math. Zeit. **221** (1996), 415–420.

[MR1] B. Mazur, K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Annals of Math. **166** (2007), 581–614.

[MR2] 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), S.M.F., Paris.

[N3] 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.

[N4] J. Nekovář, *Growth of Selmer groups of Hilbert modular forms over ring class fields*, Ann. E.N.S., sér. 4, **41** (2008), 1003–1022.

[T1] R. Taylor, *Remarks on a conjecture of Fontaine and Mazur*, J. Inst. Math. Jussieu **1** (2002), 1–19.

[T2] R. Taylor, *On icosahedral Artin representations II*, Amer. J. Math. **125** (2003), 549–566.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. Math. **141** (1995), 443–551.

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

[Zh] S.-W. Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2) **153** (2001), 27–147.

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

APPENDIX: POTENTIAL MODULARITY OF ELLIPTIC CURVES OVER TOTALLY REAL FIELDS

JEAN-PIERRE WINTENBERGER

The following theorem is well known to experts.

Theorem A.1. *Let E an elliptic curve over a totally real number field F. Then there exists a totally real number field $F' \supset F$ such that $E_{F'}$ is modular.*

We explain what we mean by "modular". Let F' be a totally real number field (a finite extension of $\mathbb{Q}$). Let π be a cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_{F'})$. We shall suppose that the archimedean components of π are such that π corresponds to a Hilbert modular form of parallel weight 2. Taylor has associated to π a compatible system $(\rho_{\pi,\lambda})$ of representations of the Galois group $G_{F'}$ ([12]). There is a conductor $\mathfrak{n}$, which is an ideal of the rings of integers of F', a Hecke algebra $\mathbb{T}$ with Hecke operators $T_{\mathfrak{q}} \in \mathbb{T}$ for $\mathfrak{q}$ a prime of F' not dividing $\mathfrak{n}$, and a morphism $\theta : \mathbb{T} \to \mathbb{C}$. The subfield L of $\mathbb{C}$ generated by the image of θ is a finite extension of $\mathbb{Q}$. For each prime λ of L, the Galois representation $\rho_{\pi,\lambda} : G_{F'} \to \mathrm{GL}_2(L_\lambda)$ is absolutely irreducible (prop. 2.1. of [14]), unramified outside the primes dividing $\mathfrak{n}$ and the rational prime ℓ below λ, and is characterized by :

$$\mathrm{tr}(\rho_{\pi,\lambda}(\mathrm{Frob}_{\mathfrak{q}})) = \theta(T_{\mathfrak{q}}),$$

for every prime $\mathfrak{q}$ of F' which is prime to $\mathfrak{n}\ell$.

When we say that E is modular over F', we mean that there exists such a π such that, for any prime λ of L, the Galois representation $\rho_{\pi,\lambda}$ is isomorphic to the Galois representation $\rho(E)_\ell$ given by the action of $G_{F'}$ on the Tate module $V_\ell(E) = \mathbb{Q}_\ell \otimes_{\mathbb{Z}_\ell} \lim_n E(\overline{\mathbb{Q}})[\ell^n]$ (ℓ is the characteristic of λ). By compatibility of the Galois representations attached to π and E and the absolute irreducibility of the Galois representations attached to π, it suffices to check the isomorphism $\rho_{\pi,\lambda} \simeq \rho(E)_\ell$ for one λ.

Of course, it is believed that one can take $F' = F$ in the theorem. The following proposition is much weaker, but it is useful (see [5] cor. 12.2.10 and def. 12.11.3, and [6] comments after thm. 1).

Proposition A.2. *Let T be a finite set of primes of F such that E has good reduction at all $\mathfrak{q} \in T$. One can then impose that F'/F is unramified at T.*

Remark. Let N be a finite extension of F. One can furthermore impose that N and F' are linearly disjoint extensions of F (prop. 2.1. of [2]).

Let us give a proof of the theorem and the proposition.

If $E_{\overline{\mathbb{Q}}}$ has complex multiplication (by a quadratic field L), $V_\ell(E)$ is induced from the Galois character of G_{LF} attached to a Hecke character of LF and E is modular over F (prop. 12.1 of [3]).

From now on, suppose that $E_{\overline{\mathbb{Q}}}$ has no complex multiplication. We denote by M the smallest Galois extension of $\mathbb{Q}$ containing F. For each prime $\mathfrak{l}$ of F such that E has good reduction at $\mathfrak{l}$, we denote by $a_\mathfrak{l}$ the trace of the Frobenius $\mathrm{Frob}_\mathfrak{l}$ of E, *i.e.* $\mathrm{Norm}(\mathfrak{l}) + 1 - a_\mathfrak{l}$ is the number of points of E in the residue field $k(\mathfrak{l})$.

The following lemma is a variant of a theorem of Serre (8.2. of [8]).

Lemma A.3. *There exist infinitely many rational primes ℓ which satisfy the following properties :*

- i) $\ell > 5$, ℓ splits completely in the Galois extension $M/\mathbb{Q}$;

- ii) E has good ordinary reduction at each prime $\mathfrak{l}$ of F above ℓ ;

- iii) $a_\mathfrak{l} \not\equiv -1, 1 \bmod. \ \ell$.

Proof. For ℓ that splits completely in F and $\mathfrak{l}$ a prime of F above ℓ such that E has good reduction at $\mathfrak{l}$, one has $\mid a_\mathfrak{l} \mid < 2\sqrt{\ell}$. Furthermore, the ordinarity condition in ii) is equivalent to the condition that ℓ does not divide $a_\mathfrak{l}$. For $\ell > 5$, it follows that the congruences $a_\mathfrak{l} \equiv -1, 0, 1 \bmod. \ \ell$ are equivalent to the equalities $a_\mathfrak{l} = -1, 0, 1$. One sees that, to prove the lemma, one has to find infinitely many rational primes ℓ satifying i), such that, at each prime $\mathfrak{l}$ of F above ℓ, E has good reduction at $\mathfrak{l}$ and $a_\mathfrak{l} \neq -1, 0, 1$.

Since $E_{\overline{\mathbb{Q}}}$ has no complex multiplication, a theorem of Serre ([9]) implies that there exists q_0 such that, for each rational prime $q > q_0$, the image of G_M in the Galois group of the extension $M_{[q]}$ of M generated by the points of order q of E is isomorphic to $\mathrm{GL}_2(\mathbb{F}_q)$. The number of elements of $\mathrm{GL}_2(\mathbb{F}_q)$ is $f(q) = (q^2-1)(q^2-q)$. The number of elements of $\mathrm{GL}_2(\mathbb{F}_q)$ of trace t is $f_0(q) = 2(q-1)^2 + (q-2)(q^2-q+1)$ if $t \neq 0$ and $f_1(q) = (q-1)^2 + (q-1)(q^2-q+1)$ if $t = 0$. The quotients $f_0(q)/f(q)$ and $f_1(q)/f(q)$ have limit 0 when q goes to ∞. By choosing $q > q_0$ sufficiently large, it follows from Chebotarev's theorem applied to $M_{[q]}/M$ that, for each $\epsilon > 0$, there exists a set $\mathcal{P}_M$ of primes of M of density $> 1 - \epsilon$ such that for $\mathfrak{l} \in \mathcal{P}_M$, one has $a_\mathfrak{l} \neq -1, 0, 1$. Let $\mathcal{P}'_M$ be the set of primes $\mathfrak{l}$ of M such that $\sigma(\mathfrak{l}) \in \mathcal{P}_M$ for all σ in the Galois group of $M/\mathbb{Q}$. The density of $\mathcal{P}'_M$ is bigger than $1 - [M : \mathbb{Q}]\epsilon$. By that we mean that the lower limit of $\sum_{\mathfrak{l} \in \mathcal{P}'_M} \mathrm{Norm}(\mathfrak{l})^{-s} / \sum_\mathfrak{l} \mathrm{Norm}(\mathfrak{l})^{-s}$ when $s \to 1^+$ is bigger than $1 - [M : \mathbb{Q}]\epsilon$. Choosing $\epsilon < 1/[M : \mathbb{Q}]$, we see that $\mathcal{P}'_M$ is infinite, which proves the lemma. □

Let ℓ be as in the lemma and such that

- no prime of F above ℓ belongs to T,

- G_M maps surjectively onto $\mathrm{GL}_2(\mathbb{F}_\ell)$.

Apply Taylor's potential modularity theorem 1.6. of [13] to the representation $\bar{\rho}$ of G_F in $\mathrm{GL}(E[\ell])$. As E has good ordinary reduction at primes

above ℓ, the reducibility hypotheses of the restriction of $\bar{\rho}$ to the decomposition group of primes above ℓ are satisfied. We get :

- a totally real finite extension F' of F, F'/F Galois, such that every prime $\mathfrak{l}$ of F above ℓ splits completely in F';

- a cuspidal automorphic representation π of of $\mathrm{GL}_2(\mathbb{A}_{F'})$, whose archimedean components are as described above after the statement of the theorem, and a place λ of the field of coefficients of π above ℓ such that $\rho_{\pi,\lambda}$ and $\bar{\rho}_{|G_{F'}}$ have isomorphic reductions : $\bar{\rho}_{\pi,\lambda} \simeq \bar{\rho}_{|G_{F'}}$;

- for every prime $\mathfrak{l}'$ of F' above ℓ, the restriction of $\rho_{\pi,\lambda}$ to the inertia subgroup $I_{\mathfrak{l}'}$ is of the form :

$$\begin{pmatrix} \chi_\ell & * \\ 0 & 1 \end{pmatrix},$$

where χ_ℓ is the cyclotomic character.

To prove the proposition, we furthermore require that no prime of F in T ramifies in F'.

We explain what we have to add to the arguments of Taylor in [13] to check that this is possible. Let p as in [13] be the auxiliary prime such that the considered moduli problem for Hilbert-Blumenthal abelian varieties has p-level structure induced from a character of a quadratic extension L of F.

Firstly, we can choose the level structure at p so that it is unramified at all primes in T. We choose the auxiliary prime p such that no prime of F above p is in T. When we apply lemma 1.1. of [13], we impose that every prime of T splits in the quadratic extension L of $F = K$. We choose the set S of primes of F such that it contains our T. We choose the characters $\overline{\psi}_x$ for $x \in T$ unramified. We have that ϕ in lemma 1.1. is the cyclotomic character. In the proof of lemma 1.1. on page 132, we have that ψ_x is unramified. We see that $\mathrm{Ind}_{G_L}^{G_K}\psi$ is unramified at all primes in T.

We apply the theorem of Moret-Bailly ([4] ; prop. 2.1. of [2]) to the Hilbert-Blumenthal modular variety X on page 136 of [13]. We want to ensure that F'/F is unramified at all primes in T. By Moret-Bailly, this will follow from the fact that $X(F_{v,\mathrm{ur}})$ is non-empty, for each $v \in T$, where $F_{v,\mathrm{ur}}$ is the maximal unramified extension of F_v. We deduce that $X(F_{v,\mathrm{ur}})$ is non-empty from the fact that the p and ℓ level structures are unramified at $v \in T$ and the following fact proved by Rapoport and Deligne-Pappas ([7], [1]) : X has a compactification $\overline{X}$ proper over $\mathbb{Z}[1/p\ell]$, smooth over $\mathbb{Q}$, with absolutely irreducible fibers and there is an open subscheme U of $\overline{X}$ smooth over $\mathbb{Z}[1/p\ell]$ which is dense in each fiber and which parametrizes abelian schemes with suitable additional structures. For $v \in T$, we take the open subset $\Omega_v \subset X(F_v)$ of prop. 2.1. of [2] to be the set of points of U with values in the ring of integers $O_{v,\mathrm{ur}}$ of $F_{v,\mathrm{ur}}$. The set Ω_v is not empty as the scheme U has a point with values in the algebraic closure of the residue field of F_v, and, by smoothness, this point can be lifted to a point with values in $O_{v,\mathrm{ur}}$.

We finish the proof of the theorem and the proposition. A theorem of Skinner and Wiles (th. 5.1. of [10]) implies the modularity of $\rho_{|G_{F'}}$. The theorem of Skinner and Wiles is quoted as theorem 4 in [11]. In [11], Skinner also states a "theorem 3", which he says should be possible to prove. The proof of theorem 4 relies on a deep and difficult argument using Hida's theory, and is mainly concerned with Galois representations whose reduction does not have "big image". This is not our problem, and the "less sophisticated" "theorem 3" should be enough for our argument. Indeed, it follows from the congruences $a_{\mathfrak{l}'} \not\equiv -1, 1 \bmod. \ell$ that for each prime $\mathfrak{l}'$ of E' above ℓ, $\pi_{\mathfrak{l}'}$ is not a twist of the special representation and we have the minimality hypothesis for $\rho_{\pi,\lambda}$ needed to apply "theorem 3".

References

[1] P. Deligne and G. Pappas Singularités des espaces de modules de Hilbert, en les caractéristiques divisant le discriminant. Compositio Mathematica, vol. 90 (1), 59–79, 1994.

[2] M. Harris, N. Shepherd-Barron and R. Taylor. A family of Calabi-Yau varieties and potential automorphy. Ann. Math., to appear.

[3] H. Jacquet and R. P. Langlands. Automorphic forms on GL(2). Lecture Notes in Mathematics, Vol. 114, Springer-Verlag, Berlin, 1970.

[4] L. Moret-Bailly. Groupes de Picard et problèmes de Skolem. I, II. *Ann. Sci. École Norm. Sup. (4)*, 22(2):161–179, 181–194, 1989.

[5] J. Nekovář. Selmer complexes. Astérisque, Vol. 310, 2006.

[6] J. Nekovář. On the parity of ranks of Selmer groups IV.

[7] M. Rapoport. Compactifications de l'espace de modules de Hilbert-Blumenthal. Compositio Mathematica, vol. 36 (3), 255–335, 1978.

[8] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev, Institut des Hautes Études Scientifiques. Publications Mathématiques, 54, 1981, 323–401.

[9] J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Inventiones Mathematicae, 15(4), 259–331,1972.

[10] C. M. Skinner and A. Wiles. Nearly ordinary deformations of irreducible residual representations. Annales de la Faculté des Sciences de Toulouse. Mathématiques. Série 6, 10(1), 185–215, 2001.

[11] C. M. Skinner. Modularity of Galois representations. Les XXIIèmes Journées Arithmetiques (Lille, 2001), Journal de Théorie des Nombres de Bordeaux, 15(1), 367–381, 2003.

[12] R. Taylor. On Galois representations associated to Hilbert modular forms. *Invent. Math.*, 98(2):265–280, 1989.

[13] R. Taylor. Remarks on a conjecture of Fontaine and Mazur. *J. Inst. Math. Jussieu*, 1(1):125–143, 2002.

[14] A. Wiles. On p-adic representations for totally real fields. *Ann. of Math.*, 123: 407-456, 1986.

E-mail address: wintenb@math.u-strasbg.fr

J.-P. Wintenberger, Université Louis Pasteur, membre de l'Institut universitaire de France, Département de Mathématique, 9 rue René Descartes, 67084 Strasbourg Cedex, France