THE EQUIVARIANT TAMAGAWA NUMBER CONJECTURE AND MODULAR SYMBOLS

WERNER BLEY

Abstract. We show that for each elliptic curve $E/\mathbb{Q}$ with $L(E/\mathbb{Q},1) \neq 0$ there are infinitely many odd primes l and for each such l infinitely many abelian l-extensions $K/\mathbb{Q}$ such that the l-part of the equivariant Tamagawa number conjecture holds for the pair $(h^1(E_K)(1), \mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})])$.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ a finite Galois extension with group G. We write E_K for the base change of E and consider the motive $M_K := h^1(E_K)(1)$ as a motive over $\mathbb{Q}$ with a natural action of the semi-simple $\mathbb{Q}$-algebra $\mathbb{Q}[G]$.

In this manuscript we study the equivariant Tamagawa number conjecture (for short, ETNC) as formulated by Burns and Flach in [3] for the pair $(M_K, \mathbb{Z}[G])$ in the case where $K/\mathbb{Q}$ is an abelian l-extension where l denotes an odd prime. In this context the l-part of the ETNC, here denoted by ETNC_l, is of particular interest. Combining recent results of Fearnley, Kisilevsky and Kuwata [6] and of the author [2] with the theory of modular symbols as introduced by Mazur and Tate in [7] we prove ETNC_l for infinitely many pairs (E, K). More precisely, we show that for any elliptic curve $E/\mathbb{Q}$ with $L(E/\mathbb{Q},1) \neq 0$ there exist infinitely many primes l and for each such l infinitely many abelian l-extensions $K/\mathbb{Q}$ satisfying the the explicit hypotheses below. By important results of Gross and Zagier and Kolyvagin (see [5] for a survey) we may assume the l-part of the Birch and Swinnerton-Dyer conjecture for $E/\mathbb{Q}$. Together with our explicit conditions this allows us to deduce ETNC_l. We want to emphasize here that ETNC_l cannot be deduced from the Birch and Swinnerton-Dyer conjectures for E/F where F runs through the subfields of $K/\mathbb{Q}$ (see Remark 2.2).

To present our results in more detail we need to introduce some notations most of which are standard. Throughout the manuscript we write d_K for the discriminant of K and N_E for the conductor of E. For a prime p we write $c_p(E, \mathbb{Q})$ for the usual Tamagawa factor at p and if $p \nmid N_E$ we let $\bar{E}(\mathbb{F}_p)$ denote the group of $\mathbb{F}_p$-rational points on the reduced curve E modulo p. As usual we write $E(K)$ for the Mordell-Weil group and $Ш(E/K)$ for the Tate-Shafarevic group.

We impose the following

Hypotheses 1.1.

(i) $[K : \mathbb{Q}] = l^n, l$ *an odd prime,*
(ii) $(d_K, l) = 1, \quad (d_K, N_E) = 1,$
(iii) $l \nmid \#E(\mathbb{Q})_{tors} \prod_{p \mid d_K} \#\bar{E}(\mathbb{F}_p),$

Date: November 4, 2011.

(iv) $l \nmid N_E$,
(v) $l \nmid \prod_{p \mid N_E} c_p(E, \mathbb{Q})$,
(vi) $\mathrm{rk}_{\mathbb{Z}} E(K) = 0$,
(vii) $l \nmid \#Ш(E/K)$.

In the following a pair (E, K) satisfying Hypotheses 1.1 is called *l-arithmetically trivial.*

Let $X_0(N_E)$ denote the modular curve of level N_E and let $\varphi \colon X_0(N_E) \longrightarrow E$ be a modular parametrization. Let $c(\varphi)$ be the Manin constant associated to φ.

The main results of this manuscript are as follows.

Theorem 1.2. *Let l be an odd prime, $K/\mathbb{Q}$ an abelian extension and $E/\mathbb{Q}$ an elliptic curve such that (E, K) is l-arithmetically trivial. Assume that $l \nmid c(\varphi)\#Ш(E/\mathbb{Q})$ and that the l-part of the Birch and Swinnerton-Dyer conjecture for $E/\mathbb{Q}$ is valid. Then ETNC$_l$ holds for the pair $(M_K, \mathbb{Z}[G])$.*

Theorem 1.3. *Let $E/\mathbb{Q}$ be an elliptic curve such that $L(E/\mathbb{Q}, 1) \neq 0$. Then there are infinitely many primes l and for each such prime l infinitely many abelian extensions $K/\mathbb{Q}$ such that (E, K) is l-arithmetically trivial.*

If $L(E/\mathbb{Q}, 1) \neq 1$, then it is well known that $Ш(E/\mathbb{Q})$ is finite and that the Birch and Swinnerton-Dyer conjecture holds up to a rational factor. Hence we deduce

Corollary 1.4. *Let $E/\mathbb{Q}$ be an elliptic curve such that $L(E/\mathbb{Q}, 1) \neq 0$. Then there are infinitely many primes l and for each such l infinitely many abelian l-extensions $K/\mathbb{Q}$ such that ETNC$_l$ holds for the pair $(M_K, \mathbb{Z}[G])$.*

The author thanks Christian Wuthrich for very helpful discussions concerning the application of modular symbols and valuable comments on a preliminary version of this manuscript.

2. A special case of ETNC

In this section we briefly recall the relevant results of [2]. In particular, we will state (in our very special setting) a very explicit reformulation of ETNC$_l$. Throughout this section we assume that l is an odd prime such that the pair (E, K) is l-arithmetically trivial.

For a finite group G we write $\mathrm{Irr}(G)$ for the set of absolutely irreducible characters. For any ring R we let $\zeta(R)$ denote the center of R. As usual, we canonically identify the center $\zeta(\mathbb{C}[G])$ of the complex group ring $\mathbb{C}[G]$ with $\bigoplus_{\chi \in \mathrm{Irr}(G)} \mathbb{C}$. We recall that the equivariant motivic L-function $L(M_K, s)$ attached to M_K is given by the $\zeta(\mathbb{C}[G])$-valued function $(L(E/\mathbb{Q}, \bar{\chi}, s+1))_{\chi \in \mathrm{Irr}(G)}$ (for some further details see the paragraph preceding [1, Remark 3.2]). For each character χ we let $L^*(E/\mathbb{Q}, \chi, 1)$ denote the leading coefficient in the Taylor expansion at $s = 1$ and set

$$\mathcal{L}^* := (L^*(E/\mathbb{Q}, \bar{\chi}, 1))_{\chi \in \mathrm{Irr}(G)} .$$

From [2, Prop. 2.8] we deduce $\mathcal{L}^* \in \zeta(\mathbb{R}[G])$.

We let ω_0 denote a Néron differential and write γ_+ and γ_- for $\mathbb{Z}$-generators of $H_1(E(\mathbb{C}), \mathbb{Z})^+$ and $H_1(E(\mathbb{C}), \mathbb{Z})^-$, respectively. We define

$$\Omega_+ := \int_{\gamma_+} \omega_0, \quad \Omega_- := \int_{\gamma_-} \omega_0,$$

and normalize $\gamma_\pm$ such that Ω_+ is positive real and Ω_- is a positive real multiple of i.

We fix an embedding $\iota\colon K \hookrightarrow \mathbb{C}$. Since l is unramified in $K/\mathbb{Q}$, the ring $\mathcal{O}_{K,l} := \mathcal{O}_K \otimes_{\mathbb{Z}} \mathbb{Z}_l$ is $\mathbb{Z}_l[G]$-free. Let $\alpha_0 \in K$ be a $\mathbb{Z}_l[G]$-generator of $\mathcal{O}_{K,l}$ and set

$$\lambda_{\alpha_0} := \Omega_+ \left(\sum_{\sigma \in G} (\iota \circ \sigma)(\alpha_0)\sigma^{-1} \right)^{-1}$$

Since l is odd K is totally real and therefore we deduce from [1, Prop. 3.1] that the equivariant period is given by $\mathrm{Nrd}_{\mathbb{R}[G]}(\lambda_{\alpha_0})$. Explicitly we obtain

$$\mathrm{Nrd}_{\mathbb{R}[G]}(\lambda_{\alpha_0}) := \frac{\Omega}{R(\alpha_0)}$$

with

$$\begin{aligned} R_\chi &= R_\chi(\alpha_0) = \det\left(\sum_{\sigma\in G} \iota(\sigma(\alpha_0))T_\chi(\sigma^{-1}) \right), \\ \Omega_\chi &= \Omega_+^{\chi(1)}, \end{aligned}$$

where $T_\chi : G \longrightarrow \mathrm{Gl}_{\chi(1)}(\mathbb{C})$ is a representation associated to the character χ.

Finally we set

$$u_l = u_l(\alpha_0) := \frac{\mathcal{L}^* R(\alpha_0)}{\Omega} = \left(\frac{L^*(E/\mathbb{Q}, \bar\chi, 1) R_\chi(\alpha_0)}{\Omega_+^{\chi(1)}} \right)_{\chi \in \mathrm{Irr}(G)} \tag{1}$$

and

$$\xi_l := \prod_{p | d_K} \left(L_p(E/\mathbb{Q}, \bar\chi, 1) \right)^{-1}_{\chi\in\mathrm{Irr}(G)} \tag{2}$$

where $L_p(E/\mathbb{Q}, \bar\chi, 1)$ denotes the local Euler factor at $s = 1$. By equation (8) of [2] and the paragraphs following it we have

$$\mathrm{ETNC}_l \text{ is valid } \iff u_l \equiv \xi_l (\mathrm{mod}\ \mathrm{Nrd}_{\mathbb{R}[G]}(\mathbb{Z}_l[G]^\times)). \tag{3}$$

Note that by [1, Rem. 3.6] the validity of the right hand side does not depend on the choice of α_0.

Remark 2.1. We will use the Hypotheses 1.1 to establish ETNC_l by proving the equivalent congruence condition in (3). It seems to be possible to prove this congruence in greater generality, however, all of Hypotheses 1.1 is needed to show the equivalence to ETNC_l.

Remark 2.2. It does not seem to be possible to deduce ETNC_l from the validity of the Birch and Swinnerton-Dyer conjectures for E/F where F runs over all subfields of $K/\mathbb{Q}$. For example, if $K/\mathbb{Q}$ is cyclic of order l and $L(E/K, 1) \neq 0$, then one can prove that $u_l\xi_l^{-1} \in \zeta(\mathbb{Q}[G])^\times = \mathbb{Q}[G]^\times$. However, $\mathbb{Q}_l[G] \simeq \mathbb{Q}_l \oplus \mathbb{Q}_l(\zeta_l)$ and an element $\lambda \in \mathbb{Q}_l[G]^\times$ corresponding to $(\lambda_0, \lambda_1) \in \mathbb{Q}_l \oplus \mathbb{Q}_l(\zeta_l)$ is contained in $\mathbb{Z}_l[G]^\times$ if and only if $\lambda_0 \in \mathbb{Z}_l^\times$, $\lambda_1 \in \mathbb{Z}_l[\zeta_l]^\times$ and $\lambda_0 \equiv \lambda_1 (\mathrm{mod}\ (1 - \zeta_l))$. For more examples of these congruences we refer the reader to [1, Sec. 2.3] and [2, Sec. 5].

3. Abelian extensions and modular symbols

In this section we briefly recall the definition and relevant properties of modular symbols as introduced by Mazur and Tate in [7] and normalized by Darmon in [4]. We combine this with the explicit formulation of ETNC$_l$ given in (3) in order to prove Theorem 1.2.

Let f be a square-free positive integer such that $(f, N_E) = 1$. Let $\mathbb{Q}(\zeta_f)^+$ denote the maximal real subfield of the f-th cyclotomic field $\mathbb{Q}(\zeta_f)$. We set $G_f := \mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})$ and $G_f^+ := \mathrm{Gal}(\mathbb{Q}(\zeta_f)^+/\mathbb{Q})$. As usual, for any $a \in (\mathbb{Z}/f\mathbb{Z})^\times$ we write σ_a for the automorphism which sends ζ_f to ζ_f^a.

Let $\Lambda \subseteq \mathbb{C}$ denote a Néron lattice. Then we can identify $E(\mathbb{C})$ with $\mathbb{C}/\Lambda$ and ω_0 with dz. We define $\Omega^\pm \in \mathbb{R}_{>0}$ such that $\Lambda \subseteq \mathbb{Z}\Omega^+ \oplus \mathbb{Z}i\Omega^-$ with minimal index. We let c_∞ denote the number of components of $E(\mathbb{R})$, i.e., $c_\infty = 2$ if $E(\mathbb{R})$ is rectangular and $c_\infty = 1$ otherwise. Then $\Omega^\pm = \frac{c_\infty}{2}\Omega_\pm$.

If $\varphi\colon X_0(N_E) \longrightarrow E$ is a modular parametrization, then the pullback of the Néron differential ω_0 defines a cusp form of weight 2 on $X_0(N_E)$,

$$\varphi^*\omega_0 = c(\varphi)f(q)dq/q = c(\varphi)\cdot 2\pi i f(z)dz,$$

where $f(q) = \sum_{n\geq 1} a_n q^n$, $q = \exp(2\pi i z)$, is normalized such that $a_1 = 1$ and $c(\varphi)$ denotes the Manin constant.

Following Mazur and Tate [7] we define the modular symbols by the equality

$$2\pi i \int_{a/t}^{a/t+i\infty} f(z)dz = \left[\frac{a}{t}\right]^+ \Omega^+ + i\left[\frac{a}{t}\right]^- \Omega^-.$$

The modular symbol $\left[\frac{a}{t}\right]^\pm$ depends only on the value of a modulo t. Since we will only consider totally real abelian extensions $K/\mathbb{Q}$ we will henceforth only consider the modular symbols $[\ ]^+$. Following Darmon [4] we define the regularized modular symbols by

$$\left[\frac{a}{f}\right]^* := \sum_{1\leq t|f} \mu\left(\frac{f}{t}\right)\left[\frac{a(f/t)^{-1}}{t}\right]^+$$

where μ denotes the Möbius function and $(f/t)^{-1}$ is the inverse of f/t modulo t. Recall here that f is square-free so that f/t and t are relatively prime.

We set

$$\Theta_f^{MT} := \frac{1}{2}\sum_{a\in(\mathbb{Z}/f\mathbb{Z})^\times}\left[\frac{a}{f}\right]^*\sigma_a \in \mathbb{Q}[G_f]$$

and call it the *Mazur-Tate element.*

We recall the main properties of Θ_f^{MT}. Since l is odd and $l \nmid \#E(\mathbb{Q})_{tors}$ we have

$$\Theta_f^{MT} \in \mathbb{Z}_l[G_f]. \tag{4}$$

If $p \nmid f$ and $z_p : \mathbb{Q}[G_{fp}] \longrightarrow \mathbb{Q}[G_f]$ denotes the canonical projection, then

$$z_p(\Theta_{fp}^{MT}) = -\sigma_p(p - \sigma_p^{-1}a_p + \sigma_p^{-2})\Theta_f^{MT}. \tag{5}$$

This is precisely Lemma 2.2 of [4]. Finally we recall the relation to twisted Hasse-Weil-L-functions. We write

$$L^{MT}(E/\mathbb{Q},\chi,s) = \sum_{n=1}^\infty \chi(n)a_n n^{-s}$$

for the L-series considered in [7] and [4]. Here we consider χ as a primitive character defined modulo its conductor f_χ. If f is a positive multiple of f_χ, then we write $L_f^{MT}(E/\mathbb{Q}, \chi, s)$ for the L-function where we omit the primes dividing f in the definition via the usual Euler product, i.e., we consider χ as a character modulo f. If χ is an even Dirichlet character of conductor f_χ dividing f, then by [4, Prop. 2.3]

$$\chi(\Theta_f^{MT}) = c(\varphi)\frac{f}{f_\chi}\frac{\tau(\chi)L_f^{MT}(E/\mathbb{Q}, \bar{\chi}, 1)}{2\Omega^+} \tag{6}$$

with the Gauss sum

$$\tau(\chi) = \sum_{a=1} \chi(a)e^{2\pi i a/f},$$

where χ is considered as a character modulo f, i.e., $\chi(a) = 0$ whenever a and f are not coprime.

Unfortunately our L-functions are not normalized in the same way as the L-functions in [7] and [4]. In the following we describe how they are related.

We let $T_l(E) := \varprojlim E[l^n]$ denote the l-adic Tate module. We define $V_l(E) := T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ and set

$$H_l(E) := \mathrm{Hom}(V_l(E), \mathbb{Q}_l) \otimes_{\mathbb{Q}_l} \bar{\mathbb{Q}}_l.$$

For $\chi \in \mathrm{Irr}(G)$ we write V_χ for a representation space for χ and without loss of generality we regard V_χ as a $\bar{\mathbb{Q}}_l$-vector space. For primes $p \neq l$ the local polynomials used to define the equivariant motivic L-function (see [3, Remark 7]) are given by

$$P_p(E/\mathbb{Q}, \chi, T) := \det\left(1 - Fr_p^{-1}T \mid \left(H_l(E) \otimes_{\bar{\mathbb{Q}}_l} V_\chi\right)^{I_p}\right).$$

Let α, β denote the eigenvalues of Fr_p on $V_l(E)$. It follows that for abelian characters χ and primes p such that $p \nmid d_K N_E$ one has

$$P_p(E/\mathbb{Q}, \chi, T) = (1 - \bar{\chi}(p)\alpha T)(1 - \bar{\chi}(p)\beta T) = 1 - \bar{\chi}(p)a_p T + \bar{\chi}(p)^2 p T^2. \tag{7}$$

Since $(f, N_E) = 1$ we have $\left(H_l(E) \otimes_{\bar{\mathbb{Q}}_l} V_\chi\right)^{I_p} = H_l(E)^{I_p} \otimes_{\bar{\mathbb{Q}}_l} V_\chi^{I_p}$. Furthermore,

$$V_\chi^{I_p} = 0 \iff I_p \not\subseteq \ker(\chi) \iff p \mid f_\chi. \tag{8}$$

It follows from (7) and (8) that $L(E/\mathbb{Q}, \chi, s) = \sum_{n=1}^\infty \bar{\chi}(n)a_n n^{-s}$ where χ is considered as a primitive character modulo f_χ. For future reference we record

$$L^{MT}(E/\mathbb{Q}, \chi, s) = L(E/\mathbb{Q}, \bar{\chi}, s). \tag{9}$$

We rewrite (6) and obtain

$$\chi(\Theta_f^{MT}) = c(\varphi)\frac{f}{f_\chi}\frac{\tau(\chi)L_f(E/\mathbb{Q}, \chi, 1)}{2\Omega^+}. \tag{10}$$

Our next aim is to relate the Gauss sum $\tau(\chi)$ to our resolvent $R_\chi(\alpha_0)$ for a suitable choice of normal basis element α_0. Let $f = f_K$ denote the conductor of K. Since l is unramified in $K/\mathbb{Q}$ by (ii) the conductor f is squarefree. By Hilbert's Theorem 132 the element ζ_f generates a normal integral basis for $\mathbb{Q}(\zeta_f)/\mathbb{Q}$ and consequently $\alpha_0 := \mathrm{Tr}_{\mathbb{Q}(\zeta_f)/K}(\zeta_f)$ is an integral normal basis element for $K/\mathbb{Q}$. We let $\iota\colon K \hookrightarrow \mathbb{C}$ denote the embeding which is induced by $\zeta_f \mapsto \exp(2\pi i/f)$, but usually omit ι from the notation. We obtain

$$\begin{aligned}\lambda_0 = \lambda_0(\alpha_0) &= \sum_{\sigma\in G}\sigma(\alpha_0)\sigma^{-1} = \sum_{\sigma\in G}\sigma\left(\sum_{\tau\in\mathrm{Gal}(\mathbb{Q}(\zeta_f)/K)}\tau(\zeta_f)\right)\sigma^{-1}\\ &= \sum_{\gamma\in\mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})}\gamma(\zeta_f)\left(\gamma|_K\right)^{-1} = \sum_{a\in(\mathbb{Z}/f\mathbb{Z})^\times}\zeta_f^a\left(\sigma_a|_K\right)^{-1}.\end{aligned}$$

We conclude that for each character $\chi \in \mathrm{Irr}(G)$ we have

$$R_\chi(\alpha_0) = \chi(\lambda_0) = \tau(\bar\chi). \tag{11}$$

Proof of Theorem 1.2 By (3) we must show that the element $\eta_l := u_l\xi_l^{-1}$ is contained in $\mathrm{Nrd}_{\mathbb{R}[G]}(\mathbb{Z}_l[G]^\times) = \mathbb{Z}_l[G]^\times$, where u_l and ξ_l are defined in (1) and (2), respectively. From (10), (11) and $\Omega^+ = \frac{c_\infty}{2}\Omega_+$ we deduce

$$\eta_l = \left(\frac{c_\infty f_\chi}{c(\varphi)f}\bar\chi(\Theta_f^{MT})\right)_{\chi\in\mathrm{Irr}(G)}.$$

Let $^\#: \mathbb{Q}_l[G] \longrightarrow \mathbb{Q}_l[G]$ denote the involution induced by $g \mapsto g^{-1}$. We obtain the fundamantal relation

$$\chi(\Theta_f^{MT,\#}) = \frac{c(\varphi)f}{c_\infty f_\chi}\eta_{l,\chi}, \quad \forall\chi\in\mathrm{Irr}(G). \tag{12}$$

For $\chi \in \mathrm{Irr}(G)$ we let $e_\chi := \sum_{g\in G}\chi(g)g^{-1}$ denote the primitive idempotent attached to χ. Since G is abelian we may and will identify $\eta_l = (\eta_{l,\chi})_{\chi\in\mathrm{Irr}(G)}$ with the group ring element $\eta_l = \sum_{\chi\in\mathrm{Irr}(G)}\eta_{l,\chi}e_\chi$. We write Θ_K^{MT} for the image of Θ_f^{MT} under the canononical map $\mathbb{Z}_l[G_f] \longrightarrow \mathbb{Z}_l[G]$. Then we obtain from (12)

$$\Theta_K^{MT,\#} = \frac{c(\varphi)}{c_\infty}\left(\sum_{\chi\in\mathrm{Irr}(G)}\frac{f}{f_\chi}e_\chi\right)\eta_l.$$

By Proposition 3.1 (see below) we know that $\sum_\chi \frac{f}{f_\chi}e_\chi \in \mathbb{Z}_l[G]^\times$, so that it remains to show that $\Theta_K^{MT,\#} \in \mathbb{Z}_l[G]^\times$. Let χ_0 denote the trivial character. For $\alpha, \beta \in \mathbb{Q}_l^\times$ we wite $\alpha =_l \beta$ if $\alpha/\beta \in \mathbb{Z}_l^\times$. Then

$$\begin{aligned}\chi_0(\Theta_f^{MT,\#}) &= c(\varphi)f\frac{\tau(\chi_0)L_f(E/\mathbb{Q},1)}{2\Omega^+}\\ &= c(\varphi)f\tau(\chi_0)\left(\prod_{p|d_K}L_p(E/\mathbb{Q},1)\right)\frac{L(E/\mathbb{Q},1)}{c_\infty\Omega_+}\\ &=_l c(\varphi)f\left(\prod_{p|d_K}L_p(E/\mathbb{Q},1)\right)\frac{\#Ш(E/\mathbb{Q})}{(\#E(\mathbb{Q})_{tors})^2}\prod_{p|N_E}c_p(E,\mathbb{Q}),\end{aligned}$$

where we used $\tau(\chi_0) = \pm1$ and the validity of the l-part of the Birch and Swinnerton-Dyer conjecture for $E/\mathbb{Q}$. We claim that under our hypotheses the right hand side is an l-adic unit. For each of the factors in the product, except the Euler factors, this is immdiately clear from Hypotheses 1.1 (i)-(vii) and the additional assumptions made in the statement of Theorem 1.2. Each of the Euler factors is of the form

$$L_p(E/\mathbb{Q}, s) = 1 - a_p p^{-s} + p^{1-2s},$$

with $a_p = p + 1 - \#\bar{E}(\mathbb{F}_p)$, so that $pL_p(E/\mathbb{Q}, 1) = \#\bar{E}(\mathbb{F}_p)$. Hence hypothesis (iii) implies that $L_p(E/\mathbb{Q}, 1)$ is indeed an l-adic unit.

Since G is an l-group, the group ring $\mathbb{Z}_l[G]$ is a local ring with maximal ideal given by the kernel of the natural map $\mathbb{Z}_l[G] \longrightarrow \mathbb{F}_l$ which is induced by $\lambda \mapsto \chi_0(\lambda) \bmod l\mathbb{Z}_l$. It follows that $\Theta_f^{MT,\#}$ is contained in $\mathbb{Z}_l[G]^\times$.

To complete the proof of Theorem 1.2 it remains to show the following proposition.

Proposition 3.1. *a) Let $K/\mathbb{Q}$ be a tame abelian extension with group G and conductor $f = f_K$. Then*

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{f}{f_\chi} e_\chi \in \mathbb{Z}[G].$$

b) If, in addition, G is an l-group and $l \nmid f$, then

$$\sum_{\chi \in \mathrm{Irr}(G)} \frac{f}{f_\chi} e_\chi \in \mathbb{Z}_l[G]^\times.$$

Proof. a) For a divisor d of f we set

$$f(d) = \sum_{f_\chi = d} e_\chi, \quad g(d) = \sum_{f_\chi \mid d} e_\chi.$$

Let n be any positive divisor of f. Then $\sum_{d|n} f(d) = g(n)$ and by Möbius inversion $\sum_{d|n} \mu(n/d) g(d) = f(n)$, or rather,

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{f_\chi | d} e_\chi = \sum_{f_\chi = n} e_\chi.$$

Since $\sum_\chi \frac{f}{f_\chi} e_\chi = \sum_{n|f} \frac{f}{n} \sum_{f_\chi = n} e_\chi$ it remains to show

$$\sum_{n|f} \frac{f}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{f_\chi|d} e_\chi \in \mathbb{Z}[G]. \tag{13}$$

Let $H_d := \mathrm{Gal}(K/K \cap \mathbb{Q}(\zeta_d))$. By definition of the conductor we obtain

$$f_\chi \mid d \iff K^{\ker(\chi)} \subseteq K \cap \mathbb{Q}(\zeta_d) \iff H_d \subseteq \ker(\chi).$$

It follows that $\sum_{f_\chi|d} e_\chi = e_{H_d}$, where we write $e_H := \frac{1}{\#H} \sum_{h \in H} h$ for the idempotent attached to a subgroup H of G. Substituting this in (13) we further conclude

$$\sum_{n|f} \frac{f}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{f_\chi|d} e_\chi = \sum_{d|f} \left(\sum_{t|\frac{f}{d}} \frac{f/d}{t} \mu(t) \right) e_{H_d}.$$

By induction it is easily shown that for any squarefree integer s one has

$$\sum_{t|s} \frac{s}{t} \mu(t) = \prod_{p|s} (p-1).$$

Hence it suffices to show that

$$\left(\prod_{p\mid\frac{f}{d}}(p-1)\right)e_{H_d}\in\mathbb{Z}[G].$$

This finally follows from

$$\#H_d=[K:K\cap\mathbb{Q}(\zeta_d)]\mid[\mathbb{Q}(\zeta_f):\mathbb{Q}(\zeta_d)]=\prod_{p\mid\frac{f}{d}}(p-1).$$

b) In this case $\chi_0\left(\sum_{\chi\in\mathrm{Irr}(G)}\frac{f}{f_\chi}e_\chi\right)=f$, so that $\sum_{\chi\in\mathrm{Irr}(G)}\frac{f}{f_\chi}e_\chi$ is not contained in the maximal ideal of the local ring $\mathbb{Z}_l[G]$.

□

4. Satisfying the hypothesis

In this section we will prove Theorem 1.3.

Proof of Theorem 1.3 By results of Kolyvagin we know that $Ш(E/\mathbb{Q})$ is finite. If E does not have complex multiplication, then fundamental work of Serre [10] shows that $\mathrm{Gal}(\mathbb{Q}(E[l])/\mathbb{Q})$ is isomorphic to $\mathrm{Gl}_2(\mathbb{F}_l)$ for almost all primes l. If E has complex multiplication, say by some order in the imaginary-quadratic field k, then the classical results of the theory of complex multiplication show that for almost all primes l one has

$$[\mathbb{Q}(E[l]):\mathbb{Q}]=\begin{cases}\frac{1}{w_k}(l-1)^2, & \text{if } l \text{ is split in } k/\mathbb{Q},\\ \frac{1}{w_k}(l^2-1), & \text{if } l \text{ is inert in } k/\mathbb{Q}.\end{cases}$$

Here w_k denotes the number of roots of unity in k.

It easily follows that for each elliptic curve $E/\mathbb{Q}$ there are infinitely many primes l such that

$$\begin{array}{ll}(a) & l\nmid\#E(\mathbb{Q})_{tors}\#Ш(E/\mathbb{Q})N_E\prod_{p\mid N_E}c_p(E,\mathbb{Q}),\\ (b) & [\mathbb{Q}(E[l]):\mathbb{Q}(\zeta_l)]\text{ is not a power of } l.\end{array}$$

For any finite extension $K/\mathbb{Q}$ let $S^{(l)}(E/\mathbb{Q})$ and $S^{(l)}(E/K)$ denote the respective Selmer groups. Let $S:=\{l,\infty\}\cup\{q: q\text{ divides }N_E\}$ and denote by S_K the set of places of K lying over the places in S. Let $H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}},E[l];S)$ (resp. $H^1(G_{\bar{\mathbb{Q}}/K},E[l];S_K)$) denote the set of cohomology classes which are unramified outside S (resp. S_K). Then by [9, Ch. X, Cor.4.4]

$$\begin{aligned}S^{(l)}(E/\mathbb{Q})&\subseteq H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}},E[l];S),\\ S^{(l)}(E/K)&\subseteq H^1(G_{\bar{\mathbb{Q}}/K},E[l];S_K).\end{aligned}$$

By [8, Ch. I, Prop.3.8] we obtain

$$\begin{aligned}S^{(l)}(E/\mathbb{Q})&=\ker\left(H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}},E[l];S)\longrightarrow\prod_{p\in S}H^1(G_{\bar{\mathbb{Q}}_p/\mathbb{Q}_p},E)\right),\\ S^{(l)}(E/K)&=\ker\left(H^1(G_{\bar{\mathbb{Q}}/K},E[l];S_K)\longrightarrow\prod_{v\in S_K}H^1(G_{\bar{K}_v/K_v},E)\right).\end{aligned}$$

Let $S = \{\infty, l, q_1, \dots, q_t\}$. We will first show that there is a positive density of primes p such that

$$\begin{array}{ll} (c) & p \equiv 1 (\mathrm{mod}\ l), \\ (d) & q \equiv y_q^l (\mathrm{mod}\ p) \text{ with } y_q \in \mathbb{Z}/p\mathbb{Z} \text{ for all } q \in S \setminus \{\infty\}, \\ (e) & a_p - 2 \not\equiv 0 (\mathrm{mod}\ l). \end{array}$$

For this purpose we consider the tower of fields

$$\mathbb{Q} \subseteq E \subseteq F \subseteq L$$

with

$$E := \mathbb{Q}(\zeta_l), \quad F := E(\sqrt[l]{l}, \sqrt[l]{q_1}, \dots, \sqrt[l]{q_t}), \quad L := F(E[l]).$$

Because of (b) there exists $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma \neq id$ and $\sigma|_F = id$. Hence $\sigma|_{\mathbb{Q}(E[l])} \neq id$. By Chebotarev's density theorem there are infinitely many unramified primes $\mathfrak{P}$ of L such that the Frobenius of $\mathfrak{P}$ is contained in the conjugacy class of σ. Let p denote the residue characteristic of $\mathfrak{P}$. Then p is completely split in $F/\mathbb{Q}$ and (c) and (d) are immediate from our construction. We now demonstrate (e). Let α, β denote the eigenvalues of Fr_p on $V_l(E)$. Then α and β are contained in $\mathbb{Z}_l$ and satisfy $\alpha + \beta = a_p$ and $\alpha\beta = p$. Because of (c) the eigenvalues α and β are actually units in $\mathbb{Z}_l$. Now suppose that $a_p \equiv 2(\mathrm{mod}\ l)$. Then one easily shows that $\alpha \equiv \beta \equiv 1(\mathrm{mod}\ l)$, and hence, Fr_p acts trivial on $E[l]$. This is a contradiction to $\sigma|_{\mathbb{Q}(E[l])} \neq id$.

Let K denote the unique subfield of $\mathbb{Q}(\zeta_p)$ with $[K : \mathbb{Q}] = l$ and set $G := \mathrm{Gal}(K/\mathbb{Q})$. It remains to show (iii), (vi) and (vii).

Combining (c) and (e) we deduce (iii) from $a_p - 2 = p - 1 - \#\bar{E}(\mathbb{F}_p)$. From (e) and the proof of [6, Th. 3.7] we deduce that $L(E/\mathbb{Q}, \chi, 1) \neq 0$ for each non-trivial character χ of $\mathrm{Gal}(K/\mathbb{Q})$. Hence $L(E/K, 1) \neq 0$ and by results of Longo and Tian and Zhang (see e.g. [5, Theorem 3.7]) we conclude that $\mathrm{rk}(E(K)) = 0$. This is (vi).

Since G is an l-group (iii) implies that $l \nmid \#E(K)_{tors}$. From the exact sequence

$$0 \longrightarrow E(K)/lE(K) \longrightarrow S^{(l)}(E/K) \longrightarrow Ш(E/K)[l] \longrightarrow 0$$

we derive $Ш(E/K)[l] \simeq S^{(l)}(E/K)$ (and analogously $Ш(E/\mathbb{Q})[l] \simeq S^{(l)}(E/\mathbb{Q})$). Hence it suffices to show that $S^{(l)}(E/K) = 0$.

From the inflation-restriction sequence (see [11, VII, §6]) we see that the restriction map induces an isomorphism

$$res\colon H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E[l]) \xrightarrow{\simeq} H^1(G_{\bar{\mathbb{Q}}/K}, E[l])^G.$$

Let $S_{ram} = \{p\}$ denote the set of primes which ramify in $K/\mathbb{Q}$. We set $S' := S \cup S_{ram}$ and write S'_K for the set of primes of K lying above primes in S'. Then it is straightforward to show that res induces an isomorphism between $H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E[l]; S')$ and $H^1(G_{\bar{\mathbb{Q}}/K}, E[l]; S'_K)^G$. Hence we have the diagram

$$\begin{tikzcd} S^{(l)}(E/\mathbb{Q}) \arrow[r, "\subseteq"] \arrow[d] & H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E[l]; S') \arrow[d, "\simeq"', "res"] \\ S^{(l)}(E/K)^G \arrow[r, "\subseteq"] & H^1(G_{\bar{\mathbb{Q}}/K}, E[l]; S'_K)^G \end{tikzcd}$$

Assume that there is a non-trivial element $\xi \in S^{(l)}(E/K)^G$. Let $\eta \in H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E[l]; S')$ such that $res(\eta) = \xi$. Then η becomes trivial in $H^1(G_{\bar{K}_v/K_v}, E)$ for all $v \in S'_K$.

Let $v \mid q$. If $q \in S$, then $K_v = \mathbb{Q}_q$ since finite primes q split completely in $K/\mathbb{Q}$ by (d) and K is totally real. If $q = p$, then $K_v = \mathbb{Q}_q$ since p is totally ramified in $K/\mathbb{Q}$ by construction. As a consequence, the element η is a non-trivial element in $S^{(l)}(E/\mathbb{Q})$ which contradicts (a).

Since G is an l-group, it follows immediately that $S^{(l)}(E/K)$ is trivial. Indeed,

$$|S^{(l)}(E/K)| = |S^{(l)}(E/K)^G| + \sum(\text{cardinality of } G\text{-orbits of length } > 1),$$

so that $|S^{(l)}(E/K)| = 1$.

Remark 4.1. In the proof we only constructed fields K of prime conductor p. But one can easily prove that any composite K of these fields will also satisfy Hypotheses 1.1. For the conditions (i) - (v) this is obvious. The proof of [6, Th. 3.7] shows that $L(E/\mathbb{Q}, \chi, 1) \neq 0$ for each non-trivial character χ of $\mathrm{Gal}(K/\mathbb{Q})$ since we have (e) for each of the prime divisors of f_K. Finally an induction argument very similar as above shows (vii).

References

[1] W. Bley, *Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture*, to appear in Exp. Math.

[2] W. Bley, *Numerical evidence for the equivariant Birch and Swinnerton-Dyer conjecture (part II)*, to appear in Math. Comp.

[3] D. Burns, M. Flach *Tamagawa numbers for motives with (non-commutative) coefficients*, Documenta Math. **6** (2001) 501-570.

[4] H. Darmon, *Euler systems and refined conjectures of Birch and Swinnerton-Dyer type*, Contemporary Mathematics **165** (1994), 265–276.

[5] H. Darmon, *Heegner points, Stark-Heegner points and values of L-series*, International Congress of Mathematicians. Vol.II, 313–345, Eur. Math. Soc., Zürich, 2006.

[6] J. Fearnley, H. Kisilevsky, M. Kuwata, *Vanishing and non-vanishing Dirichlet twists of L-functions of elliptic curves*, preprint 2008.

[7] B. Mazur, J. Tate: *Refined Conjectures of the Birch and Swinnerton-Dyer Type* , Duke Math.J., **54** (1987), 711–750.

[8] J. S. Milne: Arithmetic Duality Theorems, Second edition, BookSurge, LLC (2006).

[9] J.H. Silverman: The arithmetic of elliptic curves, Springer Verlag (1986).

[10] J.-P. Serre, *Propriété galoisiennes des points d'orde fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.

[11] J.-P. Serre, *Local fields*, Springer Verlag (1979).

Mathematisches Institut der Universität München, Theresienstr. 39, 80333 München, Germany

E-mail address: bley@math.lmu.de