NUMERICAL EVIDENCE FOR THE EQUIVARIANT BIRCH AND SWINNERTON-DYER CONJECTURE (PART II)

WERNER BLEY

ABSTRACT. We continue the study of the Equivariant Tamagawa Number Conjecture for the base change of an elliptic curve begun in [1]. We recall that the methods developed in [1], apart from very special cases, cannot be applied to verify the l-part of the ETNC if l divides the order of the group. In this note we focus on extensions of l-power degree (l an odd prime) and describe methods for computing numerical evidence for ETNC_l. For cyclic l-power extensions we also express the validity of ETNC_l in terms of explicit congruences.

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 rational group ring $\mathbb{Q}[G]$.

In [1] we described an explicit formulation (under certain hypothesis) of the "Equivariant Tamagawa Number Conjecture" for the pair $(M_K, \mathbb{Z}[G])$ and developed algorithmic methods for computing numerical evidence. We recall that the "Equivariant Tamagawa Number Conjecture" is formulated in much greater generality. However, in this manuscript we will exclusively deal with the special case of the base change of an elliptic curve as above. The abbreviation ETNC will always refer to this special case of the conjecture.

It is well known that the ETNC should be an equivariant form of the Birch and Swinnerton-Dyer conjecture (for short BSD). However, this is not obvious from the very general and comparatively abstract formulation of the ETNC in [9]. If $K = \mathbb{Q}$ (so no group is acting), the equivalence of the two conjectures is shown in [18] or [25]. For arbitrary Galois extensions $K/\mathbb{Q}$ one can make use of the notion of refined Euler characteristics introduced in [10] in order to formulate the ETNC as an explicit equality in a relative algebraic K-group which makes the relation to the BSD conjecture transparent. This is the main theoretical result of the manuscript [1], see in particular Proposition 4.4 of loc.cit. However, we had to impose quite strong hypothesis in order to derive this result. The aim of this paper is to relax part of these hypothesis.

Assuming that the Mordell-Weil group $E(K)$ is computable, we showed in loc.cit. how to verify the rationality part of the ETNC up to the precision of the computation. We further described how one can use these computations to numerically verify the l-part of the ETNC for all primes l outside a finite set of difficult primes. This finite set contains in most cases the prime divisors of $\#G$ and $\#Ш(E/K)$

Date: August 2, 2010.

(which we always assume to be finite!). To explain the reason why we had to exclude prime divisors of $\#G$ we recall that the approach of loc.cit. is restricted to the case that certain groups (e.g. the Mordell-Weil group $E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l)$), which occur as cohomology modules of naturally defined perfect complexes, are $\mathbb{Z}_l[G]$-perfect. If $l \nmid \#G$ this condition is always fulfilled because $\mathbb{Z}_l[G]$ is a regular ring. However, if $l \mid \#G$, then there are only some very rare cases where the cohomology modules under consideration are perfect.

In this note we focus on the l-part of the ETNC (for short ETNC_l) for primes l dividing $\#G$. Under certain (quite strong) assumptions on E and K we show that there exists an 'augmented trivialized extension' $\tau = \tau_{\mathbb{Z}_l[G],\mathbb{C}_l}$ of $\mathbb{Z}_l[G]$-modules in the sense of [11] with a trivialisation induced by the Néron-Tate height pairing such that the associated refined Euler characteristic $\chi_{\mathbb{Z}_l[G],\mathbb{C}_l}(\tau)$ vanishes if and only if ETNC_l is valid. This is essentially based on work of Burns in [11].

We briefly recall the definition of an 'augmented trivialized extension' from [11, Sec. 3]. Let Λ be a Dedekind domain of characteristic zero and quotient field F. We fix an extension field E of F, a finite dimensional semisimple F-algebra A and a Λ-order $\mathcal{A}$ in A. Then an augmented E-trivialized extension of $\mathcal{A}$-modules is a triple $\tau = (\epsilon_\tau, \lambda_\tau, \mathcal{L}_\tau^*)$ consisting of a perfect 2-extension $\epsilon_\tau \in \mathrm{Ext}^2_{\mathcal{A}}(H^1_\tau, H^0_\tau)$ of finitely generated $\mathcal{A}$-modules H^0_τ and H^1_τ, an isomorphism $\lambda_\tau : E \otimes_\Lambda H^0_\tau \longrightarrow E \otimes_\Lambda H^1_\tau$ of $E \otimes_F A$-modules and an element $\mathcal{L}_\tau^*$ in the center of $E \otimes_F A$.

In our applications we look for elliptic curves $E/\mathbb{Q}$ and Galois extensions $K/\mathbb{Q}$ such that the validity of ETNC_l can be decided by considering an augmented trivialized extension with $\Lambda = \mathbb{Z}_l, E = \mathbb{C}_l, A = \mathbb{Q}_l[G], \mathcal{A} = \mathbb{Z}_l[G]$ and $H^0_\tau = \mathbb{Z}_l \otimes_{\mathbb{Z}} E(K), H^1_\tau = \mathrm{Hom}_{\mathbb{Z}_l}(\mathbb{Z}_l \otimes_{\mathbb{Z}} E(K), \mathbb{Z}_l) =: (\mathbb{Z}_l \otimes_{\mathbb{Z}} E(K)^*$. The trivialisation $\lambda_\tau := \lambda_{NT}$ is induced by the Néron-Tate height pairing and $\mathcal{L}_\tau^*$ is the leading term $L^*(M_K)$ of the equivariant motivic L-function at $s = 0$. Note that $H^0_\tau, H^1_\tau, \lambda_\tau$ and $\mathcal{L}_\tau^*$ do not depend on the extension class ϵ_τ. The extension class $\epsilon_\tau \in \mathrm{Ext}^2_{\mathbb{Z}_l[G]}(H^1_\tau, H^0_\tau)$ is specified by the ETNC, however, it is not clear how to use this information for explicit numerical experiments.

We therefore adopt the following strategy in this paper. We compute the Ext-group $\mathcal{E}xt := \mathrm{Ext}_{\mathbb{Z}_l[G]}((\mathbb{Z}_l \otimes_{\mathbb{Z}} E(K))^*, \mathbb{Z}_l \otimes_{\mathbb{Z}} E(K))$ and for each extension class $\epsilon \in \mathcal{E}xt$ the refined Euler characteristic $\chi(\tau(\epsilon)) = \chi_{\mathbb{Z}_l[G],\mathbb{C}_l}(\tau(\epsilon))$ associated to $\tau(\epsilon) = (\epsilon, \lambda_{NT}, L^*(M_K))$. In this way we compute an explicit subset

$$\mathcal{C} := \{\chi(\tau(\epsilon)) \mid \epsilon \in \mathcal{E}xt\} \subseteq K_0(\mathbb{Z}_l[G], \mathbb{C}_l).$$

The validity of ETNC_l now predicts that $\mathcal{C}$ is contained in $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors}$ and contains the trivial element. This can be numerically verified by the methods of [5].

If $\mathrm{rk}(E(K)) = 0$ and $l \nmid E(K)_{tors}$, then $\mathcal{E}xt$ is trivial, so that we can numerically verify the full ETNC_l (provided that we assume the rationality conjecture). Of course, in the case $\mathrm{rk}(E(K)) > 0$ it would be very interesting to describe the 'correct' extension class theoretically, but explicitly enough, so that the information can be used to fully verify the l-part of the ETNC numerically.

If G is cyclic of prime power order l^n, l odd, and E satisfies a variety of hypothesis, we are able to define a relatively small subgroup $\mathcal{E}$ of $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)$ and show that ETNC_l is valid modulo $\mathcal{E}$, if and only if $\mathcal{E} = \mathcal{C}$ (see Theorem 4.3). Note that by Proposition 5.4 we have

$$l^{n-1}(l-1) = \#\mathcal{E} << \#K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors} = (l-1)^n l^e \text{ with } e = \frac{l^n - 1}{l - 1} - n.$$

Moreover,we will express the validity of ETNC_l for cyclic groups of prime power order in terms of explicit congruences (see Propostion 5.2).

We recall that ETNC_l modulo $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors}$ is equivalent to ETNC_l for the pair $(M_K, \mathcal{M})$ where $\mathcal{M}$ is a maximal order such that $\mathbb{Z}[G] \subseteq \mathcal{M} \subseteq \mathbb{Q}[G]$. Studying the ETNC in this case is much easier (but still very difficult) because $\mathcal{M}$ is regular so that we do not have to consider questions of perfectness of modules, and consequently, also do not have to use any extension class information. In return, ETNC_l for the pair $(M_K, \mathcal{M})$ will not imply any of the fine explicit congruences predicted by ETNC_l for the pair $(M_K, \mathbb{Z}[G])$.

As in [1] this manuscript mainly deals with the additional difficulties and consequences of equivariant integrality conjectures. We therefore usually assume the rationality conjecture. We recall, however, that there are important results in the literature (without being exhaustive we only mention [16, 19, 20, 21, 26] and recent results of Bertolini and Darmon) from which one can possibly deduce the equivariant rationality conjecture provided that the analytic (equivariant) rank is at most 1. Furthermore we throughout assume that the Tate-Shafarevic group $Ш(E/K)$ is finite. Again it is possible to deduce finiteness of $Ш(E/K)$ in many examples provided that the analytic rank is at most 1 from the above mentioned work.

The structure of this paper is as follows. In Section 2 we describe an algorithm for the computation of Ext-groups $\mathrm{Ext}_{\mathbb{Z}[G]}(H^1, H^0)$ where H^0, H^1 denote finitely generated $\mathbb{Z}[G]$-modules. In Section 3 we show how to compute the refined Euler characteristic associated to augmented trivialized extensions $\tau = (\epsilon, \lambda, \mathcal{L}^*)$ where $\lambda : \mathbb{R} \otimes_{\mathbb{Z}} H^0 \xrightarrow{\simeq} \mathbb{R} \otimes_{\mathbb{Z}} H^1$ is an isomorphism of $\mathbb{R}[G]$-modules, $\mathcal{L}^*$ an element in the center of $\mathbb{R}[G]$ and $\epsilon \in \mathrm{Ext}^2_{\mathbb{Z}[G]}(H^1, H^0)$. By localisation we obtain the set $\mathcal{C}$ from above. In Section 4 we focus on cyclic extensions of l-power degree and explicitly work out the approach sketched in the previous sections. Section 5 is dedicated to the study of explicit congruences which are implied by the triviality of elements of $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)$ for cyclic groups of prime power order l^n. We also compute the order of the torsion subgroup. Finally, in Section 6 we give a brief account of our numerical experiments.

Notations: For a ring R we write $\zeta(R)$ for its center. For a commutative ring Λ and a Λ-module M we write M^* for the Λ-linear dual $\mathrm{Hom}_\Lambda(M, \Lambda)$. For a $\mathbb{Z}_l$-module W we write $W^\vee$ for the Pontriyagin dual $\mathrm{Hom}_{cont}(W, \mathbb{Q}_l/\mathbb{Z}_l)$. If E/Λ is an extension of commutative rings and M a Λ-module, then we often set $M_E := M \otimes_\Lambda E$.

2. Computation of Ext-groups

Let X, Y be finitely generated $\mathbb{Z}[G]$-modules. In this section we describe an algorithm which computes $\mathrm{Ext}^n_{\mathbb{Z}[G]}(X, Y), n \geq 1$, as an abstract finitely generated abelian group.

We assume that X and Y are given in the form

$$\begin{aligned} X &= \mathbb{Z}x_{t,1} \oplus \ldots \oplus \mathbb{Z}x_{t,m} \oplus \mathbb{Z}x_{tf,1} \oplus \ldots \oplus \mathbb{Z}x_{tf,n} \\ Y &= \mathbb{Z}y_{t,1} \oplus \ldots \oplus \mathbb{Z}y_{t,r} \oplus \mathbb{Z}y_{tf,1} \oplus \ldots \oplus \mathbb{Z}y_{tf,s} \end{aligned}$$

with free generators $x_{tf,1}, \ldots, x_{tf,n}, y_{tf,1}, \ldots, y_{tf,s}$ and torsion elements $x_{t,1}, \ldots, x_{t,m}, y_{t,1}, \ldots, y_{t,r}$.

In addition, we assume that the G-action on these generators is explicitly computable. It is then straightforward to write down a naive algorithm which computes a short exact sequence

$$0 \longrightarrow R \longrightarrow \mathbb{Z}[G]^k \longrightarrow X \longrightarrow 0 \tag{1}$$

for any $\mathbb{Z}[G]$-module X given in the above form. Furthermore, R can again be described by a set of $\mathbb{Z}$-generators with explicit G-action. Hence we can compute n-syzygies of modules X as above for all $n \geq 1$. Note, however, that it is not clear how to compute a presentation of the form (1) with small or even minimal k. We will not discuss this problem in this manuscript.

We compute once and for all an n-syzygy

$$0 \longrightarrow Z \stackrel{\iota}{\longrightarrow} F^0 \longrightarrow F^1 \longrightarrow \cdots \longrightarrow F^{n-1} \longrightarrow X \longrightarrow 0$$

with finitely generated free $\mathbb{Z}[G]$-modules $F^0, \ldots, F^{n-1}$ and a finitely generated $\mathbb{Z}[G]$-module Z. Then, e.g. by [12, (8.3)],

$$\mathrm{Ext}^n_{\mathbb{Z}[G]}(X, Y) \simeq \mathrm{Hom}_{\mathbb{Z}[G]}(Z, Y)/\iota^* \left(\mathrm{Hom}_{\mathbb{Z}[G]}(F^0, Y)\right)$$

and we will explicitly describe how the right hand side can be computed as a finitely generated abelian group.

We compute a resolution

$$0 \longrightarrow R \longrightarrow \mathbb{Z}[G]^k \longrightarrow Z \longrightarrow 0$$

and let R_0 denote a finite $\mathbb{Z}$-generating set for R. Each $\varphi \in \mathrm{Hom}_{\mathbb{Z}[G]}(Z, Y)$ is uniquely determined by the images $y_i := \varphi(w_i + R)$, $i = 1, \ldots, k$, where we write $w_1, \ldots, w_k$ for the canonical $\mathbb{Z}[G]$-basis of $\mathbb{Z}[G]^k$. Conversely, a set $\{y_1, \ldots, y_k\}$ determines a map φ, if and only if $\varphi(\rho) = 0$ for all $\rho \in R_0$. If we set

$$\rho = \sum_{i=1}^k \lambda_i^{(\rho)} w_i \text{ with } \lambda_i^{(\rho)} \in \mathbb{Z}[G],$$

then

$$\varphi(\rho) = \varphi\left(\sum_{i=1}^k \lambda_i^{(\rho)} w_i\right) = \sum_{i=1}^k \lambda_i^{(\rho)} y_i.$$

Let $y_i = \sum_{j=1}^r a_{ij} y_{t,j} + \sum_{j=1}^s b_{ij} y_{tf,j}$ with $a_{ij}, b_{ij} \in \mathbb{Z}$. Note that the a_{ij} are only determined modulo $\mathrm{ord}(y_{t,j})$ by y_i. Then

$$\begin{aligned}
0 &= \varphi(\rho) = \sum_{i=1}^k \lambda_i^{(\rho)} y_i = \sum_{i=1}^k \left(\sum_{j=1}^r a_{ij} \lambda_i^{(\rho)} y_{t,j} + \sum_{j=1}^s b_{ij} \lambda_i^{(\rho)} y_{tf,j} \right) \\
&= \sum_{i=1}^k \left(\sum_{j=1}^r a_{ij} \sum_{q=1}^r c_{ijq}^{(\rho)} y_{t,q} + \sum_{j=1}^s b_{ij} \left(\sum_{q=1}^r d_{ijq}^{(\rho)} y_{t,q} + \sum_{q=1}^s e_{ijq}^{(\rho)} y_{tf,q} \right) \right) \\
&= \sum_{q=1}^r \left(\sum_{i=1}^k \sum_{j=1}^r a_{ij} c_{ijq}^{(\rho)} + \sum_{i=1}^k \sum_{j=1}^s b_{ij} d_{ijq}^{(\rho)} \right) y_{t,q} + \\
&\quad \sum_{q=1}^s \left(\sum_{i=1}^k \sum_{j=1}^s b_{ij} e_{ijq}^{(\rho)} \right) y_{tf,q}
\end{aligned}$$

where for $\rho \in R_0$ and $i = 1, \ldots, k$,

$$\lambda_i^{(\rho)} y_{t,j} = \sum_{q=1}^{r} c_{ijq}^{(\rho)} y_{t,q},$$
$$\lambda_i^{(\rho)} y_{tf,j} = \sum_{q=1}^{r} d_{ijq}^{(\rho)} y_{t,q} + \sum_{q=1}^{s} e_{ijq}^{(\rho)} y_{tf,q}.$$

Equating coefficients we obtain the equivalent system of linear congruences and equations

$$\sum_{i=1}^{k}\sum_{j=1}^{r} a_{ij} c_{ijq}^{(\rho)} + \sum_{i=1}^{k}\sum_{j=1}^{s} b_{ij} d_{ijq}^{(\rho)} \equiv 0 (\mathrm{mod}\ \mathrm{ord}(y_{t,q})), \quad 1 \le q \le r, \rho \in R_0,$$
$$\sum_{i=1}^{k}\sum_{j=1}^{s} b_{ij} e_{ijq}^{(\rho)} = 0, \quad 1 \le q \le s, \rho \in R_0.$$

Let $\mathcal{W}$ denote the set of solutions for the vectors $(a_{ij}, b_{ij})^t \in \mathbb{Z}^{kr+ks}$. Then $\mathcal{W}$ is of the form

$$\mathcal{W} = \mathbb{Z}\begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \oplus \ldots \oplus \mathbb{Z}\begin{pmatrix} a_m \\ b_m \end{pmatrix}, \quad m \ge 0, \quad a_l \in \mathbb{Z}^{kr}, b_l \in \mathbb{Z}^{ks}, l = 1, \ldots, m.$$

Consider $\mathcal{W}_0 = \langle (e_{ij}, 0)^t, 1 \le i \le k, 1 \le j \le r \rangle_{\mathbb{Z}}$ with

$$e_{ij} = (\underbrace{0, \ldots, 0}, \ldots, \underbrace{0, \ldots, 0, m_j, 0, \ldots, 0}_{i-\text{th component}}, \ldots, \underbrace{0, \ldots, 0})^t \in \mathbb{Z}^{kr},$$

where the only non zero entry is in the i-th component and is given by $m_j = \mathrm{ord}(y_{t,j})$ at the j-th position. Then $(e_{ij}, 0)^t$ corresponds to $y_i = 0$, so clearly $\mathcal{W}_0 \subseteq \mathcal{W}$. The quotient $\mathcal{W}/\mathcal{W}_0$, which can be computed by [13, Alg. 4.1.7], and is easily shown to represent $\mathrm{Hom}_{\mathbb{Z}[G]}(Z, Y)$.

Finally we have to compute the submodule $\iota^*(\mathrm{Hom}_{\mathbb{Z}[G]}(F^0, Y))$. Since F^0 is a free $\mathbb{Z}[G]$-module, say $F^0 \simeq \mathbb{Z}[G]^l$, we obtain $\mathrm{Hom}_{\mathbb{Z}[G]}(F^0, Y)) \simeq Y^l$. So we may assume that $\mathrm{Hom}_{\mathbb{Z}[G]}(F^0, Y))$ is given by a finite set of $\mathbb{Z}$-generators Ψ. Then for each $\psi \in \Psi$ the homomorphism $\iota^*(\psi) = \psi \circ \iota$ can be identified with an element of $\mathcal{W}/\mathcal{W}_0$ (by computing discrete logarithms as described after [13, Alg. 4.1.7]) and again using [13, Alg. 4.1.7] we determine the quotient $(\mathcal{W}/\mathcal{W}_0)/\langle\Psi\rangle$ which by construction is isomorphic to $\mathrm{Ext}^n_{\mathbb{Z}[G]}(X, Y)$.

3. Computation of refined Euler characteristics

The main references for this section are [10] and [11, Sec. 3].

Let H^0, H^1 be finitely generated $\mathbb{Z}[G]$-modules such that there exists an $\mathbb{R}[G]$-isomorphism $\lambda : \mathbb{R}\otimes_{\mathbb{Z}} H^0 \longrightarrow \mathbb{R}\otimes_{\mathbb{Z}} H^1$. In addition, we fix an element $\mathcal{L}^* \in \zeta(\mathbb{R}[G])$. Then, for each perfect extension class $\epsilon \in \mathrm{Ext}^2_{\mathbb{Z}[G]}(H^1, H^0)$, the triple $\tau_\epsilon = (\epsilon, \lambda, \mathcal{L}^*)$ is an augmented $\mathbb{R}$-trivialized extension of $\mathbb{Z}[G]$-modules. We let $\chi(\tau_\epsilon) = \chi_{\mathbb{Z}[G],\mathbb{R}}(\tau_\epsilon)$ denote the refined Euler characteristic defined in [11, Sec. 3.1]. Our aim is to combine the computation of $\mathrm{Ext}^2_{\mathbb{Z}[G]}(H^1, H^0)$ with methodes developed in [5] to compute the set

$$\mathcal{C} = \mathcal{C}(H^0, H^1, \lambda, \mathcal{L}^*) := \left\{ \chi_{\mathbb{Z}[G],\mathbb{R}}(\tau_\epsilon) \mid \epsilon \in \mathrm{Ext}^2_{\mathbb{Z}[G]}(H^1, H^0) \text{ perfect } \right\} \subseteq K_0(\mathbb{Z}[G], \mathbb{R}).$$

Recall that $\epsilon \in \mathrm{Ext}^2_{\mathbb{Z}[G]}(H^1, H^0)$ is perfect, if it can be represented as a Yoneda extension by an exact sequence

$$0 \longrightarrow H^0 \longrightarrow M^0 \longrightarrow M^1 \longrightarrow H^1 \longrightarrow 0$$

with perfect $\mathbb{Z}[G]$-modules M^0 and M^1.

Actually, when considering the integrality part of the ETNC we will work prime by prime. Let l be a prime and let $\mathbb{C}_l$ denote the completion of a fixed algebraic closure of $\mathbb{Q}_l$. For every embedding $j : \mathbb{R} \longrightarrow \mathbb{C}_l$ we obtain induced maps $j_* : K_0(\mathbb{Z}[G], \mathbb{R}) \longrightarrow K_0(\mathbb{Z}_l[G], \mathbb{C}_l)$ and $j_* : \zeta(\mathbb{R}[G]) \longrightarrow \zeta(\mathbb{C}_l[G])$. We are then interested in the set $\mathcal{C}_{l,j} := j_*(\mathcal{C})$. Note that

$$\mathcal{C}_{l,j} = \left\{ \chi_{\mathbb{Z}_l[G],\mathbb{C}_l}\left(\epsilon_l, \lambda_{l,j}, j_*(\mathcal{L}^*)\right) \mid \epsilon_l \in \mathrm{Ext}^2_{\mathbb{Z}_l[G]}(\mathbb{Z}_l \otimes_{\mathbb{Z}} H^1, \mathbb{Z}_l \otimes_{\mathbb{Z}} H^0) \text{ perfect } \right\}$$

where

$$\mathbb{C}_l \otimes_{\mathbb{R},j} (\mathbb{R} \otimes_{\mathbb{Z}} H^0) \simeq \mathbb{C}_l \otimes_{\mathbb{Z}} H^0 \xrightarrow{\lambda_{l,j}} \mathbb{C}_l \otimes_{\mathbb{Z}} H^1 \simeq \mathbb{C}_l \otimes_{\mathbb{R},j} (\mathbb{R} \otimes_{\mathbb{Z}} H^1)$$

is induced by λ.

Recall also that for finitely generated $\mathbb{Z}[G]$-modules H^0 and H^1 one has

$$\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathrm{Ext}^2_{\mathbb{Z}[G]}(H^1, H^0) \simeq \mathrm{Ext}^2_{\mathbb{Z}_l[G]}(\mathbb{Z}_l \otimes_{\mathbb{Z}} H^1, \mathbb{Z}_l \otimes_{\mathbb{Z}} H^0), \tag{2}$$

$$\mathrm{Ext}^2_{\mathbb{Z}[G]}(H^1, H^0) \simeq \bigoplus_{l \mid \#G} \mathrm{Ext}^2_{\mathbb{Z}_l[G]}(\mathbb{Z}_l \otimes_{\mathbb{Z}} H^1, \mathbb{Z}_l \otimes_{\mathbb{Z}} H^0). \tag{3}$$

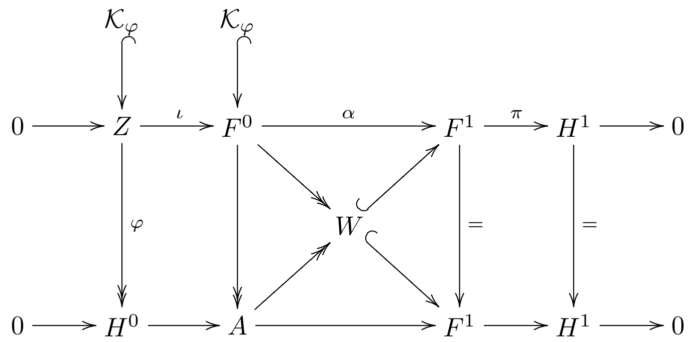
By (2) we can use the computational approach of Section 2 in order to compute $\mathrm{Ext}^2_{\mathbb{Z}_l[G]}(\mathbb{Z}_l \otimes_{\mathbb{Z}} H^1, \mathbb{Z}_l \otimes_{\mathbb{Z}} H^0)$. In the following we therefore assume that $\Lambda = \mathbb{Z}$ or $\mathbb{Z}_l$, H^0 and H^1 are finitely generated $\Lambda[G]$-modules and either $\lambda : H^0_{\mathbb{R}} \longrightarrow H^1_{\mathbb{R}}$ or $\lambda : H^0_{\mathbb{C}_l} \longrightarrow H^1_{\mathbb{C}_l}$.

We fix a 2-syzygy

$$0 \longrightarrow Z \xrightarrow{\iota} F^0 \xrightarrow{\alpha} F^1 \xrightarrow{\pi} H^1 \longrightarrow 0$$

and compute $\mathrm{Ext}^2_{\Lambda[G]}(H^1, H^0)$ as described in Section 2. So each element $\epsilon \in \mathrm{Ext}^2_{\Lambda[G]}(H^1, H^0)$ is represented by a $\Lambda[G]$-homomorphism $\varphi : Z \longrightarrow H^0$. Without loss of generality we may assume that φ is onto. We set $\mathcal{K}_\varphi := \ker(\varphi)$ and obtain a diagram of the form

(4)



with $W := \ker(\pi)$ and A denoting the pushout along ι and φ. We write $\epsilon(\varphi) \in \mathrm{Ext}_{\Lambda[G]}(H^1, H^0)$ for the 2-extension represented by the bottom exact sequence.

We recall that a finitely generated Λ-torsion free Λ-module is $\Lambda[G]$-projective, if and only if it is G-cohomologically trivial (which we abbreviate by c.t. in the following). It follows that any finitely generated c.t. $\Lambda[G]$-module is of projective dimension at most 2, in particular, each such module is perfect.

Lemma 3.1. *$\epsilon(\varphi)$ is a perfect 2-extension, if and only if $\mathcal{K}_\varphi$ is $\Lambda[G]$-projective (or equivalently, G-c.t.).*

Proof. If $\mathcal{K}_\varphi$ is c.t., then the long exact sequence of Galois cohomology implies that A is also c.t.. Conversely, if $\epsilon(\varphi)$ is perfect, then $\epsilon(\varphi)$ induces an isomorphism $H^i(G, H^1) \longrightarrow H^{i+2}(G, H^0)$ in all degrees of cohomology. This implies that A is c.t. and again from the long exact sequence of Galois cohomology we deduce the cohomological triviality of $\mathcal{K}_\varphi$. □

In order to select the extension classes which are perfect we need a method to decide whether $\mathcal{K}_\varphi$ is $\Lambda[G]$-projective. From our algorithm in Section 2 we obtain $\mathbb{Z}[G]$-homomorphisms $\varphi : Z \longrightarrow H^0$ representing the extension classes of $\mathrm{Ext}_{\mathbb{Z}[G]}(H^1, H^0)$. Hence we can compute the $\mathbb{Z}[G]$-module $\mathcal{K}_\varphi$. We recall from [12, Theorem (32.11)] that a finitely generated $\mathbb{Z}[G]$-module is projective, if and only if it is locally free. Similary, if $l \mid \#G$, then the $\mathbb{Z}_l[G]$-module $\mathbb{Z}_l \otimes_{\mathbb{Z}} \mathcal{K}_\varphi$ is projective, if and only if it is $\mathbb{Z}_l[G]$-free. This follows from [12, Theorem (32.1)] together with the fact that $\mathbb{Q}_l \otimes_{\mathbb{Z}} \mathcal{K}_\varphi \simeq \mathbb{Q}_l[G]^m$ with $m = \dim(\mathbb{Q}_l \otimes_{\mathbb{Z}} F^1) - \dim(\mathbb{Q}_l \otimes_{\mathbb{Z}} F^0)$ (which, in turn, follows from diagram (4) or (5) below). Finally, if p is a rational prime such that $p \nmid \#G$, then $\mathbb{Z}_p[G]$ is regular and each finitely generated $\mathbb{Z}_p$-free $\mathbb{Z}_p[G]$-module is actually projective.

For the prime divisors p of $\#G$ (or for $p = l$ if $\Lambda = \mathbb{Z}_l$) we therefore apply the algorithm of [5, Sec. 4.2]. This algorithm either detects that $\mathcal{K}_\varphi$ is not locally free at p or computes a $\mathbb{Z}_p[G]$-basis. Alternatively we combine the algorithms of D.Holt which are already implemented in MAGMA [22] with [23, IX, Th. 8] to decide whether $\mathcal{K}_\varphi$ is c.t.. However, for our purposes the former method is preferable since we anyway need the local basis for the computation of the refined Euler characteristics.

Let E denote either $\mathbb{R}$ or $\mathbb{C}_l$. Let $\delta : \zeta(E[G])^\times \longrightarrow K_0(\Lambda[G], E)$ denote the extended boundary homomorphism introduced in [9, Sec. 4.2] or [7, Lemma 2.1]. Let $\epsilon(\varphi)$ be the perfect 2-extension represented by the bottom row of diagram (4) and set $\tau(\varphi) := (\epsilon(\varphi), \lambda, \mathcal{L}^*)$. Adapting the proof of [11, Lemma 3.2(i)] one can show that the refined Euler characteristic associated to $\tau(\varphi)$ is given by

$$\chi_{\Lambda[G],E}(\tau(\varphi)) = [F^0, \lambda(\varphi)_{triv}, F^1 \oplus \mathcal{K}_\varphi] - \delta(\mathcal{L}^*) \in K_0(\Lambda[G], E)$$

where $\lambda(\varphi)_{triv}$ is the composite

$$\begin{aligned} F^0_E &\xrightarrow{\sigma_1} W_E \oplus Z_E \xrightarrow{\sigma_2} W_E \oplus H^0_E \oplus \mathcal{K}_{\varphi,E} \\ &\xrightarrow{\sigma_3} W_E \oplus H^1_E \oplus \mathcal{K}_{\varphi,E} \xrightarrow{\sigma_4} F^1_E \oplus \mathcal{K}_{\varphi,E}. \end{aligned} \qquad (5)$$

Here σ_1 is induced by choosing a splitting of $0 \longrightarrow Z_E \xrightarrow{\iota} F^0_E \longrightarrow W_E \longrightarrow 0$, σ_2 by choosing a splitting of $0 \longrightarrow \mathcal{K}_{\varphi,E} \longrightarrow Z_E \xrightarrow{\varphi} H^0_E \longrightarrow 0$, σ_4 by choosing a splitting of $0 \longrightarrow W_E \longrightarrow F^1_E \xrightarrow{\pi} H^1_E \longrightarrow 0$ and, finally, σ_3 by λ. It is worth mentioning that $\chi_{\Lambda[G],E}(\tau(\varphi))$ does not depend on any of the choices made in the construction of diagram (4) or the choices of the splittings in the definition of $\lambda(\varphi)_{triv}$.

4. ETNC for cyclic extensions

Let E be an elliptic curve defined over $\mathbb{Q}$ and K a finite Galois extension with group G. We always assume that the Tate-Shafarevic group $Ш(E/K)$ of E over

K is finite. We write d_K for the discriminant of $K/\mathbb{Q}$ and N_E for the conductor of E. For a number field F we write G_F for the absolute Galois group. We let $T_l(E) := \varprojlim E[l^n]$ denote the l-adic Tate module of E and view $T_l(E)$ as a G_K-module. We set $T_l := \mathrm{ind}_{G_K}^{G_{\mathbb{Q}}}(T_l(E))$ and define

$$V_l(E) := T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l, \quad V_l := T_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

Let $S_{ram}(K/\mathbb{Q})$ be the set of primes which ramify in $K/\mathbb{Q}$ and $S_{bad}(E)$ the set of primes where E has bad reduction. We put $S := S_{ram}(K/\mathbb{Q}) \cup S_{bad}(E)$ and for a fixed prime l we set $S_l := S \cup \{l\}$.

For each absolutely irreducible character $\psi \in \mathrm{Irr}(G)$ we write $L(E/\mathbb{Q}, \psi, s)$ for the twisted Hasse-Weil-L-function. Assuming that $L(E/\mathbb{Q}, \psi, s)$ has meromorphic continuation to the complex plane we let $L^*(E/\mathbb{Q}, \psi, 1)$ denote the leading coefficient in its Taylor expansion at $s = 1$. We set $\mathcal{L}^* := \left(L^*(E/\mathbb{Q}, \bar{\psi}, 1)\right)_{\psi \in \mathrm{Irr}(G)}$ and recall (for example, from [1, page 17]) that $\mathcal{L}^* = L^*(M_K)$.

We consider the complex

$$(T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Z}_l[G]^*)^{I_p} \stackrel{1-Fr_p^{-1}}{\longrightarrow} (T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Z}_l[G]^*)^{I_p} \tag{6}$$

with the non-trivial modules placed in degrees 0 and 1. If $(T_l(E) \otimes_{\mathbb{Z}_l} \mathbb{Z}_l[G]^*)^{I_p}$ is $\mathbb{Z}_l[G]$-perfect, then by [1, Rem. 3.2] the refined Euler characteristic associated with the above complex is given by $(L_p(E, \bar{\chi}, 1))_{\chi \in \mathrm{Irr}(G)}$. Furthermore, we have

$$\det\left(1 - Fr_p^{-1} \mid (V_l(E) \otimes_{\mathbb{Q}_l} \mathbb{Q}_l[G]^*)^{I_p}\right) = (L_p(E, \bar{\chi}, 1))_{\chi \in \mathrm{Irr}(G)}.$$

As in [1, page 19] we write $\mathrm{Reg} = \left(\mathrm{Reg}_\psi\right)_{\psi \in \mathrm{Irr}(G)}$ for the equivariant regulator, $R = (R_\psi)_{\psi \in \mathrm{Irr}(G)}$ for the vector of resolvents and $\Omega = (\Omega_\psi)_{\psi \in \mathrm{Irr}(G)}$ for the vector of periods. In this notation the equivariant periods are given by $R^{-1}\Omega$ (see [1, Prop. 3.1]). If we set $u := \frac{\mathcal{L}^* R}{\Omega \mathrm{Reg}}$, then the rationality part of the ETNC is equivalent to the statement $u \in \zeta(\mathbb{Q}[G])^\times$. Note that if $E(K)$ is explicitly known, then we can compute numerical approximations to u.

In Section 4 of [1] we developed methods to compute numerical evidence for the integrality part of the ETNC assuming the validity of the rationality conjecture and that $u \in \zeta(\mathbb{Q}[G])^\times$ is explicitly known. We showed that the precise knowledge of u can be used to prove the l-part of the integrality conjecture for almost all primes l.

We briefly recall the approach of loc. cit. The ETNC_l is formulated in terms of a perfect complex $R\Gamma_c(\mathbb{Z}_{S_l}, T_l)$ (see [9, Sec. 3.2-3.4]). To analyse this complex and to explicitly compute its cohomology one usually tries to define perfect complexes $R\Gamma_f(\mathbb{Q}, T_l)$ and $R\Gamma_f(\mathbb{Q}_p, T_l)$ for each $p \in S_l \cup \{\infty\}$ such that one has a true triangle

$$R\Gamma_c(\mathbb{Z}_{S_l}, T_l) \longrightarrow R\Gamma_f(\mathbb{Q}, T_l) \longrightarrow \bigoplus_{p \in S_l \cup \{\infty\}} R\Gamma_f(\mathbb{Q}_p, T_l).$$

This approach is motivated by work of Bloch and Kato and carried out in [8, Sec. 1.5.1] by Burns and Flach. However, if l divides $\#G$, it is not clear that it is always possible to define the complexes $R\Gamma_f(\mathbb{Q}, T_l)$ and $R\Gamma_f(\mathbb{Q}_p, T_l)$ so that they are perfect (see the comment at the beginning of Sec. 1.5.1 of [8]). For that reason one is forced to introduce additional hypothesis which do not occur in the general statement of the ETNC.

For a finite place v of K we write $\mathcal{O}_{K_v}$ for the valuation ring in the completion K_v and $\mathfrak{m}_v$ for the maximal ideal. Let $k_v := \mathcal{O}_{K_v}/\mathfrak{m}_v$ denote the residue class field.

We write $E_0(K_v)$ for the points of $E(K_v)$ which reduce to a non-singular point on the reduced curve $\bar{E}(k_v)$. Let $\bar{E}_{ns}(k_v)$ denote the group of non-singular points of $\bar{E}(k_v)$.

For the approach in [1] we used the following hypothesis.

Hypothesis:

(H0) $Ш(E/K)$ is finite.
(H1) l is at most tamely ramified in $K/\mathbb{Q}$.
(H2) (a) If $l \in S$ or $l = 2$, then $l \nmid \#G$.
(b) If $l \notin S$ and $l \neq 2$, then $l \nmid \bar{I}_p$ for all $p \in S$.
(H3) $S_{bad}(E) \cap S_{ram}(K/\mathbb{Q}) = \emptyset$.
(H4) If $l \mid \#G$, then
(a) $E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l$, $(E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l)^*$ are $\mathbb{Z}_l[G]$-perfect and $l \nmid \#E(K)_{tors}$.
(b) $l \nmid \#Ш(E/K)$.
(H5) If $l \notin S$ and $l \neq 2$, then $l \nmid \#(E(K_v)/E_0(K_v))$ for all $v \in S(K)$.

Not that only (H2) and (H3) were needed to show that the complexes $R\Gamma_f(\mathbb{Q}, T_l)$ and $R\Gamma_f(\mathbb{Q}_p, T_l)$ are perfect (see [1, Lemma 4.1]). Hypothesis (H1), (H4) and (H5) guaranteed that all of the cohomology groups of the complexes $R\Gamma_f(\mathbb{Q}, T_l)$ and $R\Gamma_f(\mathbb{Q}_p, T_l)$ were perfect. By [9, Prop. 2.1 (4)] we can therefore work entirely with the cohomology modules and avoid the numerical computation of the complexes. However, the above hypothesis force to exclude finitely many primes l from our considerations.

In this note we will relax part of (H4). For prime divisors l of $\#G$ the condition on the cohomolgy groups of $R\Gamma_f(\mathbb{Q}, T_l)$ forced $\mathrm{rk}(E(K)) = 0$, or in other words, our hypothesis forced to exclude prime divisors l of $\#G$ whenever E/K has non-trivial Mordell-Weil rank.

We write N_E for the conductor of $E/\mathbb{Q}$ and d_K for the discriminant of K. We let $c_p(E, \mathbb{Q})$ denote the Tamagawa factors introduced in [11, Sec. 12.1].

We will combine the approach of [1] with Proposition 4.3.1 of [11]. To that end we replace or hypothesis (H1)-(H5) by condition (B) of [11], explicitly

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

Recall from [17, Exp. IX, (11.3.8)] that (v) holds if all of the usual Tamagawa numbers for E/K are coprime with l.

For the definition of the complexes $R\Gamma_f(\mathbb{Q}_p, T_l)$ we refer the reader to [11, Sec. 12]. Note that by [11, Rem. 12.4.2] this definition essentially coincides with the definitions of [1]. We can still compute elements u_l and ξ_l as in [1, Prop. 4.4], however, there are some changes in the computation which we indicate in the following. The changes concern the computation of the Euler characteristics

a) $\chi_{\mathbb{Z}_l[G], \mathbb{C}_l}(R\Gamma_f(\mathbb{Q}, T_l), \lambda_{NT}^{-1})$,
b) $\chi_{\mathbb{Z}_l[G], \mathbb{C}_l}(R\Gamma_f(\mathbb{Q}_p, T_l), 0)$ for $p \neq l, \infty$,

Note that the λ_{NT} was denoted by δ in [1].

We first look at b). Hypothesis (ii) and (iv) imply $l \notin S$. If $p \notin S_{ram}(K/\mathbb{Q})$, then the definitions of $R\Gamma_f(\mathbb{Q}_p, T_l)$ in [11, Sec. 12.2] and [1, Sec. 4] coincide. Explicitly,

$R\Gamma_f(\mathbb{Q}_p, T_l)$ is given by the complex (6) and the refined Euler characteristic is $(L_p(E/\mathbb{Q}, \bar\chi, 1))_{\chi\in \mathrm{Irr}(G)}$. Assuming (H2)(b) the same is true for all $p \in S$.

On the other hand, if $p \in S_{ram}(K/\mathbb{Q})$, then l violates (H2)(b) and the computation in [1] is no longer valid. In contrast, by [11, Lemma 12.2.2] $R\Gamma_f(\mathbb{Q}_p, T_l)$ as defined in [11] is perfect, and in fact, the proof shows that as a consequence of (iii) $R\Gamma_f(\mathbb{Q}_p, T_l)$ is actually acyclic. Therefore the refined Euler characteristic $\chi_{\mathbb{Z}_l[G],\mathbb{C}_l}(R\Gamma_f(\mathbb{Q}_p, T_l), 0)$ is trivial in this case.

Recall the definition of ξ_l in [1, Prop. 4.4] and its proof. Assuming (H2)(b) the Euler factors arising from $R\Gamma_f(\mathbb{Q}_p, T_l)$ cancelled with Euler factors arising from certain identifications made in [9] for all $p \in S$.

Assuming our hypothesis (i)-(v) instead of (H0)-(H5) the Euler factors for $p \in S_{ram}(K/\mathbb{Q})$ survive and we have to set

$$\xi_l := \prod_{p\in S_{ram}(K/\mathbb{Q})} (L_p(E, \bar\chi, 1))^{-1}_{\chi\in\mathrm{Irr}_{\mathbb{Q}}(G)}$$

where $L_p(E, \chi, 1)$ denotes the local Euler factor at $s = 1$. Indeed, since by assumption $l \nmid \#E(K)_{tors}$ and $l \nmid \#Ш(E/K)$ the ξ_l of [1, Prop. 4.4] is trivial and we just obtain the Euler factors as explained above. Note that we did not use (v) for this computation.

We now turn to the computation of the Euler characteristic in a). In principle we could work in the generality of [11], but for simplicity we introduce the additional hypothesis

(vi) $G = \langle g_0\rangle$ is cyclic of order l^n, $n > 0$,
(vii) $\mathrm{rk}_{\mathbb{Z}} E(K) = \mathrm{rk}_{\mathbb{Z}} E(\mathbb{Q})$,
(viii) $l \nmid \#Ш(E/K)$.

Lemma 4.1. *We assume (i) - (viii). Then* $E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l = E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Z}_l$.

Proof. Since G is a l-group condition (iii) implies that $l \nmid \#E(K)_{tors}$. Therefore $E(K)\otimes_{\mathbb{Z}}\mathbb{Z}_l$ and $E(\mathbb{Q})\otimes_{\mathbb{Z}}\mathbb{Z}_l$ are both torsion free. By the elementary divisor theorem we may find $\mathbb{Z}_l$-basis $P_1, \dots, P_r$ of $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ and $Q_1, \dots, Q_r$ of $E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ such that

$$P_i = l^{n_i} Q_i \text{ with } 0 \le n_1 \le n_2 \le \ldots \le n_r.$$

For each $\sigma \in G$ and each i one then has $l^{n_i}(Q_i^\sigma - Q_i) = 0$, and therefore $Q_i^\sigma = Q_i$. This implies $Q_i \in E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Z}_l$. □

The following should be considered as a variant of [11, Prop. 4.3.1]. The Euler characteristic $\chi_{\mathbb{Z}_l[G],\mathbb{C}_l}(R\Gamma_f(\mathbb{Q}, T_l), \lambda_{NT}^{-1})$ was computed in [1, Lemma 4.2] under the assumption (H0) - (H5). As in [1, Sec. 4.2] we see that by our new assumptions (i) - (viii) the only non trivial cohomolgy groups of $R\Gamma_f(\mathbb{Q}, T_l)$ are given by

$$H^1_f(\mathbb{Q}, T_l) \simeq E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l, \quad H^2_f(\mathbb{Q}, T_l) \simeq (E(K) \otimes_{\mathbb{Z}} \mathbb{Z}_l)^*.$$

Since $H^1_f(\mathbb{Q}, T_l)$ and $H^2_f(\mathbb{Q}, T_l)$ are no longer assumed to be perfect, the computation of $\chi_{\mathbb{Z}_l[G],\mathbb{C}_l}(R\Gamma_f(\mathbb{Q}, T_l), \lambda_{NT}^{-1})$ has to change.

We set $H^0 := E(K)$, $H^1 := E(K)^*$, $H^0_l := H^0 \otimes_{\mathbb{Z}} \mathbb{Z}_l$ and $H^1_l := H^1 \otimes_{\mathbb{Z}} \mathbb{Z}_l$. From general theory we know that the shifted complex $R\Gamma_f(\mathbb{Q}, T_l)[1]$ can be represented by a perfect 2-extension ϵ_0 of H^1_l by H^0_l. Consider the augmented trivialized extension $\tau = (\epsilon_0, \lambda_{NT}, 1)$. Then

$$\chi_{\mathbb{Z}_l[G],\mathbb{C}_l}(R\Gamma_f(\mathbb{Q}, T_l), \lambda_{NT}^{-1}) = \chi_{\mathbb{Z}_l[G],\mathbb{C}_l}(\tau).$$

We recall that 2-extensions of H_l^1 by H_l^0 are parametrized by $\mathrm{Ext}^2_{\mathbb{Z}_l[G]}(H_l^1, H_l^0)$.

We first consider the case $\mathrm{rk}(E(K)) = 0$. Then the Ext-group is obviously trivial. We set

$$u_l := \frac{\mathcal{L}^* R}{\Omega}.$$

Then the l-part of the ETNC is valid, if and only if $u_l = \xi_l$. We can fully verify the l-part of the ETNC in this case.

If $\mathrm{rk}(E(K)) > 0$ we are not able to pin down the extension class ϵ_0 more concretely and therefore will compute the refined Euler characteristic for all augmented trivialized 2-extensions $\tau = (\epsilon, \lambda_{NT}, \mathcal{L}^*)$, $\epsilon \in \mathrm{Ext}_{\mathbb{Z}_l[G]}(H_l^1, H_l^0)$ perfect.

By the methods introduced in Section 2 we could do this without assuming (vi) and (vii), however, with these assumptions we can do a little better. We fix a $\mathbb{Z}$-basis $P_1, \dots, P_r$ of $E(\mathbb{Q})_{tf}$ and write $P_1^*, \dots, P_r^*$ for the dual basis (i.e. $P_i^*(P_j) = \delta_{ij}$). By Lemma 4.1 we may identify the modules H_l^0 and H_l^1 with ${\mathbb{Z}_l}^r$ by this choice of basis.

We set $N_G := \sum_{g \in G} g$ and consider the standard exact sequence

$$\begin{array}{ccccccccccc} 0 & \longrightarrow & \mathbb{Z}_l & \xrightarrow{N_G} & \mathbb{Z}_l[G] & & \xrightarrow{\quad g_0-1 \quad} & & \mathbb{Z}_l[G] & \xrightarrow{aug} & \mathbb{Z}_l \longrightarrow 0 \\ & & & & & \searrow & & \nearrow & & & \\ & & & & & & W & & & & \end{array} \tag{7}$$

with $W = \mathbb{Z}_l[G](g_0 - 1)$. Let $e_0 = \frac{1}{\#G} N_G$ and $e_1 = 1 - e_0$. Then $W_{\mathbb{Q}_l} = \mathbb{Q}_l[G]e_1$ and we have a splitting of $\mathbb{Q}_l[G] \longrightarrow W_{\mathbb{Q}_l} = \mathbb{Q}_l[G]e_1$ defined by $e_1 \mapsto \frac{1}{g_0-1} e_1$. This splitting induces the isomorphism

$$\mathbb{Q}_l[G] \simeq \mathbb{Q}_l \oplus W_{\mathbb{Q}_l}, \quad 1 \mapsto (\frac{1}{\#G}, g_0 - 1). \tag{8}$$

For the splitting of $\mathbb{Q}_l[G] \xrightarrow{aug} \mathbb{Q}_l$ we use $1 \mapsto e_0$. Then

$$\mathbb{Q}_l[G] \simeq \mathbb{Q}_l \oplus W_{\mathbb{Q}_l}, \quad 1 \mapsto (1, e_1). \tag{9}$$

We take r copies of the sequence (7) and use this to compute $\mathrm{Ext}^2_{\mathbb{Z}_l[G]}(H_l^1, H_l^0)$. For each map $\varphi \in \mathrm{Hom}_{\mathbb{Z}_l[G]}({\mathbb{Z}_l}^r, {\mathbb{Z}_l}^r)$ we obtain a commutative diagram of the form

$$\begin{CD} @. @. @. @. H_l^1 @. \\ @. @. @. @. @VV{\simeq}V @. \\ 0 @>>> {\mathbb{Z}_l}^r @>{\oplus N_G}>> \mathbb{Z}_l[G]^r @>{\oplus(g_0-1)}>> \mathbb{Z}_l[G]^r @>{\oplus aug}>> {\mathbb{Z}_l}^r @>>> 0 \\ @. @VV{\varphi}V @VVV @VV{=}V @VV{=}V @. \\ 0 @>>> {\mathbb{Z}_l}^r @>>> A @>>> \mathbb{Z}_l[G]^r @>>> {\mathbb{Z}_l}^r @>>> 0 \\ @. @VV{\simeq}V @. @. @. @. \\ @. H_l^0 @. @. @. @. \end{CD}$$

Lemma 4.2. *a) Each element of* $\mathrm{Ext}^2_{\mathbb{Z}_l[G]}({\mathbb{Z}_l}^r, {\mathbb{Z}_l}^r)$ *can be represented by an injective map* φ.

b) Suppose that φ is injective. Then A is c.t. if and only if φ is surjective (or equivalenty, if and only if $l \nmid \det(\varphi)$).

Proof. a) φ and $\varphi + Nid$ define the same element in the Ext-group for all $N \in \mathbb{N}$ which are divisible by $\#G$. If $-N$ is not an eigenvalue of φ, then $\varphi + Nid$ is injective.

b) If φ is an isomorphism, then $A \simeq \mathbb{Z}_l[G]^r$. Conversely, if A is c.t., then the finite module $\mathrm{cok}(\varphi)$ is also c.t. Now we use the fact that a finite l-group C with trivial G-action is c.t. if and only if $C = 0$. □

Following the recipe in Section 3, see in particular (5), we have to compute the element $[\mathbb{Z}_l[G]^r, \lambda_{NT}(\varphi)_{triv}, \mathbb{Z}_l[G]^r] \in K_0(\mathbb{Z}_l[G], \mathbb{C}_l)$, where $\lambda_{NT}(\varphi)_{triv}$ is the following composite of isomorphisms

$$\begin{array}{ccl} \mathbb{C}_l[G]^r & \stackrel{(8)}{\longrightarrow} & (\mathbb{C}_l)^r \oplus W_{\mathbb{C}_l} \\ & \stackrel{(\varphi,id)}{\longrightarrow} & (E(K) \otimes_{\mathbb{Z}} \mathbb{C}_l) \oplus W_{\mathbb{C}_l} \\ & \stackrel{(\lambda_{NT},id)}{\longrightarrow} & (E(K) \otimes_{\mathbb{Z}} \mathbb{C}_l)^* \oplus W_{\mathbb{C}_l} \\ & \stackrel{(9)}{\longrightarrow} & \mathbb{C}_l[G]^r. \end{array}$$

Let $e_1, \ldots, e_r$ denote the standard basis of $\mathbb{Z}_l^r$ and write $\Phi \in \mathrm{Gl}_r(\mathbb{Z}_l)$ for the coordinate matrix of φ, explicitly $\varphi(e_i) = \sum_{j=1}^r \Phi_{ji} e_j$. We also recall the definition of $\lambda_{NT} : H_l^0 \longrightarrow H_l^1$. Explicitly, $\lambda_{NT}(P) = \langle P, \cdot \rangle$ for $P \in E(K)$, where $\langle \cdot, \cdot \rangle$ denotes the height pairing. Then one has

$$\lambda_{NT}(P_j) = \sum_{k=1}^r \langle P_k, P_j \rangle P_k^*, \quad j = 1, \ldots, r.$$

We write $w_1, \ldots, w_r$ for the standard basis of $\mathbb{C}_l[G]^r$ and set

$$\Psi := \left(\langle P_k, P_j \rangle \right)_{1 \le k,j \le r}.$$

Then

$$\begin{aligned} w_i &\mapsto \left((\ldots, \frac{1}{\#G}, \ldots), (\ldots, g_0 - 1, \ldots) \right) \\ &\mapsto \left(\frac{1}{\#G} \sum_{j=1}^r \Phi_{ji} P_j, (\ldots, g_0 - 1, \ldots) \right) \\ &\mapsto \left(\frac{1}{\#G} \sum_{j=1}^r \Phi_{ji} \sum_{k=1}^r \langle P_k, P_j \rangle P_k^*, (\ldots, g_0 - 1, \ldots) \right) \\ &\mapsto \left(\frac{1}{\#G} \sum_{j=1}^r \Phi_{ji} \langle P_k, P_j \rangle e_0 \right)_{k=1,\ldots,r} + (\ldots, g_0 - 1, \ldots) \\ &= \left(\frac{1}{\#G} \left(\Psi\Phi \right)_{ki} e_0 \right)_{k=1,\ldots,r} + (\ldots, g_0 - 1, \ldots), \\ &= \left((g_0 - 1) + \frac{1}{\#G} \left(\Psi\Phi \right)_{ii} e_0 \right) w_i + \sum_{k=1, k \neq i}^r \left(\frac{1}{\#G} \left(\Psi\Phi \right)_{ki} e_0 \right) w_k. \end{aligned}$$

With respect to the basis $w_1, \dots, w_r$ of $\mathbb{C}_l[G]^r$ the map $\lambda_{NT}(\varphi)_{triv}$ is therefore represented by the matrix

$$\begin{pmatrix} g_0 - 1 & & \\ & \ddots & \\ & & g_0 - 1 \end{pmatrix} + \left(\frac{1}{\#G} (\Psi\Phi)_{ik} \, e_0 \right)_{1 \le i,k \le r}$$

Upon taking determinants one obtains

$$\det_{\mathbb{Z}_l[G]}(\lambda_{NT}(\varphi)_{triv}) = (g_0 - 1)^r + \frac{1}{(\#G)^r} \det(\Psi)\det(\Phi) e_0.$$

We define $\mathrm{Reg}(\varphi) = \left(\mathrm{Reg}_\chi(\varphi)\right)_{\chi \in \mathrm{Irr}(G)}$ by

$$\mathrm{Reg}_\chi(\varphi) = \begin{cases} (\chi(g_0) - 1)^r, & \text{if } \chi \text{ is non-trivial,} \\ \frac{1}{(\#G)^r} \det(\Psi)\det(\Phi), & \text{if } \chi \text{ is trivial,} \end{cases}$$

and set

$$u_l(\varphi) := \frac{\mathcal{L}^* R}{\Omega \mathrm{Reg}(\Phi)} = \frac{\mathcal{L}^* R}{\Omega \mathrm{Reg}(id)} \cdot \frac{1}{E(\varphi)}$$

with

$$E(\varphi) = (E_\chi(\varphi)), \quad E_\chi(\varphi) = \begin{cases} 1, & \text{if } \chi \text{ is non-trivial,} \\ \det(\Phi), & \text{if } \chi \text{ is trivial.} \end{cases} \tag{10}$$

By our construction it is clear that $\mathrm{Ext}_{\mathbb{Z}_l[G]}(H_l^1, H_l^0) \simeq \mathrm{Gl}_r(\mathbb{Z}_l/\#G\mathbb{Z}_l)$. We write $\delta_l \colon \mathbb{Q}_l[G]^\times / \mathbb{Z}_l[G]^\times \longrightarrow K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)$ for the canonical isomorphism (see e.g. [5, Th. 2.2]). From (10) we deduce that

$$\mathcal{E} := \{\delta_l\left(E(\varphi)\right) \mid \Phi \in \mathrm{Gl}_r(\mathbb{Z}_l/\#G\mathbb{Z}_l)\}$$

is a subgroup of $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors}$ of order $l^{n-1}(l-1)$.

We summarize the preceeding discussion in the next theorem.

Theorem 4.3. *We assume (i) - (viii). Then the following are equivalent:*

(i) *The $ETNC_l$ is true module $\mathcal{E}$.*
(ii) $\mathcal{E} = \left\{\delta_l\left(u_l(\varphi)\xi_l^{-1}\right) \mid \Phi \in \mathrm{Gl}_r(\mathbb{Z}_l/\#G\mathbb{Z}_l)\right\}$.
(iii) $\delta_l\left(u_l(id)\xi_l^{-1}\right) \in \mathcal{E}$.

Proof. Let $\alpha_0 : {\mathbb{Z}_l}^r \longrightarrow {\mathbb{Z}_l}^r$ represent the correct extension class. Recall that $\delta_l\left(u_l(\varphi)\right) = \delta_l\left(u_l(id) \cdot \frac{1}{E(\varphi)}\right)$.

We first proof that (i) implies (ii). Let $\delta_l\left(u_l(\alpha_0)\xi_l^{-1}\right) = \delta_l\left(E(\varphi_0)\right)$ for some $\varphi_0 : {\mathbb{Z}_l}^r \longrightarrow {\mathbb{Z}_l}^r$. Then

$$\begin{aligned} & \{\delta_l\left(u_l(\varphi)\xi_l^{-1}\right) \mid \Phi \in \mathrm{Gl}_r(\mathbb{Z}_l/\#G\mathbb{Z}_l)\} \\ = \; & \{\delta_l\left(u_l(id)\xi_l^{-1}E(\varphi)^{-1}\right) \mid \Phi \in \mathrm{Gl}_r(\mathbb{Z}_l/\#G\mathbb{Z}_l)\} \\ = \; & \{\delta_l\left(u_l(\alpha_0)\xi_l^{-1}E(\varphi)^{-1}\right) \mid \Phi \in \mathrm{Gl}_r(\mathbb{Z}_l/\#G\mathbb{Z}_l)\} \\ = \; & \{\delta_l\left(E(\varphi_0)E(\varphi)^{-1}\right) \mid \Phi \in \mathrm{Gl}_r(\mathbb{Z}_l/\#G\mathbb{Z}_l)\} \\ = \; & \mathcal{E}. \end{aligned}$$

(ii) obviously implies (iii). Finally suppose that (iii) holds. Then there exists $\varphi_0 : \mathbb{Z}_l{}^r \longrightarrow \mathbb{Z}_l{}^r$ such that $\delta_l\left(u_l(id)\xi_l^{-1}\right) = \delta_l\left(E(\varphi_0)\right)$. Hence

$$\delta_l\left(u_l(\alpha_0)\xi_l^{-1}\right) = \delta_l\left(\frac{E(\varphi_0)}{E(\alpha_0)}\right) \in \mathcal{E}.$$

□

By the methods of [5] we can numerically test (ii) or (iii) of Theorem 4.3 and thus verify ETNC_l modulo the subgroup $\mathcal{E}$.

If $r = 0$ the subgroup $\mathcal{E}$ is trivial and we can numerically fully verify the validity of the ETNC_l. In the next section we will express the validity of the ETNC_l in terms of explicit congruences.

For $r > 0$ we are not able to fully verify the ETNC. We note that for $n = 1$ one has $\mathcal{E} = K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors}$, so that in this case we study the ETNC_l modulo torsion. However, for $n \geq 2$ our computational results have a much stronger meaning because, as we will prove in the next section,

$$\#K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors} = (l-1)^n l^{\frac{l^n-1}{l-1}-n} >> l^{n-1}(l-1) = \#\mathcal{E}.$$

We will now very explicitly describe what has to be done to verify the ETNC_l. Let $G = \langle g_0 \rangle$. We fix a primitive l^n-th root of unity ζ_{l^n} and for $m = 0, \dots, n$ we set $\zeta_{l^m} := \zeta_{l^n}^{l^{n-m}}$. For $i = 0, \dots, n$ we define an irreducible character χ_i by $\chi_i(g_0) := \zeta_{l^i}$. Then

$$\mathbb{Q}_l[G] \simeq \bigoplus_{i=0}^{n} \mathbb{Q}_l(\zeta_{l^i}), \quad \lambda \mapsto (\chi_i(\lambda))_i . \tag{11}$$

and via this identification the maximal order $\mathcal{M}$ of $\mathbb{Q}_l[G]$ is identified with $\bigoplus_{i=0}^{n} \mathbb{Z}_l[\zeta_{l^i}]$. We will often consider this identification as an equality.

For a positive integer k with $l \nmid k$ we write σ_k for the Galois automorphism which sends ζ_{l^i} to $\zeta_{l^i}^k$. Then the rationality conjecture holds, if and only if for each $i \in \{0, \dots, n\}$ and each $k = 1, \dots, l^{i-1}(l-1)$ with $l \nmid k$ one has

$$\frac{L^*(E/\mathbb{Q}, \bar{\chi}_i^k, 1) R_{\chi_i^k}}{\Omega_{\chi_i^k} \mathrm{Reg}_{\chi_i^k}(id)} \in \mathbb{Q}(\zeta_l^i) \tag{12}$$

and

$$\frac{L^*(E/\mathbb{Q}, \bar{\chi}_i^k, 1) R_{\chi_i^k}}{\Omega_{\chi_i^k} \mathrm{Reg}_{\chi_i^k}(id)} = \left(\frac{L^*(E/\mathbb{Q}, \bar{\chi}_i, 1) R_{\chi_i}}{\Omega_{\chi_i} \mathrm{Reg}_{\chi_i}(id)}\right)^{\sigma_k} . \tag{13}$$

Note that we can only provide numerical evidence for the rationality conjecture. Nevertheless, if we compute good complex approximations and if we have a guess for the denominator, then we can compute $\frac{L^*(E/\mathbb{Q}, \bar{\chi}_i, 1) R_{\chi_i}}{\Omega_{\chi_i} \mathrm{Reg}_{\chi_i^k}(id)}$ as an element of $\mathbb{Q}(\zeta_{l^i})$. Note also that for the computation of R_{χ_i} we need an integral normal basis element for $\mathcal{O}_K$. Such an element can be computed by the algorithms developed in [3] and [4].

Henceforth we assume the rationality conjecture and set

$$\eta_i := \frac{L^*(E/\mathbb{Q}, \bar{\chi}_i, 1) R_{\chi_i}}{\Omega_{\chi_i} \mathrm{Reg}_{\chi_i}(id)} \cdot \prod_{p \in S_{ram}(K/\mathbb{Q})} L_p(E/\mathbb{Q}, \bar{\chi}_i, 1)^{-1}. \tag{14}$$

The vector $\eta := (\eta_0, \dots, \eta_n)$ represents $u_l(id)\xi_l^{-1}$ via the Wedderburn decomposition (11).

Now the l-part of the ETNC holds modulo the torsion subgroup $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors}$, if and only if $\eta_i \in \mathbb{Z}_l[\zeta_{l^i}]^\times$ for $i = 0, \dots, n$. Finally, the l-part of the ETNC is valid modulo $\mathcal{E}$, if and only if $\eta \in \mathcal{E}$. In the case $r = 0$ we can be more precise, because $\mathcal{E}$ is trivial. In this case we obtain that the ETNC$_l$ is true if and only $(\eta_0, \dots, \eta_n)$ satisfies the recursive congruences which we will describe in the next section. In the simplest case when $n = 1$ we obtain that the l-part is true, if and only if $\eta_1 \equiv \eta_0 (\text{mod } (1 - \zeta_l))$.

Remark 4.4. In the case $r = 0$ one can use the theory of modular symbols to compute the precise value of $\frac{\tau(\chi)L(E/\mathbb{Q},\chi,1)}{\Omega_\chi}$ where $\tau(\chi)$ denotes a certain Gauss sum (see e.g. [14, Prop. 2.3]). Studying the relation between Gauss sums and and the resolvents used in [1] and in this manuscript it seems to be possible to provide proofs for ETNC$_l$ by combining results on BSD for $E/\mathbb{Q}$ (e.g. from [24]) with our Theorem 4.3. This will be the subject of a further research project.

5. Relative K-groups for cyclic l-groups

Let l be a prime and G an arbitrary finite group. We let $\mathcal{M} \subseteq \mathbb{Q}_l[G]$ denote a maximal order which contains $\mathbb{Z}_l[G]$ and write $C = \zeta(\mathbb{Q}_l[G])$ for the center of $\mathbb{Q}_l[G]$. We write $\mathcal{O}_C$ for the integral closure of $\mathbb{Z}_l$ in C and recall that $\mathcal{O}_C = C \cap \mathcal{M}$. From [5, Th. 2.4] we obtain

$$K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors} \simeq \mathcal{O}_C^\times / \mathrm{nr}(\mathbb{Z}_l[G]^\times).$$

Let now $G = \langle g_0 \rangle$ be cyclic of order l^n, $n \geq 1$. We fix a primitive l^n-th root of unity ζ_{l^n} and set $\zeta_{l^m} := \zeta_{l^n}^{l^{n-m}}$ for $m = 0, \dots, n$. Consider the Wedderburn decomposition (11). Recall that we identify $\mathcal{M}$ and $\oplus_{i=0}^n \mathbb{Z}_l[\zeta_{l^i}]$. The basic question is now to decide which $(n+1)$-tuples $(\gamma_0, \dots, \gamma_n) \in \mathcal{M}^\times$ are actually contained in $\mathbb{Z}_l[G]^\times$.

It is well known that for $n = 1$ one has $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors} \simeq \mathbb{F}_l^\times$ (see [5, Cor. 8.2]) and that $(\gamma_0, \gamma_1) \in \mathbb{Z}_l[G]$, if and only if $\gamma_1 \equiv \gamma_0 (\text{mod } (1 - \zeta_l))$.

In this section we compute the order of $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors}$ for arbitrary n and develop a recursive test which describes the image of $\mathbb{Z}_l[G]$ in $\mathcal{O}_C$ in terms of explicit congruences.

Let $m \in \{1, \dots, n\}$ and set $C_{l^m} := \langle g_0 \text{ mod } \langle g_0^{l^m} \rangle \rangle$. The results of this section are based on the following cartesian square

$$\begin{array}{ccc} \mathbb{Z}_l[C_{l^m}] & \longrightarrow & \mathbb{Z}_l[C_{l^{m-1}}] \\ \downarrow & & \downarrow \\ \mathbb{Z}_l[\zeta_{l^m}] & \longrightarrow & \mathbb{F}_l[C_{l^{m-1}}]. \end{array} \tag{15}$$

This cartesian square is best understood in terms of polynomial rings. Let $\Phi_{l^m}(T)$ be the l^m-th cyclotomic polynomial. From

$$\Phi_{l^m}(T) \equiv l (\text{mod } (T^{l^{m-1}} - 1))$$

we immediately deduce the following equality of $\mathbb{Z}_l[T]$-ideals

$$\left(\Phi_{l^m}(T), T^{l^{m-1}} - 1 \right) = \left(l, T^{l^{m-1}} - 1 \right). \tag{16}$$

Now consider the pull back of

$$\begin{array}{ccc} & & \mathbb{Z}_l[T]/(T^{l^{m-1}}-1) \\ & & \big\downarrow{\scriptstyle \mathrm{mod}\ l} \\ \mathbb{Z}_l[T]/(\Phi_{l^m}(T)) & \xrightarrow[\mathrm{mod}\ (l, T^{l^{m-1}}-1)]{} & \mathbb{F}_l[T]/(T^{l^{m-1}}-1). \end{array}$$

We shall prove that this pull back is canonically isomorphic to $\mathbb{Z}_l[T]/(T^{l^m}-1)$.

Lemma 5.1. *The canonical map*

$$\begin{array}{rcl} \dfrac{\mathbb{Z}_l[T]}{(T^{l^m}-1)} & \longrightarrow & \left\{(f,g) \in \dfrac{\mathbb{Z}_l[T]}{(T^{l^{m-1}}-1)} \oplus \dfrac{\mathbb{Z}_l[T]}{(\Phi_{l^m}(T))} \mid f \equiv g (\mathrm{mod}\ (l, T^{l^{m-1}}-1))\right\} \\ h & \mapsto & \Big(h \bmod (T^{l^{m-1}}-1), h \bmod (\Phi_{l^m}(T))\Big) \end{array}$$

is an isomorphism.

Proof. We first prove injectivity. Suppose that $h \in \Big(T^{l^{m-1}}-1\Big) \cap (\Phi_{l^m}(T))$. Let $a(T) \in \mathbb{Z}_l[T]$ be such that $l = \Phi_{l^m}(T) + a(T)(T^{l^{m-1}}-1)$. We recall that $\Phi_{l^m}(T)(T^{l^{m-1}}-1) = T^{l^m}-1$. Therefore the equality $lh(T) = \Phi_{l^m}(T)h(T) + a(T)(T^{l^{m-1}}-1)h(T)$ implies that $lh(T) \in \big(T^{l^m}-1\big)$. Since $\mathbb{Z}_l[T]$ is factorial and $l \nmid T^{l^m}-1$ it follows that $T^{l^m}-1 \mid h(T)$.

In order to prove surjectivity we let (f,g) be such that $f \equiv g(\mathrm{mod}\ (l, T^{l^{m-1}}-1))$. From (16) we deduce that there exist polynomials h_1, h_2 such that

$$f(T) - g(T) = h_1(T)\Phi_{l^m}(T) + h_2(T)(T^{l^{m-1}}-1).$$

Therefore

$$h(T) := f(T) - h_2(T)(T^{l^{m-1}}-1) = g(T) + h_1(T)\Phi_{l^m}(T) \tag{17}$$

maps to (f,g). □

Let

$$f(T) = \sum_{i=0}^{l^{m-1}-1} a_i T^i \text{ and } g(T) = \sum_{j=0}^{l^{m-1}(l-1)-1} b_j T^j$$

and suppose that (f,g) is an element in the pull back. One easily shows that

$$\begin{aligned} & f(T) \equiv g(T)(\mathrm{mod}\ (l, T^{l^{m-1}}-1)) \\ \Longleftrightarrow \quad & a_i \equiv \sum_{k=0}^{l-2} b_{i+kl^{m-1}} (\mathrm{mod}\ l), \quad i = 0, \ldots, l^{m-1}-1. \end{aligned} \tag{18}$$

Via the canonical identification $\mathbb{Z}_l[T]/(\Phi_{l^m}(T)) \simeq \mathbb{Z}_l[\zeta_{l^m}]$ the polynomial $g(T)$ corresponds to $\gamma_m = \sum_{j=0}^{l^{m-1}(l-1)-1} b_j \zeta_{l^m}^j$. One has

$$\begin{aligned} & \gamma_m \equiv \sum_{i=0}^{l^{m-1}-1} a_i \zeta_{l^m}^i (\mathrm{mod}\ (1-\zeta_l)) \\ \Longleftrightarrow \quad & a_i \equiv \sum_{k=0}^{l-2} b_{i+kl^{m-1}} (\mathrm{mod}\ l), \quad i = 0, \ldots, l^{m-1}-1. \end{aligned} \tag{19}$$

Combining (18) and (19) we obtain

$$f(T) \equiv g(T)(\mathrm{mod}\ (l, T^{l^{m-1}} - 1)) \iff \gamma_m \equiv \sum_{i=0}^{l^{m-1}-1} a_i \zeta_{l^m}^i (\mathrm{mod}\ (1-\zeta_l)).$$

We define a homomorphism

$$\varphi_{m-1} \colon \mathbb{Z}_l[C_{l^{m-1}}] \longrightarrow \mathbb{Z}_l[\zeta_{l^m}]/(1-\zeta_l), \quad g_0 \bmod \langle g_0^{l^{m-1}} \rangle \mapsto \zeta_{l^m} \bmod (1-\zeta_l)$$

and are finally in position to formulate our recursive test in terms of congruences. Let $(\gamma_0, \dots, \gamma_n) \in \mathcal{M}^\times$ and set $\lambda_0 := \gamma_0$. Let $m \in \{1, \dots, n\}$ and suppose that by induction we have constructed $\lambda_{m-1} \in \mathbb{Z}_l[C_{l^{m-1}}]$. If $\gamma_m \equiv \varphi_{m-1}(\lambda_{m-1})(\mathrm{mod}\ (1-\zeta_l))$, then $(\gamma_0, \dots, \gamma_m)$ defines an element $\lambda_m \in \mathbb{Z}_l[C_{l^m}]$ and we can continue the recursive test. Note that λ_m can easily be computed from (17). We summarize our result in the following proposition.

Proposition 5.2. *Let l be a prime and let G be a cyclic group of order l^n. Let $(\gamma_0, \dots, \gamma_n) \in \mathcal{M}^\times$. Then*

$$(\gamma_0, \dots, \gamma_n) \in \mathbb{Z}_l[C_{l^n}]^\times \iff \gamma_m \equiv \varphi_{m-1}(\lambda_{m-1})(\mathrm{mod}\ (1-\zeta_l)), \quad m = 1, \dots, n.$$

Remark 5.3. Let $G = \langle \sigma, \tau \mid \sigma^{l^n} = \tau^2 = 1, \tau\sigma = \sigma^{-1}\tau \rangle$ be the dihedral group of order 2^{l^n}, where l is an odd prime. Then

$$\mathbb{Q}[G] \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q}(\zeta_l)^+) \oplus \ldots \oplus M_2(\mathbb{Q}(\zeta_{l^n})^+).$$

Let $H = \langle \sigma \rangle$. By [6, Prop. 3.2] we know that the restriction map

$$\mathrm{res} \colon K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors} \longrightarrow K_0(\mathbb{Z}_l[H], \mathbb{Q}_l)_{tors}$$

is injective. Let

$$\alpha = (\alpha_0, \dots, \alpha_{n+1}) \in \mathbb{Z}_l{}^\times \oplus \mathbb{Z}_l{}^\times \oplus \mathbb{Z}_l[\zeta_l]^{+\times} \oplus \ldots \oplus \mathbb{Z}_l[\zeta_{l^n}]^{+\times}.$$

By [6, Lemma 3.9] or [2, page 575] one has $\mathrm{res}(\alpha) = (\alpha_0\alpha_1, \alpha_2, \dots, \alpha_{n+1})$ and we can apply our recursive test to $\mathrm{res}(\alpha)$ in order to decide whether $\delta_l(\alpha)$ is trivial in $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)$.

To conclude this section we compute the order of $K_0(\mathbb{Z}_l[C_{l^n}], \mathbb{Q}_l)_{tors}$.

Proposition 5.4. *Let l be a prime and let G be a cyclic group of order l^n. Then*

$$\#K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors} = (l-1)^n l^e \text{ with } e = \frac{l^n - 1}{l - 1} - n.$$

The exponent of $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors}$ is a divisor of $(l-1)^n l^f$ with $f = \frac{(n-1)n}{2}$

Proof. We set $DT(\mathbb{Z}_l[G]) := K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors}$. We apply [5, Th. 8.1] to the cartesian square (15). Using the fact that SK_1 of a semilocal commutative ring is trivial (see [12, Th. (45.12)]), we obtain the short exact sequence

$$0 \longrightarrow \mathbb{F}_l[C_{l^{n-1}}]^\times \longrightarrow DT(\mathbb{Z}_l[C_{l^n}]) \longrightarrow DT(\mathbb{Z}_l[C_{l^{n-1}}]) \longrightarrow 0$$

For a natural number k the ring $\mathbb{F}_l[C_{l^k}]$ is local with maximal ideal $\Delta := \ker(aug)$, where $aug : \mathbb{F}_l[C_{l^k}] \longrightarrow \mathbb{F}_l$ is the usual augmentation map. It follows that $\#\mathbb{F}_l[C_{l^k}]^\times = l^{l^k - 1}(l-1)$.

The result for the order of $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors}$ follows now easily by induction. It is also easily seen that

$$\prod_{k=0}^{n-1} \exp(\mathbb{F}_l[C_{l^k}]^\times).$$

annihilates $DT(\mathbb{Z}_l[G])$. Finally, from $\exp(\mathbb{F}_l[C_{l^k}]^\times) = l^k(l-1)$ we obtain the result for the exponent of $DT(\mathbb{Z}_l[G])$. □

Remark 5.5. a) Let l be an odd prime and let G be a cyclic group of order l^2. Then it can be shown that

$$K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors} \simeq C_{l-1}^2 \times C_l^{l-1}.$$

Of course, one would like to have a general result which describes the structure of $K_0(\mathbb{Z}_l[G], \mathbb{Q}_l)_{tors}$ for cyclic groups of (odd) prime power order. However, our proof is purely computational and although several parts obviously generalize, it finally becomes a mess for $n > 2$.

b) Running the algorithm of [5] one obtains

$$K_0(\mathbb{Z}_3[C_{27}], \mathbb{Q}_3)_{tors} \simeq C_2^3 \times C_3^4 \times C_9^3.$$

For higher values of l and n the algorithm does not terminate.

6. Numerical results

Let l be an odd prime, $n \geq 1$ a natural number and p a prime such that $p \equiv 1 (\mathrm{mod}\ l^n)$. Let K denote the unique subextension of $\mathbb{Q}(\zeta_p)$ of order l^n. We did many experiments with various elliptic curves from Cremona's database each time verifying ETNC_l numerically modulo $\mathcal{E}$. We point out once again that we only provide numerical evidence for the rationality conjecture since we only compute complex approximations to the L-values, regulators and periods. Moreover, we are only able to compute a conjectural value for the order of $Ш(E/K)$ from the classical BSD conjecture for E/K.

Assuming the rationality conjecture and that

- we have correctly computed the exact values η_i from (14) by some rounding process,
- the value for the order of $Ш(E/K)$ is correct,

the remaining computations are exact. We point out, that presently in none of the computed examples we actually have a rigorous proof. We only provide numerical evidence.

The MAGMA implementation, sample files and two tables are available from

`http://www.mathematik.uni-kassel.de/~bley/pub.html.`

We have produced two tables of examples. Table 1 contains a list of examples as described above where we have checked the ETNC at l. More precisely, we considered all elliptic curves with split multiplicative reduction of conductor $N_E \leq 500$, primes $p \leq 50$ and triples

$$\begin{aligned}(r,l,n) \quad \in \quad & \{[0,3,1],[0,3,2],[0,5,1],[0,7,1],[0,11,1],\\ & [1,3,1],[1,3,2],[1,5,1],[1,7,1],[1,11,1],\\ & [2,3,1],[2,3,2],[2,5,1],[2,7,1],[2,11,1]\}\end{aligned}$$

such that the pair (E, K) satisfies our Hypothesis (i)-(viii). The table contains in total 1507 examples.

If $r = 0$ we can fully verify the ETNC_l numerically and, in addition, the methods of [1] are available. Also note that by [15, Th. 3.3 and 3.5] we know that if the analytic rank is trivial then $E(K)$ and $Ш(E/K)$ are finite. Note also that the theory of modular symbols would allow to compute the precise value of the L-series (see also Remark 4.4). However, this is not implemented. In Table 2 we list all examples as described above where we tried to check the full ETNC. More precisely, we considered all elliptic curves with split multiplicative reduction of conductor $N_E \leq 100$, primes $p \leq 50$ and triples

$$(r, l, n) \in \{[0, 3, 1], [0, 3, 2], [0, 5, 1], [0, 7, 1], [0, 11, 1], \}.$$

such that the pair (E, K) satisfies our Hypothesis (i)-(viii). Each of the examples is followed by a set of primes which contains the primes where we could not apply the methods of [1] because the Hypothesis (H0)-(H5) were not satisfied. In all cases this set consist of at most 3 primes. The table contains in total 208 examples. Note that for 52 examples we obtained a numerical verification of ETNC at all primes.

References

[1] W. Bley, *Numerical evidence for the euivariant Birch and Swinnerton-Dyer conjecture*, Preprint 2009, 41 pages.

[2] W. Bley, D. Burns, *Equivariant epsilon constants, discriminants and étale cohomology*, Proc. London Math. Soc. **87** (2003), 545–590.

[3] W. Bley, H. Johnston, *Computing generators of free modules over orders in group algebras*, J.Algebra (Computational Section). **320** (2008), 836–852.

[4] W. Bley, H. Johnston, *Computing generators of free modules over orders in group algebras, part 2*, preprint 2010.

[5] W. Bley, Wilson, *Computations in relative algebraic K-groups*, LMS JCM . **12** (2009), 166–194.

[6] M. Breuning, *On equivariant global epsilon constants for certain dihedral extensions*, Math. Comp. **73** (2004), 881–898.

[7] M. Breuning, D. Burns,*Leading terms of Artin L-functions at $s = 0$ and $s = 1$*, Compositio Math. **143** (2007), 1427-1464.

[8] D. Burns, M. Flach*Motivic L-functions and Galois module structures*, Math. Ann. **305** (1996) 65-102.

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

[10] D. Burns, *Equivariant Whitehead torsion and refined Euler characteristics*, CRM Proceedings and Lecture Notes, vol. 36 (American Mathematical Society, Providence, RI, 2004), 35-59. Whitehead.

[11] D. Burns, *On leading terms and values of equivariant motivic L-functions*, to appear in the 'Tate volume'.

[12] C. Curtis, I. Reiner: Methods of representation theory, volume I and II. Wiley, 1981 and 1987.

[13] H. Cohen, *Advanced topics in computational number theory*, Springer Verlag (2000).

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

[15] 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.

[16] B. H. Gross,D. B. Zagier, *Heegner points and derivatives of L-series*, Inventiones Mathematicae **84 (2)**, (1986) 225-320.

[17] A. Grothendieck: *Groupes de Monodromie en Géométrie Algébrique (SGA 7 I)*, Lecture Notes in Math. **288**, Springer Verlag, 1972.

[18] G. Kings: *An introduction to the equivariant Tamagawa number conjecture: the relation to the Birch-Swinnerton-Dyer conjecture*, Preprint Nr. 26/2009, Universit"at Regensburg.

[19] V.A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, *Progr. in Math.* **87**, Boston, Boston, MA (1990).

[20] V.A. Kolyvagin, D.Y. Logachev *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Leningrad Math.J. **1**, (1990) 1229-1253.

[21] V.A. Kolyvagin, D.Y. Logachev *Finiteness of over totally real fields*, USSR Izvestiya **39**, (1992) 829-853.

[22] MAGMA, Version V2.12, Sydney 2005.

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

[24] G. Grigorov, A. Jorza, S. Patrikis, W. A. Stein, C. Tarnita-Patrascu, *Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves*, Mathematics of Computation **78** (2009), 2397–2425.

[25] O. Venjakob, *From the Birch and Swinnerton-Dyer Conjecture over the Equivariant Tamagawa Number Conjecture to non-commutative Iwasawa theory*, to appear in 'L-functions and Galois representations', Proceedings of the 2004 Durham Symposium, C.U.P.

[26] S. Zhang, *Heights of Heegner points on Shimura curves*, Annals of Math. **153**, (2001) 27-147.

Institut für Mathematik der Universität Kassel, Heinrich-Plett-Str. 40, 34132 Kassel, Germany

E-mail address: bley@mathematik.uni-kassel.de