ACTA ARITHMETICA
146.2 (2011)

On the Birch and Swinnerton-Dyer conjecture

by

Cristian Virdol (New York)

1. Introduction. Let E be an elliptic curve defined over a number field F. Then the Birch and Swinnerton-Dyer conjecture for elliptic curves predicts that:

Conjecture 1.1 (Birch and Swinnerton-Dyer conjecture). *The Tate–Shafarevich group* $Ш(E/F)$ *of* E *over* F *is finite, the L-function* $L(s, E/F)$ *of* E *over* F *has a meromorphic continuation to the entire complex plane, satisfies a functional equation* $s \leftrightarrow 2-s$, *and:*

1) *The rank* $r(E/F)$ *of* E *over* F *equals the order of vanishing of the function* $L(s, E/F)$ *at* $s = 1$.
2)
$$\lim_{s\to 1} \frac{L(s, E/F)}{(s-1)^{r(E/F)}} = \frac{\Omega_E \cdot |Ш(E/F)| \cdot R(E/F) \cdot \prod_{\wp|\mathcal{N}} c_\wp(E)}{|E(F)_{\mathrm{tors}}|^2},$$
where Ω_E = *the real period,* $E(F)_{\mathrm{tors}}$ *is the subgroup of torsion points of* $E(F)$, $R(E/F)$ = *the regulator of* $E(F)/E(F)_{\mathrm{tors}}$, $\mathcal{N}$ *is the conductor of* E, *and* $c_\wp(E) = [E(F_\wp) : E_{\mathrm{ns}}(F_\wp)]$ *is the arithmetic component group of* E *at* $\wp$.

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 in particular the following result (see Remark 3.3 for a more general statement regarding the product of several elliptic curves):

2010 *Mathematics Subject Classification*: 11F41, 11F80, 11R42, 11R80, 11G05.
Key words and phrases: elliptic curves, Birch and Swinnerton-Dyer conjecture, potential modularity.

DOI: 10.4064/aa146-2-4

THEOREM 1.2. *Let E be an elliptic curve defined over a totally real number field F. Then the function $L(s, E/F)$ has a meromorphic continuation to the entire complex plane and satisfies a functional equation $s \leftrightarrow 2 - s$. Also if we assume that Conjecture* 1.1 *is true for all totally real number fields and all modular elliptic curves, then it is true for all totally real number fields and all elliptic curves.*

We remark that there exists a statement for the Birch and Swinnerton-Dyer conjecture for a general abelian variety A defined over a number field F, and Theorem 1.2 remains true if one replaces the elliptic curve E/F by $(E_1 \times \cdots \times E_r)/F$, where $r \leq 4$ and $E_1, \ldots, E_r$ are elliptic curves defined over the totally real field F (see Remark 3.3 for the reason). Also for general r, we have a similar result, but when $r > 4$ we do not know the meromorphy and the functional equation of $L(s, (E_1 \times \cdots \times E_r)/F)$.

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

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

which is unramified outside the primes dividing $\mathbf{n}l$. Here O is the coefficient ring of π, λ is a prime ideal of O above some prime number l, and $\mathbf{n}$ 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 (Theorem 1.1 of [V]):

THEOREM 2.1. *Let F be a totally real number field, and for $i = 1, \ldots, r$, 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 $i = 1, \ldots, r$, the elliptic curve E_i/F' is modular.*

3. The proof of Theorem 1.2. We fix an elliptic curve E defined over a totally real number field F. Then from Theorem 2.1 we know that there exists a totally real finite Galois extension F' of F such that E/F' is modular.

From Theorem 15.10 of [CR] we know that there exist some subfields $F_i \subseteq F'$ such that $\mathrm{Gal}(F'/F_i)$ are solvable, and some integers n_i such that the trivial representation

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

can be written as

$$1_F = \sum_{i=1}^{u} n_i \operatorname{Ind}_{\mathrm{Gal}(F'/F_i)}^{\mathrm{Gal}(F'/F)} 1_{F_i} \quad \text{(a virtual sum)}, \tag{3.1}$$

from which we obtain

$$L(s, E/F) = \prod_{i=1}^{u} L(s, E/F_i)^{n_i}.$$

Since E/F' is modular, and $\mathrm{Gal}(F'/F_i)$ is solvable, from Langlands' base change for solvable extensions ([L]) one can deduce easily that E/F_i is modular. Hence the function $L(s, E/F)$ has a meromorphic continuation to the entire complex plane and satisfies a functional equation $s \leftrightarrow 2-s$ because the functions $L(s, E/F_i)$ have meromorphic continuations to the entire complex plane and satisfy functional equations $s \leftrightarrow 2 - s$.

We know (see [M1]):

THEOREM 3.1. *Let L/K be a finite separable extension, and A be an abelian variety defined over L. Then the Birch and Swinnerton-Dyer conjecture holds for A if and only if it holds for* $\mathrm{Res}_{L/K} A$.

We know (Theorem 7.3 of [M2]):

THEOREM 3.2. *Let A and B be two isogeneous abelian varieties defined over a number field L. Then the Birch and Swinnerton-Dyer conjecture holds for A if and only if it holds for B.*

Assume now that Conjecture 1.1 is true for modular elliptic curves. Since the elliptic curve E/F_i is modular, the Birch and Swinnerton-Dyer conjecture holds for E/F_i, and thus from Theorem 3.1, it holds for $\mathrm{Res}_{F_i/F} E/F_i$. Now from (3.1) we deduce that $E/F \times \prod_{i'} -n_{i'} \mathrm{Res}_{F_{i'}/F} E/F_{i'}$ and $\prod_{i''} n_{i''} \mathrm{Res}_{F_{i''}/F} E/F_{i''}$ are isogenous (for details see the proof of Theorem 2.3 of [D]), where i' is such that $n_{i'}$ is negative and i'' is such that $n_{i''}$ is positive. Using now Theorem 3.2 we find that the Birch and Swinnerton-Dyer conjecture holds for E, which concludes the proof of Theorem 1.2. ∎

REMARK 3.3. There exists a statement for the Birch and Swinnerton-Dyer conjecture for a general abelian variety A defined over a number field F, and Theorem 1.2 remains true if one replaces the elliptic curve E/F by $(E_1 \times \cdots \times E_r)/F$, where $r \leq 4$ and $E_1, \ldots, E_r$ are elliptic curves defined over the totally real field F. This is true because of Theorem 2.1, Theorem 3.1, and the fact that the L-function $L(s, \pi_1 \times \cdots \times \pi_r)$, where $\pi_1, \ldots, \pi_r$ are automorphic representations of $\mathrm{GL}(2)/F$, has a meromorphic continuation and satisfies a functional equation (see [JS] and [R]). The proof of this result is similar to the one of Theorem 1.2.

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.

[CR] C. W. Curtis and I. Reiner, *Methods of Representation Theory*, Vol. I, Wiley, New York, 1981.

[D] T. Dokchitser and V. Dokchitser, *On the Birch–Swinnerton-Dyer quotients modulo squares*, Ann. of Math. 172 (2010), 567–596.

[JS] H. Jacquet and J. A. Shalika, *On Euler products and the classification of automorphic forms I, II*, Amer. J. Math. 103 (1981), 499–558, 777–815.

[L] R. P. Langlands, *Base Change for GL_2*, Ann. of Math. Stud. 96, Princeton Univ. Press, 1980.

[M1] J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. 17 (1972), 177–190.

[M2] —, *Arithmetic Duality Theorems*, Perspectives Math. 1, Academic Press, 1986.

[R] D. Ramakrishnan, *Modularity of the Rankin–Selberg L-series, and multiplicity one for* SL(2), Ann. of Math. 152 (2000), 45–111.

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

[V] C. Virdol, *Potential modularity for elliptic curves and some applications*, J. Number Theory 129 (2009), 3109–3114.

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

Cristian Virdol
Department of Mathematics
Columbia University
New York, NY 10027, U.S.A.
E-mail: virdol@math.columbia.edu

Received on 3.8.2009
and in revised form on 25.5.2010 (6107)