

Potential modularity for elliptic curves and some applications

Cristian Virdol
Department of Mathematics
Columbia University

August 20, 2009

1 Introduction

It is conjectured that an elliptic curve E defined over a totally real number field F is modular i.e. the associated l -adic representation $\rho_E := \rho_{E,l}$ of $\Gamma_F := \text{Gal}(\bar{F}/F)$, for some rational prime l , is isomorphic to the l -adic representation $\rho_\pi := \rho_{\pi,l}$ of Γ_F associated to some automorphic representation π of $\text{GL}(2)/F$ (see §2 below for details). This conjecture was proved when $F = \mathbb{Q}$ (see [BCDT], [W]). In this paper we prove the following theorem, which is a particular case of Taylor's paper [T2] when the elliptic curves E_i have split multiplicative reduction at some finite place v of F :

Theorem 1.1. *Let F be a totally real number field, and for $i = 1, \dots, r$, let E_i be an elliptic curve defined over F . Then there exists a totally real Galois finite extension F' of F such that for $i = 1, \dots, r$, the elliptic curve E_i/F' is modular.*

As an application to Theorem 1.1, in Theorem 4.1 of §4 we prove the meromorphic continuation of some L -functions, and also the Tate conjecture for a product of two or four elliptic curves defined over some totally real number field.

The author wishes to thank Brian Conrad and Haruzo Hida for helpful correspondence and to the referee for useful comments.

2 Modularity

Let E be an elliptic curve over a number field F . For a rational prime l , we denote by $T_l(E)$ the Tate module associated to E and by $\rho_E := \rho_{E,l}$ the natural l -adic representation of Γ_F on $T_l(E)$. By fixing an isomorphism $i : \bar{\mathbb{Q}}_l \rightarrow \mathbb{C}$ we can regard ρ_E as a complex-valued representation.

Consider now a totally real number field F . If π is an automorphic representation that is discrete series at infinity of weight 2 of $\text{GL}(2)/F$, then there exists ([T]) a λ -adic representation

$$\rho_\pi := \rho_{\pi,\lambda} : \Gamma_F \rightarrow \text{GL}_2(O_\lambda) \hookrightarrow \text{GL}_2(\bar{\mathbb{Q}}_l),$$

which is unramified outside the primes dividing $\mathbf{n}l$. Here O is the coefficients ring of π and λ is a prime ideal of O above some prime number l , \mathbf{n} is the level of π .

We say that an elliptic curve E defined over a totally real number field F is modular if there exists an automorphic representation π of weight 2 of $\mathrm{GL}(2)/F$ such that $\rho_E \sim \rho_\pi$. Here \sim , when we refer to equality of the corresponding L -functions of E and π , means that the Frobenius at almost all places have equal characteristic polynomials concerning the two representations.

3 The proof of Theorem 1.1

Let F be a totally real number field, and for $i = 1, \dots, r$, let E_i be an elliptic curve defined over F . If E_i has CM it is well known that E_i/F' is modular for any totally real finite extension F' of F (see for example Theorem 7.4 of [G]). Hence it is sufficient to prove Theorem 1.1 when each E_i does not have CM. We assume this fact from now on. In this paper, for a rational prime l , we denote by ϵ_l the l -adic cyclotomic character, or its reduction mod l , of $\Gamma_{\mathbb{Q}}$.

We know the following proposition, which for $r = 1$ this is Theorem 1.6 of [T1], but this result is true for general r and the proof is similar (for details see the proof of Theorem 3.1 of [HSBT]):

Proposition 3.1. *Suppose that $l > 3$ is an odd prime and that k/\mathbb{F}_l is a finite extension. Let F be a totally real number field and for $i = 1, \dots, r$, let $\rho_i : \Gamma_F \rightarrow \mathrm{GL}_2(k)$ be a continuous representation. Suppose that the following conditions hold:*

1. *The representation ρ_i is irreducible for each i .*
2. *For every place $v|l$ of F we have*

$$\rho_i|_{G_v} \sim \begin{pmatrix} \epsilon_l \chi_{iv}^{-1} & * \\ 0 & \chi_{iv} \end{pmatrix}$$

where G_v is the decomposition group above v , and χ_{iv} is an unramified character, 3. *For every complex conjugation c , we have $\det \rho_i(c) = -1$.*

Then there exists a finite Galois totally real extension F'/F in which every prime of F above l splits completely, for each $i = 1, \dots, r$, a cuspidal automorphic representation π'_i of $\mathrm{GL}(2)/F'$ and a place $\lambda'_i|l$ of the minimal field of rationality M_i of π'_i such that $\rho_i|_{\Gamma_{F'}} \sim \bar{\rho}_{\pi'_i, \lambda'_i}$, where $\rho_{\pi'_i, \lambda'_i} : \Gamma_{F'} \rightarrow \mathrm{GL}_2(M_i \lambda'_i)$ is the representation associated to π'_i , and $\bar{\rho}_{\pi'_i, \lambda'_i}$ is the reduction of $\rho_{\pi'_i, \lambda'_i}$ modulo λ'_i .

Moreover, if v' is a place of F' above a place $v|l$ of F , the representation π'_i can be chosen such that

$$\rho_{\pi'_i, \lambda'_i}|_{G_{v'}} \sim \begin{pmatrix} \epsilon_l \chi_{iv'}^{-1} & * \\ 0 & \chi_{iv'} \end{pmatrix}$$

where $G_{v'}$ is the decomposition group above v' , and $\chi_{iv'}$ is a tamely ramified lift of χ_{iv} .

We want to prove that the hypotheses of the Proposition 3.1 are satisfied for some rational prime $l > 3$ and the representations $\bar{\rho}_{E_i, l}$ for $i = 1, \dots, r$. From [S1], because E_i does not have CM, we know that $\rho_{E_i, l}(\Gamma_F)$ contains $\mathrm{SL}_2(\mathbb{Z}_l)$ for almost all l , and hence $\bar{\rho}_{E_i, l}(\Gamma_F)$ contains $\mathrm{SL}_2(\mathbb{F}_l)$ for almost all l , and thus the representation $\bar{\rho}_{E_i, l}$ is irreducible for almost all l . Hence we can choose a prime l such that for $i = 1, \dots, r$, the representation $\bar{\rho}_{E_i, l}$ is irreducible.

We say that an elliptic curve E defined over a number field F is ordinary at some place $v|l$ of F of good reduction for E , if $l \nmid a_v$ (here if k_v denotes the residue field of F at v and E_v is the reduction of E modulo v , then $a_v = |k_v| + 1 - |E_v(k_v)|$).

Theorem 3.2. *For $i = 1, \dots, r$, let E_i be a non-CM elliptic curve defined over a totally real number field F . Then the set of rational primes l , such that for $i = 1, \dots, r$, the elliptic curve E_i is ordinary at v for each place $v|l$ of F , has positive Dirichlet density.*

Proof: Let $l \geq 5$ be a rational prime which is completely split in F such that if v is a place of F above l , then E_i has good reduction at v for each $i = 1, \dots, r$. Hence if k_v is the residue field of F at v , then $|k_v| = |\mathbb{F}_l|$, and thus from Hasse inequality we obtain that $|a_{iv}| \leq 2\sqrt{|k_v|} = 2\sqrt{l}$, for each $i = 1, \dots, r$, where $a_{iv} = |k_v| + 1 - |E_{iv}(k_v)|$. Thus if E_i is not ordinary at v , i.e. if $l \mid a_{iv}$, we get that $a_{iv} = 0$, i.e. E_i is supersingular at v . But from Theorem 2.4 of [KLR] (see also the remark after the main theorem of [E]), we know that the set of supersingular primes of E_i over F has Dirichlet density 0, and hence, because the set of rational primes $l \geq 5$ which are completely split in F has positive Dirichlet density, we deduce that the set of rational primes l such that for each $i = 1, \dots, r$, the elliptic curve E_i is ordinary at v for each place $v|l$ of F has positive Dirichlet density. Thus we conclude Theorem 3.2. \square

For each $i = 1, \dots, r$, we have that $\det \rho_{E_i, l} = \epsilon_l$, and because E_i does not have CM, from Theorem 3.2 we know that there exists an infinite set of primes l such that for $i = 1, \dots, r$, the representation $\rho_{E_i, l}$ is ordinary (in the sense of Theorem 3.2), and hence for every place v of F above l we have

$$\rho_{E_i, l}|_{G_v} \sim \begin{pmatrix} \epsilon_l \chi_{iv}^{-1} & * \\ 0 & \chi_{iv} \end{pmatrix}$$

where χ_{iv} is an unramified character. Thus one could choose the prime l such that the representation $\bar{\rho}_{E_i, l}$ satisfies also the condition 2 of Proposition 3.1. Also the condition 3 of Proposition 3.1 is satisfied. Hence, for some rational prime l and the representations $\bar{\rho}_{E_i, l}$ for $i = 1, \dots, r$, we could find a finite Galois extension F'/F as in the conclusion of Proposition 3.1.

We now use the following result (Theorem 5.1 of [SW]):

Proposition 3.3. *Let F' be a totally real number field and let $\rho : \mathrm{Gal}(\bar{F}'/F') \rightarrow \mathrm{GL}_2(\mathbb{Q}_l)$ be a representation satisfying:*

1. ρ is continuous and irreducible,
2. ρ is unramified at all but a finite number of finite places,

3. $\det \rho(c) = -1$ for all complex conjugations c ,
4. $\det \rho = \psi \epsilon_l$, where ψ is a character of finite order,
5. $\rho|_{D_i} \sim \begin{pmatrix} \psi_1^{(i)} & * \\ 0 & \psi_2^{(i)} \end{pmatrix}$, with $\psi_2|_{I_i}$ having finite order, where D_i , for $i = 1, \dots, t$ are decomposition groups at the places v_1, \dots, v_t , of F dividing l , and $I_i \subset D_i$ are inertia groups,
6. $\bar{\rho}$ is irreducible and $\bar{\rho}|_{D_i} \sim \begin{pmatrix} \chi_1^{(i)} & * \\ 0 & \chi_2^{(i)} \end{pmatrix}$, $i = 1, \dots, t$, with $\chi_1^{(i)} \neq \chi_2^{(i)}$ and $\chi_2^{(i)} = \psi_2^{(i)} \pmod{\lambda}$,
7. there exists an automorphic representation π_0 of $GL_2(\mathbb{A}_F)$ and a prime λ_0 of the field of coefficients of π_0 above l such that $\bar{\rho}_{\pi_0, \lambda_0} \sim \bar{\rho}$ and $\rho_{\pi_0, \lambda_0}|_{D_i} \sim \begin{pmatrix} \phi_1^{(i)} & * \\ 0 & \phi_2^{(i)} \end{pmatrix}$, $i = 1, \dots, t$, and $\chi_2^{(i)} = \phi_2^{(i)} \pmod{\lambda}$.

Then we have $\rho \sim \rho_{\pi, \lambda_1}$ for some automorphic representation π and some prime λ_1 of the field of coefficients of π above l .

We want to show that, for our chosen prime l and F' , the representation $\rho_{E_i, l}|_{\Gamma_{F'}}$ satisfies the hypotheses of Proposition 3.3. Since $\bar{\rho}_{E_i, l}(\Gamma_F)$ contains $SL_2(\mathbb{F}_l)$, we know from Proposition 3.5 of [V] that $\bar{\rho}_{E_i, l}(\Gamma_{F'})$ contains $SL_2(\mathbb{F}_l)$, and thus the representation $\bar{\rho}_{E_i, l}|_{\Gamma_{F'}}$ is irreducible. Also since the character χ_{iv} that appears in condition 2 of Proposition 3.1 is unramified and the mod l character ϵ_l is ramified, the entire condition 6 is satisfied. Since $\bar{\rho}$ is irreducible, we get that condition 1 is trivially satisfied. Also the conditions 2, 3, 4 are satisfied from the basic properties of the representation $\rho_{E_i, l}|_{\Gamma_{F'}}$. Condition 5 is satisfied from the ordinarity of the representation $\rho_{E_i, l}|_{\Gamma_{F'}}$, and condition 7 is satisfied from the conclusion of Proposition 3.1. Hence we finished the proof of Theorem 1.1. \square

4 Some applications to potential modularity

As an application to Theorem 1.1 we prove the following theorem (we don't try to state the most general results and of course there are other applications):

Theorem 4.1. *1) Let $r \leq 4$ be a positive integer. Let F be a totally real number field and for $j = 1, \dots, r$, let E_j/F be an elliptic curve. If ψ is a finite order character of Γ_F , then the function*

$$L(s, \rho_{E_1} \otimes \dots \otimes \rho_{E_r} \otimes \psi)$$

has a meromorphic continuation to the entire complex plane, is holomorphic and does not vanish for $\text{Re } s > 1 + r/2$, and satisfies a functional equation $s \leftrightarrow 1 + r - s$. Also if $U(E_1 \times \dots \times E_r, M)$ and $V(E_1 \times \dots \times E_r, M)$ denote the space of algebraic cycles and the space of Tate cycles of $E_1 \times \dots \times E_r$ defined over a finite extension M/F , then the Tate conjecture for $(E_1 \times \dots \times E_r)_F$ is

true, i.e. we have for any finite extension M/F that

$$U(E_1 \times \dots \times E_r, M) = V(E_1 \times \dots \times E_r, M),$$

and for any totally real finite extension M/F that

$$\dim V(E_1 \times \dots \times E_r, M) = -\text{ord}_{s=1+r/2} L(s, \rho_{E_1}|_{\Gamma_M} \otimes \dots \otimes \rho_{E_r}|_{\Gamma_M}),$$

(when $r = 1$ or $r = 3$ all these 3 numbers are equal to 0; the first two by definition).

2) Let n and m be positive integers ≤ 4 . Let E_1 and E_2 be elliptic curves defined over a totally real number field F . If ψ is a finite order character of Γ_F , then the function

$$L(s, \text{Sym}^n \rho_{E_1} \otimes \text{Sym}^m \rho_{E_2} \otimes \psi)$$

has a meromorphic continuation to the entire complex plane, is holomorphic and does not vanish for $\text{Re } s > 1 + m/2 + n/2$, and satisfies a functional equation $s \leftrightarrow 1 + m + n - s$.

Proof: 1) From Theorem 1.1 we know that there exists a totally real finite Galois extension F' of F such that for $j = 1, \dots, r$, we have $\rho_{E_j}|_{\Gamma_{F'}} \sim \rho_{\pi'_j}$ for an automorphic representation π'_j of $\text{GL}(2)/F'$ such that $\rho_{E_j}|_{\Gamma_{F'}} \sim \rho_{\pi'_j}$.

By Brauer's theorem (see Theorems 16 and 19 of [S]), we can find some subfields $F_i \subseteq F'$ such that $\text{Gal}(F'/F_i)$ are solvable, some characters $\psi_i : \text{Gal}(F'/F_i) \rightarrow \bar{\mathbb{Q}}^\times$ and some integers n_i , such that the trivial representation

$$1 : \text{Gal}(F'/F) \rightarrow \bar{\mathbb{Q}}^\times,$$

can be written as $1 = \sum_{i=1}^u n_i \text{Ind}_{\text{Gal}(F'/F_i)}^{\text{Gal}(F'/F)} \psi_i$ (a virtual sum). Then

$$\begin{aligned} L(s, \rho_{E_1} \otimes \dots \otimes \rho_{E_r} \otimes \psi) &= \prod_{i=1}^u L(s, (\rho_{E_1} \otimes \dots \otimes \rho_{E_r} \otimes \psi) \otimes \text{Ind}_{\Gamma_{F_i}}^{\Gamma_{F'}} \psi_i)^{n_i} \\ &= \prod_{i=1}^u L(s, \text{Ind}_{\Gamma_{F_i}}^{\Gamma_{F'}} ((\rho_{E_1} \otimes \dots \otimes \rho_{E_r} \otimes \psi)|_{\Gamma_{F_i}} \otimes \psi_i))^{n_i} \\ &= \prod_{i=1}^u L(s, (\rho_{E_1} \otimes \dots \otimes \rho_{E_r} \otimes \psi)|_{\Gamma_{F_i}} \otimes \psi_i)^{n_i}. \end{aligned}$$

Since $\rho_{E_j}|_{\Gamma_{F'}}$ is modular and $\text{Gal}(F'/F_i)$ is solvable, from Langlands base change for solvable extensions ([L]), one can deduce easily that the representation $\rho_{E_j}|_{\Gamma_{F_i}}$ is modular, and thus there exists an automorphic representation π_{j_i} such that $\rho_{E_j}|_{\Gamma_{F_i}} \sim \rho_{\pi_{j_i}}$. We obtain:

$$L(s, \rho_{E_1} \otimes \dots \otimes \rho_{E_r} \otimes \psi) = \prod_{i=1}^u L(s, \rho_{\pi_{1i}} \otimes \dots \otimes \rho_{\pi_{ri}} \otimes (\psi|_{\Gamma_{F_i}} \otimes \psi_i))^{n_i}. \quad (4.1)$$

Hence the function $L(s, \rho_{E_1} \otimes \dots \otimes \rho_{E_r} \otimes \psi)$ has a meromorphic continuation to the entire complex plane, is holomorphic and does not vanish for $\text{Re } s > 1 + r/2$, and satisfies a functional equation $s \leftrightarrow 1 + r - s$ because the functions $L(s, \rho_{\pi_{1i}} \otimes \dots \otimes \rho_{\pi_{ri}} \otimes (\psi|_{\Gamma_{F_i}} \otimes \psi_i))$ have meromorphic continuations to the entire complex plane, are holomorphic and do not vanish for $\text{Re } s > 1 + r/2$, and satisfy functional equations $s \leftrightarrow 1 + r - s$ (this is because from Theorem M of [R], we know that for π_1 and π_2 automorphic representations of $\text{GL}(2)/M$, where M is a number field, the representation $\pi_1 \otimes \pi_2$ is automorphic, and also that for Π_1 and Π_2 unitary automorphic representations of $\text{GL}(t_1)/M$ and $\text{GL}(t_2)/M$ respectively, the function $L(s, \Pi_1 \times \Pi_2)$ (see [JS]) has a meromorphic continuation to the entire complex plane, is holomorphic and does not vanish for $\text{Re } s > 1$, and satisfies a functional equation $s \leftrightarrow 1 - s$).

The Tate conjecture for $(E_1 \times \dots \times E_r)/F$ could be deduced, by using the potential modularity, in a similar way as Theorem 4.5.1 of [R].

2) Could be proved in the same way as 1) by using the fact that for t a positive integer ≤ 4 and for π an automorphic representation of $\text{GL}(2)/M$, where M is a number field, we know (see [JG], [KS], [K]) that $\text{Sym}^t \pi$ is an automorphic representation of $\text{GL}(t+1)$. \square

References

- [BCDT] C.Breuil, B.Conrad, F.Diamond, R.Taylor, *On the modularity of elliptic curves over \mathbb{Q} : wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), 843-939.
- [E] N.D.Elkies, *Supersingular primes for elliptic curves over real number fields*, Compositio Math., tome 72, nr. 2 (1989), 165-172.
- [G] S.S. Gelbart, *Automorphic forms on adèle groups*, Ann. of Mathematics Studies, Princeton University Press, 1975.
- [HSBT] M.Harris, N.Shepherd-Barron, R.Taylor, *A family of Calabi-Yau varieties and potential automorphy*, to appear in Ann. of Math.
- [JG] H.Jacquet, S.Gelbart, *A relation between automorphic representations of $GL(2)$ and $GL(3)$* , Ann. Sci. École Norm. Sup. 11(1979), 471-542.
- [JS] H.Jacquet, J.A.Shalika, *Euler products and the classification of automorphic forms I and II*, Amer. J. of Math. 103(1981), 499-558 and 777-815.
- [K] H.Kim, *Functoriality for the exterior square of GL_4 and the symmetric fourth of GL_2* , J. of the Amer. Math. Society, vol. 16, nr. 1, 139-183.
- [KLR] C.Khare, M.Larsen, R.Ramakrishna, *Transcendental l -adic Galois representations*, Math. Res. Lett. 12 (2005), no. 5-6, 685-699.
- [KS] H.Kim, F.Shahidi, *Functorial products for $GL_2 \times GL_3$ and the symmetric cube for GL_2* , Ann. of Math., 155 (2002), 837-893.

- [L] R.P.Langlands, *Base change for GL_2* , Ann. of Math. Studies 96, Princeton University Press, 1980.
- [R] D.Ramakrishnan, *Modularity of the Rankin-Selberg L -series, and multiplicity one for $SL(2)$* , Ann. of Math., 152(2000), 45-111.
- [S] J-P.Serre, *Linear representations of finite groups*, Springer 1977.
- [S1] J-P.Serre, *Abelian l -adic representations and elliptic curves*. Revised preprint of the 1968 edition, A.K Peters, Ltd., Wellesley, MA, 1998.
- [SW] C.Skinner and A.Wiles, *Nearly ordinary deformations of irreducible residual representations*, Ann. Fac. Sci. Toulouse MATH.(6) 10(2001),no. 1, 185-215.
- [T] R.Taylor, *On Galois representations associated to Hilbert modular forms*, Invent. Math., 98, 1989, 265-280.
- [T1] R.Taylor, *Remarks on a conjecture of Fontaine and Mazur*, Journal of the Institute of Mathematics of Jussieu 1 (2002), 125-143.
- [T2] R.Taylor, *Automorphy for some l -adic lifts of automorphic mod l representations. II*, Pub. Math. IHES 108 (2008), 183-239.
- [V] C.Virdol, *Zeta functions of twisted modular curves*, J. Aust. Math. Soc. 80 (2006), 89-103.
- [W] A.Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Mathematics 141, (1995), 443-551.