

On the Birch and Swinnerton-Dyer conjecture for elliptic curves over totally real number fields

Cristian Virdol
Department of Mathematics
Columbia University

July 17, 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]). The Birch and Swinnerton-Dyer conjecture says in particular that (more precisely, for details see [M] and also §2 below):

Conjecture 1.1. *If E is an elliptic curve defined over a totally real number field F , and ψ is a finite order character of Γ_F , then the function $L(s, \rho_E \otimes \psi)$ has a meromorphic continuation to the entire complex plane, satisfies a functional equation $s \leftrightarrow 2 - s$, and*

$$\text{rank}_{\mathbb{Z}} E(\psi) = \text{ord}_{s=1} L(s, \rho_E \otimes \psi),$$

where $E(\psi)$ is the ψ -eigensubspace of $E(\bar{F}) \otimes \mathbb{C}$.

Conjecture 1.2. *If E is an elliptic curve defined over a totally real number field F , then the Tate-Shafarevich group $\text{III}(E/F)$ of E over F is finite.*

In this paper we prove the following results:

Theorem 1.3. *The first part of conjecture 1.1 regarding the meromorphic continuation and functional equation of $L(s, \rho_E \otimes \psi)$ is true. Also if we assume that conjecture 1.1 is true for all totally real number fields and all modular elliptic curves, then conjecture 1.1 is true.*

Theorem 1.4. *Assume that conjecture 1.2 is true for all totally real number fields and all modular elliptic curves. Then conjecture 1.2 is true.*

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

2 L-functions and Mordell-Weil groups

In this section we study L-functions and Mordell-Weil groups twisted by characters (we follow closely [M]).

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).

We know the following Mordell-Weil theorem:

Theorem 2.1. (*Mordell-Weil*) *The group $E(F)$ is finitely generated. Thus one has an isomorphism*

$$E(F) \sim \mathbb{Z}^r \oplus E(F)_{\text{tor}}$$

where r is a nonnegative integer.

The integer r is called the rank of E/F . We denote by $\text{rank}_{\mathbb{Z}} E(F) := r$. The Birch and Swinnerton-Dyer conjecture for E/F predicts that:

Conjecture 2.2. *The function $L(s, \rho_E)$ has a meromorphic continuation to the entire complex plane and satisfies a functional equation $s \leftrightarrow 2 - s$, and*

$$\text{rank}_{\mathbb{Z}} E(F) = \text{ord}_{s=1} L(s, \rho_E).$$

Now let L be some finite abelian extension of F . By the Mordell-Weil theorem, $E(L)$ is finitely generated and we have the following decomposition

$$E(L) \otimes \mathbb{C} = \bigoplus E(\psi)$$

where $\psi : \text{Gal}(L/F) \rightarrow \mathbb{C}^\times$ ranges through all characters, and $E(\psi)$ is the ψ -eigensubspace in $E(L) \otimes \mathbb{C}$ defined by

$$E(\psi) := \{P \in E(L) \otimes \mathbb{C} \text{ such that } \sigma P = \psi^{-1}(\sigma)P \text{ for all } \sigma \in \text{Gal}(L/F)\}.$$

On the other hand, we have the decomposition

$$L(s, \rho_E|_{\Gamma_L}) = \prod_{\psi} L(s, \rho_E \otimes \psi).$$

Hence the Birch and Swinnerton-Dyer conjecture for E/L can be refined as follows:

Conjecture 2.3. *For any finite order character ψ of Γ_F , the function $L(s, \rho_E \otimes \psi)$ has a meromorphic continuation to the entire complex plane and satisfies a functional equation $s \leftrightarrow 2 - s$, and*

$$\text{rank}_{\mathbb{Z}} E(\psi) = \text{ord}_{s=1} L(s, \rho_E \otimes \psi).$$

Let

$$\text{III}(E/F) := \ker(H^1(F, E) \rightarrow \prod_v H^1(F_v, E)),$$

where v runs over all places of F and F_v is the completion of F at v , be the Tate-Shafarevich group of E over F . Then the Birch and Swinnerton-Dyer conjecture for E/F predicts that:

Conjecture 2.4. $\text{III}(E/F)$ is finite.

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

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

which is unramified outside the primes dividing $\mathfrak{n}l$. Here O is the coefficients ring of π and λ is a prime ideal of O above some prime number l , \mathfrak{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 $\text{GL}(2)/F$ 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 Potential modularity for elliptic curves

In this section we prove the following theorem (when E has multiplicative reduction at some place, this result is a particular case of theorem B of [T2]):

Theorem 3.1. *Let E be an elliptic curve defined over a totally real number field F . Then there exists a totally real finite extension F' of F , such that F' is Galois over F , and the elliptic curve E/F' is modular.*

When the curve E has CM theorem 3.1 is well known. Hence we assume from now on that the curve E has no CM.

We know the following result (theorem 1.6 of [T1]):

Proposition 3.2. *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 $\rho : \Gamma_F \rightarrow \text{GL}_2(k)$ 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 exists a finite Galois totally real extension F'/F in which every prime of F above l splits completely, 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 $\rho_{\pi',\lambda'} : \Gamma_{F'} \rightarrow GL_2(M_{\lambda'})$ 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 hypothesis of the proposition 3.2 are satisfied for some rational prime $l > 3$ and the representation $\bar{\rho}_{E,l}$. From [S1], because E does not have CM, we know that $\rho_{E,l}(\Gamma_F)$ contains $SL_2(\mathbb{Z}_l)$ for almost all l , and hence $\bar{\rho}_{E,l}(\Gamma_F)$ contains $SL_2(\mathbb{F}_l)$ 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 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 3.3. *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 such that E is ordinary at v for each place $v|l$ of F .*

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 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 $|a_v| \leq 2\sqrt{|k_v|} = 2\sqrt{l}$. 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 The [E] (see the remark after the main theorem of [E]), 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 $l \geq 5$ 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 3.3. \square

We have that $\det\rho_{E,l} = \epsilon_l$ and because E does not have CM, from theorem 3.3 we know that the representation $\rho_{E,l}$ is ordinary (in the sense of theorem 3.3) 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 3.2. Also the condition 3 of proposition 3.2 is satisfied. Hence, for some rational prime l and the representation $\bar{\rho}_{E,l}$, we could find a finite Galois extension F'/F as in the conclusion of proposition 3.2.

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

Proposition 3.4. *Let F' be a totally real number field and let $\rho : \text{Gal}(\bar{F}'/F') \rightarrow \text{GL}_2(\bar{\mathbb{Q}}_l)$ 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 $\text{GL}_2(\mathbb{A}_F)$ 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 $\rho_{E,l}|_{\Gamma_{F'}}$ satisfies the hypothesis of proposition 3.4. Since $\bar{\rho}_{E,l}(\Gamma_F)$ contains $\text{SL}_2(\mathbb{F}_l)$, we know from proposition 3.5 of [V] that $\bar{\rho}_{E,l}(\Gamma_{F'})$ contains $\text{SL}_2(\mathbb{F}_l)$, and thus the representation $\bar{\rho}_{E,l}|_{\Gamma_{F'}}$ is irreducible. All the other conditions of proposition 3.4 are satisfied and we conclude the proof of theorem 3.1. \square

4 The proof of theorem 1.3

We fix an elliptic curve E defined over a totally real number field F and a finite order character ψ of Γ_F . Then from theorem 3.1 we know that there exists a totally real finite Galois extension F' of F and an automorphic representation π' of $\text{GL}(2)/F'$ such that $\rho_E|_{\Gamma_{F'}} \sim \rho_{\pi'}$.

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

$$\begin{aligned} L(s, \rho_E \otimes \psi) &= \prod_{i=1}^u L(s, (\rho_E \otimes \psi) \otimes \text{Ind}_{\Gamma_{F_i}}^{\Gamma_F} \psi_i)^{n_i} \\ &= \prod_{i=1}^u L(s, \text{Ind}_{\Gamma_{F_i}}^{\Gamma_F} ((\rho_E \otimes \psi)|_{\Gamma_{F_i}} \otimes \psi_i))^{n_i} = \prod_{i=1}^u L(s, (\rho_E \otimes \psi)|_{\Gamma_{F_i}} \otimes \psi_i)^{n_i}. \end{aligned}$$

Since $\rho_E|_{\Gamma_{F'}}$ 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 $\rho_E|_{\Gamma_{F_i}}$ is modular, and thus there exists an automorphic representation π_i such that $\rho_E|_{\Gamma_{F_i}} \sim \rho_{\pi_i}$. We obtain:

$$L(s, \rho_E \otimes \psi) = \prod_{i=1}^u L(s, \rho_{\pi_i} \otimes (\psi|_{\Gamma_{F_i}} \otimes \psi_i))^{n_i}. \quad (4.1)$$

Hence the function $L(s, \rho_E \otimes \psi)$ has a meromorphic continuation to the entire complex plane and satisfies a functional equation $s \leftrightarrow 2-s$ because the functions $L(s, \rho_{\pi_i} \otimes (\psi|_{\Gamma_{F_i}} \otimes \psi_i))$ have meromorphic continuations to the entire complex plane and satisfy functional equations $s \leftrightarrow 2-s$.

Assume now that conjecture 1.1 is true for modular elliptic curves. Since the elliptic curve E/F_i is modular we get that

$$\text{rank}_{\mathbb{Z}} E(\psi|_{\Gamma_{F_i}} \otimes \psi_i) = \text{ord}_{s=1} L(s, \rho_{\pi_i} \otimes (\psi|_{\Gamma_{F_i}} \otimes \psi_i)). \quad (4.2)$$

But obviously

$$\text{rank}_{\mathbb{Z}} E(\psi) = \sum_{i=1}^u n_i \text{rank}_{\mathbb{Z}} E(\psi|_{\Gamma_{F_i}} \otimes \psi_i). \quad (4.3)$$

Hence from (4.1), (4.2) and (4.3) we deduce that

$$\text{rank}_{\mathbb{Z}} E(\psi) = \text{ord}_{s=1} L(s, \rho_E \otimes \psi),$$

and we conclude the proof of theorem 1.3. \square

5 The proof of theorem 1.4

We know the following result (theorem 6 of [KP]):

Proposition 5.1. *Let F' be a finite Galois extension field of a number field F . Let E be an elliptic curve over F . If $\text{III}(E/F')$ is finite, then so is $\text{III}(E/F)$.*

We fix an elliptic curve E defined over a totally real number field F . Then from theorem 3.1 we know that there exists a totally real finite Galois extension F' of F such that the elliptic curve E/F' is modular. Now trivially, from proposition 5.1, we deduce theorem 1.4. \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.
- [KP] D.Kim, H.Park, *Relations among Shafarevich-Tate groups*, Honam Math. J. 21 (1999), no.1, 35-42.
- [L] R.P.Langlands, *Base change for GL_2* , Ann. of Math. Studies 96, Princeton University Press, 1980.
- [M] B.Mazur, *Modular curves and arithmetic*, Proceedings of International Congress of Mathematicians, Warsaw (1983), 185-211.
- [E] N.D.Elkies, *Supersingular primes for elliptic curves over real number fields*, Compositio Math., tome 72, nr. 2 (1989), 165-172.
- [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.