Glasgow Math. J. **53** (2011) 207–210. © Glasgow Mathematical Journal Trust 2010.
doi:10.1017/S0017089510000601.

ON MAZUR'S CONJECTURE FOR TWISTED L-FUNCTIONS OF ELLIPTIC CURVES OVER TOTALLY REAL OR CM FIELDS

CRISTIAN VIRDOL
Department of Mathematics, Columbia University, New York, NY 10027, USA
e-mail: virdol@math.columbia.edu

(Received 8 October 2009; accepted 16 June 2010; first published online 25 August 2010)

2010 *Mathematics Subject Classification.* 11F03, 11F41, 11F80, 11R37, 11R42.

1. Introduction. Let E be an elliptic curve defined over a number field F, and let Σ 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 ψ 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 Section 2 for the definition). It is conjectured that (see [**3**]):

CONJECTURE 1.1 (Generalised Mazur Conjecture). For all but finitely many characters ψ unramified outside of Σ,

$$ord_{s=1}L(s, E, \psi) = m(E, \psi).$$

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 $\Gamma_F := \mathrm{Gal}(\bar{F}/F)$, 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 Section 3 for details). This conjecture was proved when $F = \mathbb{Q}$ (see [**1**, **9**]).

In this paper, we prove the following results (the meromorphic continuation of the L-functions is well known and is the consequence of the potential modularity of the elliptic curves defined over totally real number fields, see Section 4 for details):

THEOREM 1.2. *Let E be an elliptic curve defined over a totally real number field F. Then for any finite-order Hecke character ψ 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 ψ 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 ψ of F, let $L(s, E, \psi)$ be the

L-function of E twisted by ψ (see [**11**]). 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 $\Gamma_F := \mathrm{Gal}(\bar{F}/F)$ on $T_l(E)$ (by fixing an isomorphism $i : \bar{\mathbb{Q}}_l \to \mathbb{C}$ we can regard ρ_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

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

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

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

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,

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

One expects $\mathrm{ord}_{s=1}L(s, E, \psi)$ to be as small as possible most of the times (see [**3**]):

Conjecture 2.1 (Generalised Mazur Conjecture). Let Σ be a finite set of finite places of F. Then for all but finitely many characters ψ unramified outside of Σ,

$$ord_{s=1}L(s, E, \psi) = m(E, \psi).$$

For $F = \mathbb{Q}$, we have that $m(E, \psi) = 0$ unless ψ is quadratic character and the sign of the functional equation of $L(s, E, \psi)$ is equal to -1. From [**4**, **5**] 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 ψ unramified outside of Σ,*

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

Also, when F is a quadratic imaginary number field we know that Conjecture 2.1 is true in many cases (this is [**11**, Theorem 7.12]):

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 $\mathrm{ord}_p(N) = 1$. Also assume that Σ does not contain any prime dividing N and the discriminant d of $F/\mathbb{Q}$.*

https://doi.org/10.1017/S0017089510000601 Published online by Cambridge University Press

Then for all but finitely many ring class characters ψ unramified outside of Σ,

$$ord_{s=1} L(s, E_{/F}, \psi) \leq 1.$$

3. Potential modularity. 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 (see [**7**]) a λ-adic representation

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

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 $\rho_E \sim \rho_\pi$.

We know the following result (see [**10**] or [**8**, Theorem 3.1]):

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 Σ of finite places of F, and let ψ be a finite-order Hecke character of F unramified outside Σ. 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 $\mathrm{GL}(2)/F'$ such that $\rho_E|_{\Gamma_{F'}} \sim \rho_{\pi'}$.

By Brauer's theorem (see [**6**, Theorems 16 and 19]), we can find some subfields $F_i \subseteq F'$ such that $\mathrm{Gal}(F'/F_i)$ are solvable, some characters $\psi_i : \mathrm{Gal}(F'/F_i) \to \bar{\mathbb{Q}}^\times$ and some integers n_i, such that the trivial representation

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

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

$$L(s, \rho_E \otimes \psi) = \prod_{i=1}^u L\left(s, (\rho_E \otimes \psi) \otimes \mathrm{Ind}_{\Gamma_{F_i}}^{\Gamma_F} \psi_i\right)^{n_i}$$

$$= \prod_{i=1}^u L\left(s, \mathrm{Ind}_{\Gamma_{F_i}}^{\Gamma_F} ((\rho_E \otimes \psi)|_{\Gamma_{F_i}} \otimes \psi_i)\right)^{n_i} = \prod_{i=1}^u L(s, (\rho_E \otimes \psi)|_{\Gamma_{F_i}} \otimes \psi_i)^{n_i}.$$

Since $\rho_E|_{\Gamma_{F'}}$ is modular and $\mathrm{Gal}(F'/F_i)$ is solvable, from Langlands base change for solvable extensions (see [**2**]), 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 $s \leftrightarrow 2 - s$.

https://doi.org/10.1017/S0017089510000601 Published online by Cambridge University Press

Assume now that Conjecture 1.1 is true for modular elliptic curves. Since the elliptic curve $E_{/F_i}$ is modular we get that

$$\mathrm{ord}_{s=1}L(s, \rho_E|_{\Gamma_{F_i}} \otimes (\psi|_{\Gamma_{F_i}} \otimes \psi_i)) = m(E_{/F_i}, \psi|_{\Gamma_{F_i}} \otimes \psi_i) \tag{4.1}$$

for all but finitely many Hecke characters ψ unramified outside Σ.

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

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

and hence we obtain that

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

(here we use the fact that the minimal order of vanishing, when extended to the Grothendieck group of semisimple continuous representations, transforms in the same way).

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

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

for all but finitely many Hecke characters ψ unramified outside Σ, which concludes the proof of Theorem 1.2.

The proof of Theorem 1.3 is similar. □

REFERENCES

1. 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.

2. R. P. Langlands, *Base change for GL_2*, Annals of Mathematics Studies, vol. 96 (Hsiang Wu-chung, Langlands R. P., Milnor J. W., Stein E. M., Editors) (Princeton University Press, Princeton, NJ, 1980).

3. B. Mazur, Modular curves and arithmetic, in *Proceedings of the international congress of mathematicians* (Warsaw, Poland, 1983), pp. 185–211.

4. D. Rohrlich, On L-functions of elliptic curves and cyclotomic towers, *Invent. Math.* **75** (1984), 404–423.

5. D. Rohrlich, On L-functions of elliptic curves and anti-cyclotomic towers, *Invent. Math.* **75** (1984), 383–408.

6. J.-P. Serre, *Linear representations of finite groups*, Graduate Texts in Mathematics, vol. 42 (Springer-Verlag, New York–Heidelberg, 1977).

7. R. Taylor, On Galois representations associated to Hilbert modular forms, *Invent. Math.* **98** (1989), 265–280.

8. C. Virdol, On the Birch and Swinnerton–Dyer conjecture for elliptic curves over totally real number fields, *Proc. Amer. Math. Soc.* **137** (2009), 4019–4024.

9. A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. Math.* **141** (1995), 443–551.

10. J. P. Wintenberger, Appendix to: On the parity of ranks of Selmer groups IV, *Compos. Math.* **145** (2009), 1351–1359.

11. S. Zhang, Elliptic curves, L-functions, and CM-points, in *Proceedings for Harvard–MIT joint conference on current development in mathematics* (2001), pp. 179–219.

https://doi.org/10.1017/S0017089510000601 Published online by Cambridge University Press