APPENDIX: POTENTIAL MODULARITY OF ELLIPTIC CURVES OVER TOTALLY REAL FIELDS

JEAN-PIERRE WINTENBERGER

The following theorem is well known to experts.

Theorem 0.1. *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 $T_{\mathfrak{q}} \in \mathbb{T}$, $\mathfrak{q}$ prime of F' prime to $\mathfrak{n}$, 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] thm. 1).

Proposition 0.2. *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 0.3. *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) $a_\mathfrak{l} \not\equiv -1, 1$ mod. ℓ.*

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 $a_\mathfrak{l} \equiv -1, 0, 1$ mod. ℓ 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 to $\mathrm{GL}_2(\mathbb{F}_\ell)$.

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 $O_{v,\mathrm{ur}}$.