Functiones et Approximatio
45.2 (2011), 265–269

ARBITRARY POTENTIAL MODULARITY FOR ELLIPTIC CURVES OVER TOTALLY REAL NUMBER FIELDS

Cristian Virdol

Abstract: In this paper we prove the arbitrary potential modularity for an elliptic curve defined over a totally real number field.

Keywords: elliptic curves, potential modularity.

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 $\Gamma_F := \mathrm{Gal}(\bar{F}/F)$, 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 $\mathrm{GL}(2)/F$ (see §2 below for details). This conjecture was proved when $F = \mathbb{Q}$ (see [BCDT], [W]).

In this paper we prove the following result:

Theorem 1.1. *Let E be an elliptic curve defined over a totally real number field F. Then there exist a totally real number field F'', which contains F, and rational primes l and p that are totally split in F'' such that $E_{/F'}$ is modular for any totally real number field F' which contains F'' and has the property that l and p split completely in F'.*

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 $T_l(E)$.

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

$$\rho_\pi := \rho_{\pi,\lambda} : \Gamma_F \to \mathrm{GL}_2(O_\lambda) \hookrightarrow \mathrm{GL}_2(\overline{\mathbb{Q}}_l),$$

2010 Mathematics Subject Classification: primary: 11F41, 11F80, 11R80

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 $\rho_E \sim \rho_\pi$.

3. The proof of Theorem 1.1

Let E be an elliptic curve defined over a totally real number field F. When E has CM Theorem 1.1 is well known (and the base change is arbitrary). Hence we assume from now on that the curve E has no CM.

We know the following result (see Theorem 1.6 of [T1] and its proof):

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 in which l splits completely and $\rho : \Gamma_F \to GL_2(k)$ a continuous representation. Suppose that the following conditions hold:*

1. *the representation ρ is irreducible,*
2. *for every place v of F above l we have*

$$\rho|_{G_v} \sim \begin{pmatrix} \epsilon_l \chi_v^{-1} & * \\ 0 & \chi_v \end{pmatrix}$$

   where G_v is the decomposition group above v, and χ_v is an unramified character,
3. *for every complex conjugation c, we have $det\rho(c) = -1$.*

Then there exist a rational prime p and a finite totally real extension F''/F in which every prime of F above l and p splits completely, such that: for all totally real number fields F' which contain F'' and in which l and p split completely, there exists a cuspidal automorphic representation π' of $GL(2)/F'$ and a place λ' of the minimal field of rationality of π' above l such that $\rho|_{\Gamma_{F'}} \sim \bar{\rho}_{\pi',\lambda'}$, where $\rho_{\pi',\lambda'} : \Gamma_{F'} \to GL_2(M_{\lambda'})$ is the representation associated to π', the field M is the minimal field of rationality of π', and $\bar{\rho}_{\pi',\lambda'}$ is the reduction of $\rho_{\pi',\lambda'}$ modulo λ'.

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

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

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

We want to prove that the hypotheses of the Proposition 3.1 are satisfied for some rational prime $l > 3$ and the representation $\bar{\rho}_{E,l}$. From [S], because E does not have CM, we know that $\rho_{E,l}(\Gamma_F)$ contains $\mathrm{SL}_2(\mathbb{Z}_l)$ for almost all l, and hence $\bar{\rho}_{E,l}(\Gamma_F)$ contains $\mathrm{SL}_2(\mathbb{F}_l)$ for almost all l, and thus the representation

$\bar{\rho}_{E,l}$ is irreducible for almost all l. Hence we can choose the prime l which splits completely in F such that the representation $\bar{\rho}_{E,l}$ is irreducible.

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

We prove the following result:

Theorem 3.2. *Let E be a non-CM elliptic curve defined over a totally real number field F. Then there exists an infinite set of rational primes l which split completely in F such that E is ordinary at v for each place $v|l$ of F.*

Proof. Let $l \geqslant 5$ be a rational prime which is completely split in F such that if v is a place of F above l, then E has good reduction at v. 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 $|a_v| \leqslant 2\sqrt{k_v} = 2\sqrt{l}$. Hence if E is not ordinary at v, i.e. if $l \mid a_v$, we get that $a_v = 0$, i.e. E is supersingular at v. But from Theorem 2.4 of [KLR], we know that the set of supersingular primes of E over F is of density 0, and hence, because from Dirichlet density theorem we get that the set of rational primes $l \geqslant 5$ which split completely in F has positive density, we deduce that the set of rational primes l such that E is ordinary at v for each place $v|l$ of F has positive density. Thus we conclude Theorem 3.2. ■

We have that $\det\rho_{E,l} = \epsilon_l$ and because E does not have CM, from Theorem 3.2 we know that the representation $\rho_{E,l}$ is ordinary (in the sense of Theorem 3.2) at an infinite set of primes l, and hence for every place v of F above l we have

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

where χ_v is an unramified character. Thus one could choose the prime l such that the representation $\bar{\rho}_{E,l}$ 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 representation $\bar{\rho}_{E,l}$, we could find a totally real extension F''/F and a rational prime p 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 $\rho : Gal(\overline{F'}/F') \to GL_2(\overline{\mathbb{Q}}_l)$ 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 $\psi_2^{(i)}|_{I_i}$ having finite order, where D_i, for $i = 1, \ldots, t$ are decomposition groups at the places $v_1, \ldots, v_t$ of F dividing l, and $I_i \subset D_i$ are inertia groups,*

6. $\bar{\rho}$ *is irreducible and* $\bar{\rho}|_{D_i} \sim \begin{pmatrix} \chi_1^{(i)} & * \\ 0 & \chi_2^{(i)} \end{pmatrix}$, $i = 1, \ldots, t$, *with* $\chi_1^{(i)} \neq \chi_2^{(i)}$ *and* $\chi_2^{(i)} = \psi_2^{(i)} \mod \lambda$,
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* $\rho_{\pi_0,\lambda_0}|_{D_i} \sim \begin{pmatrix} \phi_1^{(i)} & * \\ 0 & \phi_2^{(i)} \end{pmatrix}$, $i = 1, \ldots, t$, *and* $\chi_2^{(i)} = \phi_2^{(i)} \mod \lambda$.

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 choosen prime l and F' as in Proposition 3.1, the representation $\rho_{E,l}|_{\Gamma_{F'}}$ satisfies the hypotheses of Proposition 3.3. Since $\bar{\rho}_{E,l}(\Gamma_F)$ contains $\mathrm{SL}_2(\mathbb{F}_l)$, we know from Proposition 3.5 of [V] that $\bar{\rho}_{E,l}(\Gamma_{F'})$ contains $\mathrm{SL}_2(\mathbb{F}_l)$, and thus the representation $\bar{\rho}_{E,l}|_{\Gamma_{F'}}$ is irreducible. Also since the character χ_v 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 $\rho_{E,l}|_{\Gamma_{F'}}$. Condition 5 is satisfied from the ordinarity of the representation $\rho_{E,l}|_{\Gamma_{F'}}$, and condition 7 is satisfied from the conclusion of Proposition 3.1. Hence we finished the proof of Theorem 1.1. ■

References

[BCDT] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.

[KLR] C. Khare, M. Larsen and R. Ramakrishna, *Transcendental* l*-adic Galois representations*, Math. Res. Lett. **12** (2005), no. 5-6, 685–699.

[L] R. P. Langlands, *Base change for* GL_2, Ann. of Math. Studies 96, Princeton University Press, 1980.

[S] 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.

[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.

Addresses: Cristian Virdol: Department of Mathematics for Industry, Kyushu University.
E-mail: virdol@imi.kyushu-u.ac.jp
Received: 10 August 2010; **revised:** 14 August 2010