

# On Mazur's conjecture for twisted L-functions of elliptic curves over totally real or CM fields

Cristian Virdol  
Department of Mathematics  
Columbia University

October 8, 2009

## 1 Introduction

Let  $E$  be an elliptic curve defined over a number field  $F$ , and let  $\Sigma$  be a finite set of finite places of  $F$ . Let  $L(s, E, \psi)$  be the  $L$ -function of  $E$  twisted by a finite order Hecke character  $\psi$  of  $F$ . It is conjectured that  $L(s, E, \psi)$  has a meromorphic continuation to the entire complex plane and satisfies a functional equation  $s \leftrightarrow 2 - s$ . Then one can define the so called *minimal order of vanishing at  $s = 1$*  of  $L(s, E, \psi)$ , denoted by  $m(E, \psi)$  (see §2 for the definition). It is conjectured that (see [M]):

**Conjecture 1.1.** (*Generalized Mazur Conjecture*) *For all but finitely many characters  $\psi$  unramified outside of  $\Sigma$ ,*

$$\text{ord}_{s=1} L(s, E, \psi) = m(E, \psi).$$

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  $\Gamma_F$  associated to some automorphic representation  $\pi$  of  $\text{GL}(2)/F$  (see §3 below for details). This conjecture was proved when  $F = \mathbb{Q}$  (see [BCDT], [W]).

In this paper we prove the following results:

**Theorem 1.2.** *Let  $E$  be an elliptic curve defined over a totally real number field  $F$ . Then for any finite order Hecke character  $\psi$  of  $F$ , the function  $L(s, E, \psi)$  has a meromorphic continuation to the entire complex plane and satisfies a functional equation  $s \leftrightarrow 2 - s$ . Moreover, if we assume that conjecture 1.1 is true for all modular elliptic curves and all totally real number fields, then conjecture 1.1 is true for all elliptic curves and all totally real number fields.*

**Theorem 1.3.** *Let  $E$  be a quadratic base change to a CM-field  $F$  of an elliptic curve defined over a totally real number field. Then for any finite order Hecke*

character  $\psi$  of  $F$ , the function  $L(s, E, \psi)$  has a meromorphic continuation to the entire complex plane and satisfies a functional equation  $s \leftrightarrow 2 - s$ . Moreover, if we assume that conjecture 1.1 is true for all CM-fields and quadratic base changes of modular elliptic curves, then conjecture 1.1 is true for all CM-fields and quadratic base changes of elliptic curves.

## 2 The minimal order of vanishing at $s = 1$

Let  $E$  be an elliptic curve over a number field  $F$ . For a finite order Hecke character  $\psi$  of  $F$ , let  $L(s, E, \psi)$  be the  $L$ -function of  $E$  twisted by  $\psi$  (see [Z]). 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  $\Gamma_F := \text{Gal}(\bar{F}/F)$  on  $T_l(E)$  (by fixing an isomorphism  $i : \mathbb{Q}_l \rightarrow \mathbb{C}$  we can regard  $\rho_E$  as a complex-valued representation). Then  $L(s, E, \psi) = L(s, \rho_E \otimes \psi)$ .

We define now the so called *minimal order of vanishing at  $s = 1$*  of  $L(s, E, \psi)$ . It is obvious that  $L(s, E, \psi) = L(s, M)$  where

$$M := \text{Ind}_{\Gamma_F}^{\Gamma_{\mathbb{Q}}}(T_l(E)(\psi)).$$

Let  $\oplus M_i$  be the semi-simplification of  $M$  as  $\Gamma_{\mathbb{Q}}$ -module, where  $M_i$  are irreducible. Then we have the decomposition

$$L(s, E, \psi) = L(s, M) = \prod_i L(s, M_i),$$

and each  $M_i$  has a conjectural functional equation

$$L(s, M_i) = \epsilon(s, M_i) L(2 - s, M_i^{\vee})$$

where

$$M_i^{\vee} = \text{Hom}(M_i, \mathbb{Z}_l(1)).$$

We define the minimal order of vanishing at  $s = 1$  of  $L(s, E, \psi)$  to be

$$m(E, \psi) := \#\{i : M_i \cong M_i^{\vee}, \epsilon(1, M_i) = -1\}.$$

Then obviously

$$\text{ord}_{s=1} L(s, E, \psi) \geq m(E, \psi).$$

One expects  $\text{ord}_{s=1} L(s, E, \psi)$  to be as small as possible most of the times (see [M]):

**Conjecture 2.1.** (*Generalized Mazur Conjecture*) *Let  $\Sigma$  be a finite set of finite places of  $F$ . Then for all but finitely many characters  $\psi$  unramified outside of  $\Sigma$ ,*

$$\text{ord}_{s=1} L(s, E, \psi) = m(E, \psi).$$

For  $F = \mathbb{Q}$ , we have that  $m(E, \psi) = 0$  unless  $\psi$  is quadratic character and the sign of the functional equation of  $L(s, E, \psi)$  is equal to  $-1$ . From [R] and [R1] we know that for  $F = \mathbb{Q}$  the conjecture 2.1 is true:

**Theorem 2.2.** (*Rohrlich*) Assume that  $F = \mathbb{Q}$ . For all but finitely many  $\psi$  unramified outside of  $\Sigma$ ,

$$L(1, E, \psi) \neq 0.$$

Also when  $F$  is a quadratic imaginary number field we know that conjecture 2.1 is true in many cases (this is theorem 7.12 of [Z]):

**Theorem 2.3.** Let  $E$  be a non-CM elliptic curve over  $\mathbb{Q}$ , and let  $F$  be an imaginary quadratic number field. Assume that for each rational prime  $p$  dividing the conductor  $N$  of  $E$ , either  $p$  is split in  $F$ , or  $p$  is inert in  $F$  and  $\text{ord}_p(N) = 1$ . Also assume that  $\Sigma$  does not contain any prime dividing  $N$  and the discriminant  $d$  of  $F/\mathbb{Q}$ .

Then for all but finitely many ring class characters  $\psi$  unramified outside of  $\Sigma$ ,

$$\text{ord}_{s=1} L(s, E/F, \psi) \leq 1.$$

### 3 Potential modularity

Consider  $F$  a totally real number field. If  $\pi$  is an automorphic representation (discrete series at infinity) of weight 2 of  $\text{GL}(2)/F$ , then there exists ([T]) a  $\lambda$ -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  $\mathfrak{nl}$ . Here  $O$  is the coefficients ring of  $\pi$  and  $\lambda$  is a prime ideal of  $O$  above some prime number  $l$ ,  $\mathfrak{n}$  is the level of  $\pi$ .

We say that an elliptic curve  $E$  defined over a totally real number field  $F$  is modular if there exists an automorphic representation  $\pi$  of weight 2 of  $\text{GL}(2)/F$  such that  $\rho_E \sim \rho_\pi$ .

We know the following result (theorem 3.1 of [V]):

**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.

### 4 The proof of theorems 1.2 and 1.3

We prove first theorem 1.2. Thus we fix an elliptic curve  $E$  defined over a totally real number field  $F$ , a finite set  $\Sigma$  of finite places of  $F$ , and let  $\psi$  be a finite order Hecke character of  $F$  unramified outside  $\Sigma$ . Then from theorem 3.1 we know that there exists a totally real finite Galois extension  $F'$  of  $F$  and an automorphic representation  $\pi'$  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  $\psi_i : \text{Gal}(F'/F_i) \rightarrow \overline{\mathbb{Q}}^\times$  and some integers  $n_i$ , such that the trivial representation

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

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. 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  $L(s, \rho_E|_{\Gamma_{F_i}} \otimes (\psi|_{\Gamma_{F_i}} \otimes \psi_i))$  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

$$\text{ord}_{s=1} L(s, \rho_E|_{\Gamma_{F_i}} \otimes (\psi|_{\Gamma_{F_i}} \otimes \psi_i)) = m(E/F_i, \psi|_{\Gamma_{F_i}} \otimes \psi_i) \quad (4.1)$$

for all but finitely many Hecke characters  $\psi$  unramified outside  $\Sigma$ .

Since  $1 = \sum_{i=1}^u n_i \text{Ind}_{\Gamma_{F_i}}^{\Gamma_F} \psi_i$ , we get that

$$\text{Ind}_{\Gamma_F}^{\Gamma_{\mathbb{Q}}} (T_l(E)(\psi)) = \sum_{i=1}^u n_i \text{Ind}_{\Gamma_{F_i}}^{\Gamma_{\mathbb{Q}}} (T_l(E/F_i)(\psi|_{\Gamma_{F_i}} \otimes \psi_i)),$$

and hence we obtain that

$$m(E, \psi) = \sum_{i=1}^u n_i \cdot m(E/F_i, \psi|_{\Gamma_{F_i}} \otimes \psi_i). \quad (4.2)$$

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

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

for all but finitely many Hecke characters  $\psi$  unramified outside  $\Sigma$ , which concludes the proof of theorem 1.2.

The proof of theorem 1.3 is similar.  $\square$

## 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.

- [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*, Proc. of Int. Cong. of Math., Warsaw (1983), 185-211.
- [R] D.Rohrlich, *On  $L$ -functions of elliptic curves and cyclotomic towers*, Invent. Math. 75 (1984), 404-423.
- [R1] D.Rohrlich, *On  $L$ -functions of elliptic curves and anti-cyclotomic towers*, Invent. Math. 75 (1984), 383-408.
- [S] J-P.Serre, *Linear representations of finite groups*, Springer 1977.
- [T] R.Taylor, *On Galois representations associated to Hilbert modular forms*, Invent. Math., 98, (1989), 265-280.
- [V] C.Virdol, *On the Birch and Swinnerton-Dyer conjecture for elliptic curves over totally real number fields*, to appear in Proc. of the Amer. Math. Society.
- [W] A.Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. 141, (1995), 443-551.
- [Z] S.Zhang, *Elliptic curves,  $L$ -functions, and  $CM$ -points*, in proceedings for Harvard-MIT joint conference on current development in mathematics (2001), 179-219.