Münster J. of Math. **7** (2014), 327–343
urn:nbn:de:hbz:6-22359592813

Münster Journal of Mathematics

Euler characteristic and congruences of elliptic curves

Sudhanshu Shekhar and R. Sujatha

(Communicated by Christopher Deninger)

Dedicated to Peter Schneider on the occasion of his 60th birthday

Abstract. Given two elliptic curves over $\mathbb{Q}$ that have good ordinary reduction at an odd prime p, and have equivalent, irreducible mod p Galois representations, we study congruences between the Euler characteristics and special L-values over certain noncommutative extensions of $\mathbb{Q}$.

Introduction

Let p be an odd prime, and $E_1,\ E_2$ be two elliptic curves defined over $\mathbb{Q}$ with good ordinary reduction at p. Suppose that the residual representations $E_1[p]$ and $E_2[p]$ are isomorphic as $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-modules and are irreducible. Consider the field $K = \mathbb{Q}(\mu_p)$ and $F = K(m^{1/p})$ where m is an integer which is p-power free and coprime to the conductors of E_1 and E_2. For a field extension L of $\mathbb{Q}$, let L_{cyc} denote the cyclotomic $\mathbb{Z}_p$-extension of L and $\mathrm{Sel}(E_j/L_{\mathrm{cyc}})$ be the p-Selmer group of $E_j,\ j = 1, 2$. We denote the False Tate extension $K_{\mathrm{cyc}}(m^{1/p^\infty})$ by F_∞. For a finite set of places Σ_0 of $\mathbb{Q}$, the imprimitive p-Selmer group (see Section 1) of $E_j,\ j = 1, 2$, with respect to Σ_0 is denoted by Sel^{Σ_0}. In [12], Greenberg and Vatsal study the Iwasawa invariants of the imprimitive p-Selmer groups of E_1 and E_2 over $\mathbb{Q}_{\mathrm{cyc}}$ for certain choices of Σ_0, and prove that they are equal under additional hypotheses. In addition, they compare the special values of the p-adic L-functions of E_1 and E_2, establishing certain congruence results between them. Our goal in this article is twofold. First, we study the Euler characteristics of the Selmer groups of E_1 and E_2 (when they are finite), both over the cyclotomic extensions K_{cyc} and F_{cyc} as well as over the extension F_∞(see Theorem 3.4). We study the conditions under which the Euler characteristics of $\mathrm{Sel}(E_j/\mathcal{L}),\ j = 1, 2$, are simultaneously trivial where $\mathcal{L}$ is either of these cyclotomic extensions or F_∞ (see Section 3). Second, we compare certain p-adic L-values of E_1 and E_2 over F, when $p = 3$ (see

Theorem 3.8). Further, we also consider similar questions when F is a dihedral extension of $\mathbb{Q}$ of degree $2p^n$ for some integer $n \geq 1$. For establishing the results on the Euler characteristics, we extend the method of [12] to study the Iwasawa invariants of the imprimitive Selmer groups. But our analysis of the optimal set Σ_0 requires results of Hachimori–Matsuno [13] and those of Emerton–Pollack–Weston [8]. In particular, the optimal set Σ_0 that is considered here is smaller than that of Greenberg and Vatsal. For the results on L-values, we rely on the results of Bouganis [1], [18] and of [12]. In addition, we have made use of results of Hachimori and Venjakob [14] and T. and V. Dokchitser [5], especially in studying the Euler characteristics over F_∞.

The article consists of five sections, Section 1 introduces notation and is preliminary in nature. In Section 2, we study the Euler characteristics of the imprimitive Selmer groups, while in Section 3, we establish congruence results for the Euler characteristics over the False Tate extension and compare the p-adic L-values for $p = 3$. In Section 4, we establish analogous results in the dihedral setting. The final section illustrates our theoretical results with concrete numerical examples.

The first author warmly thanks the University of British Columbia for hospitality provided while this work was being completed. The second author gratefully acknowledges the support of an NSERC grant, and also the hospitality accorded at Universität Münster during the early stages of this work. We warmly thank Tim Dokchitser for help with the numerical examples. Finally, we would like to thank the referee for the helpful comments which helped us improve the exposition.

1. Notation

Let E be an elliptic curve defined over a number field k and p be an odd prime such that E has good ordinary reduction at primes of k lying above p. Let Σ be a finite set of primes of k containing the primes of k lying above p, the infinite primes and the primes of bad reduction of E. Denote by k_Σ the maximal extension of k unramified outside Σ. Given an extension L such that $k \subset L \subset k_\Sigma$, the Selmer group $\mathrm{Sel}(E/L)$ of E over L is defined as the kernel of the "global to local" map

$$H^1(k_\Sigma/L, E_{p^\infty}) \xrightarrow{\gamma_L} \prod_{v\in\Sigma} H_v(L, E), \tag{1}$$

where for a finite prime v of k, $H_v(L, E) := \prod_{w|v} H^1(L_w, E[p^\infty])/\operatorname{im}(\kappa_w^L)$. Here w runs over finite places of L that lie above v, L_w is the union of completions of number fields L' at w, such that $k \subseteq L' \subset L$, and κ_w^L denotes the local Kummer map

$$E(L_w) \otimes \mathbb{Q}_p/\mathbb{Z}_p \longrightarrow H^1(L_w, E_{p^\infty}). \tag{2}$$

Since p is odd, for an archimedean prime v we have $H_v(L, E) = 0$. Let Σ_0 be a subset of Σ such that if $v|p$, then $v \notin \Sigma_0$. The *imprimitive Selmer group*

$\mathrm{Sel}^{\Sigma_0}(E/L)$ is defined as

$$\mathrm{Sel}^{\Sigma_0}(E/L) := \mathrm{Ker}(H^1(k_\Sigma/L, E_{p^\infty}) \xrightarrow{\gamma_L^{\Sigma_0}} \prod_{v\in\Sigma-\Sigma_0} H_v(L,E)).$$

We have the following exact sequence

$$0 \longrightarrow \mathrm{Sel}(E/L) \xrightarrow{i_L} \mathrm{Sel}^{\Sigma_0}(E/L) \xrightarrow{j_L^{\Sigma_0}} \prod_{v\in\Sigma_0} H_v(L,E). \tag{3}$$

Put $X^{\Sigma_0}(E/L) := \mathrm{Hom}(\mathrm{Sel}^{\Sigma_0}(E/L), \mathbb{Q}_p/\mathbb{Z}_p)$. If L/k is Galois, then $X^{\Sigma_0}(E/L)$ (resp. $\mathrm{Sel}^{\Sigma_0}(E/L)$) is a compact (resp. discrete) module over $\mathbb{Z}_p[[\mathrm{Gal}(L/k)]]$. For a compact p-adic Lie group G and a finitely generated $\mathbb{Z}_p[[G]]$-module X, the G-Euler characteristic of X is defined as

$$\chi(G,X) := \prod_i \#(H_i(G,X))^{(-1)^i},$$

provided the groups $H_i(G,X)$ are finite for all i and vanish for large i. When this is the case, we say that the G-Euler characteristic $\chi(G,X)$ of X exists. Similarly, for a discrete $\mathbb{Z}_p[[G]]$-module M, put

$$\chi(G,M) := \prod_i \#(H_i(G,\widehat{M}))^{(-1)^i},$$

where $\widehat{M}$ is the compact Pontryagin dual of M. For a number field k and a p-adic Lie extension L of k, let τ be an Artin representation of $\mathrm{Gal}(L/k)$ with coefficients in $\mathbb{Z}_p$. Let $X^{\Sigma_0}((E/L)\otimes\tau)$ be the twisted imprimitive Selmer group and put

$$\chi(L/k,\tau,E;\Sigma_0) := \chi(\mathrm{Gal}(L/k),\ X^{\Sigma_0}(E/L)\otimes\tau).$$

If τ is the trivial character then we shall drop τ from the notation of the Euler characteristic. Similarly, if Σ_0 is empty, then we shall suppress it from the notation of the imprimitive Selmer group and Euler characteristic.

Let m be a positive integer such that $m^{1/p^n} \notin k(\mu_{p^n})$ for all $n \geq 1$. Put $K_n = \mathbb{Q}(\mu_{p^n})$ and $F_n = K_n(m^{1/p^n})$ for $n \geq 1$, and $F_\infty = \cup_n F_n$. For a number field $k \subset F_\infty$, we denote by G_k the Galois group $\mathrm{Gal}(F_\infty/k)$, and $\Gamma_k := \mathrm{Gal}(k_{\mathrm{cyc}}/k)$.

2. Imprimitive Euler characteristic

Let E be an elliptic curve defined over a number field $k \subset F_\infty$ with good ordinary reduction at primes of k lying above p. We shall assume that Σ contains the primes of k lying above the prime divisors of m. To simplify matters, we shall also assume that m is coprime to the conductor N_E of the elliptic curve. In particular, this latter assumption implies that the reduction type of E does not change in any finite subextension of F_∞ containing k. We have the following result (see [16],[11, Cor. 4.9], [15]).

Theorem 2.1. *Suppose that* $\mathrm{Sel}(E/k)$ *is finite or* $k/\mathbb{Q}$ *is an abelian extension and* E *is defined over* $\mathbb{Q}$. *Then* $\mathrm{Sel}(E/k_{\mathrm{cyc}})$ *is a cotorsion* $\mathbb{Z}_p[[\Gamma_k]]$*-module.*

Corollary 2.2. *Suppose that* $\mathrm{Sel}(E/k)$ *is finite or* $k/\mathbb{Q}$ *is an abelian extension and* E *is defined over* $\mathbb{Q}$. *Then* $\gamma_{k_{\mathrm{cyc}}}$ *and* $j_{k_{\mathrm{cyc}}}^{\Sigma_0}$ *defined respectively in* (1) *and* (3) *are surjective.*

Proof. For the surjectivity of $\gamma_{k_{\mathrm{cyc}}}$, see [14, Thm. 7.2]. The surjectivity of $j_{k_{\mathrm{cyc}}}$ follows by a simple argument using the snake lemma. □

Corollary 2.3. *The maps* γ_{F_∞} *and* $j_{F_\infty}^{\Sigma_0}$ *are surjective.*

Proof. It is well known (see [4]) that the surjectivity of $\gamma_{K_{\mathrm{cyc}}}$ implies that the map γ_{F_∞} is surjective. The surjectivity of $j_{F_\infty}^{\Sigma_0}$ follows from that of γ_{F_∞}. □

Definition 2.4. We define the following subsets of Σ. The set $\Sigma_1(E)$ is the set of primes v of k such that $v \in \Sigma_0$, $v \nmid m$ and E has split multiplicative reduction at v. Define $\Sigma_2(E)$ to be the set of primes v of k such that $v \in \Sigma_0$, $v \nmid m$, E has good reduction at v and the reduced curve has a point of order p. Finally, $\Sigma_3(E)$ is the subset of Σ containing the primes v of k such that $v \mid m$, $v \nmid p$, E has good reduction at v and the corresponding reduced curve has a point of order p.

We remark that the set $\Sigma_3(E)$ is the set denoted by $P_1^k(E)$ in [14]. Let l be a finite prime of $\mathbb{Q}$. For a finite prime $v \nmid l$ of k, let

$$P_v(E,T) := \det(1 - \mathrm{Frob}_v^{-1} T | M_l(E))$$

denote the characteristic polynomial of E at v, where $M_l(E)$ denotes the l-adic Galois representation associated to the Tate module of E. As the notation suggests, the definition of $P_v(E,T)$ is independent of the choice of the prime l. Recall that the local L factor $L_v(E,s)$ of E at v is defined as

$$L_v(E,s) := (P_v(E, \mathrm{Norm}_{k/\mathbb{Q}}(v)^{-s}))^{-1},$$

where $\mathrm{Norm}_{k/\mathbb{Q}}$ denotes the norm map from k to $\mathbb{Q}$.

Lemma 2.5. *For a finite prime* $v \nmid p$ *of* k *where* E *has bad reduction, the local Euler factor* $L_v(E,1)$ *at* v *is a* p*-adic unit if and only if* E *has nonsplit multiplicative reduction or additive reduction at* v. *If* $v \nmid p$ *is a finite prime of* k *where* E *has good reduction, then* $L_v(E,1)$ *is a non* p*-adic unit if and only if the corresponding reduced curve at* v *has a point of oder* p.

Proof. This is well known (cp. [5, Rem. 4.6]). □

We remark that the above lemma says that if E has split multiplicative reduction at a prime $v \nmid p$, then $v_p(L_v(E,1)) \leq -1$, where v_p denotes the p-adic valuation such that $v_p(p) = 1$.

Lemma 2.6. *Let E be an elliptic curve over a number field k and consider the extension $F_\infty = k(\mu_{p^\infty}, m^{1/p^\infty})$. If $\chi(F_\infty/k, E; \Sigma_0)$ exists, then we have that*

$$\chi(F_\infty/k, E; \Sigma_0) = \chi(F_\infty/k, E) \times \prod_{v \in \Sigma_1(E) \cup \Sigma_2(E)} |L_v(E,1)|_p$$

where $|.|_p$ denotes the p-adic valuation normalized such that $|p|_p = 1/p$.

Proof. For a prime $w \nmid p$, it is a well known fact that $\kappa_w^{F_\infty} = 0$, where we recall that $\kappa_w^{F_\infty}$ is the local Kummer map (cp. (2)). Thus we have for a prime v in Σ_0,

$$H_v(F_\infty, E) = \prod_{w|v} H^1(F_{w,\infty}, E_{p^\infty}).$$

Fix a prime w of F_∞ that lies above v. Denote by G_w the decomposition subgroup of G_k associated to w. We have that $\chi(G_k, H_v(F_\infty, E)) = \chi(G_w, H^1(F_{w,\infty}, E_{p^\infty}))$. This follows from Shapiro's Lemma, and on using the fact that $H_v(F_\infty, E) = \mathrm{coind}_{G_w}^{G_k}(H^1(F_{w,\infty}, E_{p^\infty}))$. In fact,we see from [14, Prop. 4.7] that

$$\chi(G_k, H_v(F_\infty, E)) = \#H^0(G_k, H_v(F_\infty, E)) = \#H^0(G_w, H^1(F_{w,\infty}, E_{p^\infty}))$$

as the higher cohomology groups $H^i(G_w, H^1(F_{w,\infty}, E_{p^\infty}))$ vanish for $i \geq 1$. If $v|m$ then v ramifies in F_∞ and in this case $H^1(F_{w,\infty}, E_{p^\infty})) = 0$ (see [14, Lemma 4.8]). Thus the G_k-Euler characteristic of $H_v(E,k)$ vanishes if $v|m$. Next, suppose that $v \nmid m$, and consider the restriction map res_w

$$H^1(k_v, E_{p^\infty}) \xrightarrow{\mathrm{res}_w} H^1(F_{w,\infty}, E_{p^\infty}))^{G_w}.$$

From the proof [14, Lemma 4.8] we have that

$$\#\mathrm{Ker}(\mathrm{res}_w)/\#\mathrm{Coker}(\mathrm{res}_w) = \#H^1(k_v(\mu_{p^\infty})/k_v, E(k_v(\mu_{p^\infty})_{p^\infty}).$$

Let c_v denote the local Tamagawa number of E at v and $|.|_p$ be the p-adic valuation such that $|p|_p = 1/p$. It is known (cp. [3, Lemma 3.4]) that $|c_v|_p^{-1} = \#H^1(k_v(\mu_{p^\infty})/k_v, E(k_v(\mu_{p^\infty})_{p^\infty})$. We remark that [14, Lemma 4.8] is proved under the assumption that $p \geq 5$, but the same proof works even for $p = 3$. On the other hand, we have that $\#H^1(k_v, E_{p^\infty}) = |L_v(E,1)|_p/|c_v|_p$ (see [3, Lemma 1.11]). Thus we obtain $\#H^0(G_w, H^1(F_{w,\infty}, E_{p^\infty})) = |L_v(E,1)|_p$. Therefore

$$\chi(G_k, H_v(F_\infty, E)) = |L_v(E,1)|_p$$

From Corollary 2.3, we have that j_{F_∞} is surjective. Since the Euler characteristic is multiplicative in exact sequences, we have that

$$\chi(F_\infty/k, E; \Sigma_0) = \chi(F_\infty/k, E) \times \prod_{v \in \Sigma_0} \chi(G_k, H_v(F_\infty, E)).$$

We have already remarked that the G_k-Euler characteristic of $H_v(E/k)$ vanishes if $v|m$. Further, if v is a prime such that E has bad but not split multiplicative reduction, then by Lemma 2.5, we have that the local L-factor $L_v(E,1)$ is a p-adic unit at v. The lemma now follows from the definition of the sets $\Sigma_1(E)$ and $\Sigma_2(E)$. □

Lemma 2.7. *If* $\mathrm{Sel}(E/k)$ *is finite, then we have*

$$\chi(K_{\mathrm{cyc}}/k, E; \Sigma_0) = \chi(K_{\mathrm{cyc}}/k, E) \times \prod_{v \in \Sigma_1(E) \cup \Sigma_2(E)} |L_v(E,1)|_p.$$

Proof. Let $v \in \Sigma_0$. Let w be a prime of K_{cyc} such that that $w|v$. Then by an argument similar to Lemma 2.6 we have that

$$\chi(\mathrm{Gal}(K_{\mathrm{cyc}}/k), H_v(K_{\mathrm{cyc}}, E)) = |L_v(E,1)|_p.$$

From Corollary 2.2, we have that $j_{k_{\mathrm{cyc}}}^{\Sigma_0}$ is surjective. The lemma now follows by an argument similar to the proof of Lemma 2.6. □

Corollary 2.8. *Let* $k \subset F_\infty$ *be a number field and put* $K = k(\mu_p)$. *If* $\chi(F_\infty/k, E; \Sigma_0)$ *exists, so does* $\chi(K_{\mathrm{cyc}}/k, E; \Sigma_0)$ *and we have that*

$$\chi(F_\infty/k, E; \Sigma_0) = \chi(K_{\mathrm{cyc}}/k, E; \Sigma_0) \times \prod_{v \in \Sigma_3(E)} |L_v(E,1)|_p$$

Proof. From [14, Thm. 4.10] if $\chi(F_\infty/k, E; \Sigma_0)$ exists then $\chi(K_{\mathrm{cyc}}/k, E; \Sigma_0)$ also exists, and we have,

$$\chi(F_\infty/k, E) = \chi(K_{\mathrm{cyc}}/k, E) \times \prod_{v \in \Sigma_3(E)} |L_v(E,1)|_p.$$

We mention that [14, Thm. 4.10] is proved under the assumption that $p \geq 5$. This assumption was required in the proof of [14, Lemma 4.8]. A similar result holds under the assumption that the reduction type of E does not change in F_∞ at every prime of bad reduction, which is valid in our case as $(m, N_E) = 1$. Now the corollary follows from Lemma 2.6, Lemma 2.7 and the definition of the set $\Sigma_3(E)$. □

3. Congruence

As before, let $k \subset F_\infty$ be a number field. We shall assume through out this section that $k \supset \mu_p$. We shall need an equivalent but different definition of the Selmer group of an elliptic curve with good ordinary reduction at p. We shall use the same notation to denote this Selmer group. Let E be an elliptic curve defined over k with conductor N_E and good ordinary reduction at the primes above p. For every prime $v|p$ of k let $\widetilde{E}_v$ denote the reduced curve at v. Since E has ordinary reduction at the primes above p, for every prime $v|p$ of k, $\widetilde{E}_v[p^\infty]$ is of $\mathbb{Z}_p$-corank one. Put

$$F_v^+ E_{p^\infty} := \mathrm{kernel}(E[p^\infty] \longrightarrow \widetilde{E}_v[p^\infty]).$$

The subgroup $F_v^+ E_{p^\infty}$ has $\mathbb{Z}_p$-corank one and is invariant under the action of the decomposition group G_v at v. We mention that the G_v-submodule $F_v^+ E_{p^\infty}$ is equal to $\widehat{E}_v[p^\infty]$, where $\widehat{E}_v$ is the formal group associated to E at v.

For a prime v of k and a prime $w|v$ of k_{cyc} let $Cw = E_{p^\infty}$ if $w \nmid p$ and $Cw = E_{p^\infty}/F + vE_{p^\infty} \cong \tilde{E}_v[p^\infty]$ if $w|p$. Let Σ be a finite set of primes of k as in Section 1. Suppose $v \in \Sigma$ is a prime of k. If $v \nmid p$ then put

$$J_v(E, k_{\mathrm{cyc}}) = \prod_{w|v} H^1(k_{w,cyc}, C_w).$$

If $v|p$ then set

$$J_v(E, k_{\mathrm{cyc}}) = \prod_{w|v} H^1(k^{ur}_{w,cyc}, C_w),$$

where w varies over primes of k_{cyc} and $k^{ur}_{w,cyc}$ denotes the maximal unramified extension of $k_{w,cyc}$. The Selmer group $\mathrm{Sel}(E/k_{\mathrm{cyc}})$ is defined as the kernel of the map

$$H^1(k_\Sigma/k_{\mathrm{cyc}}, E_{p^\infty}) \longrightarrow \bigoplus_{w\in\Sigma} J_v(E, k_{\mathrm{cyc}})$$

For the equivalence between the above definition of the Selmer group and the definition considered in Section 1, we refer the reader to [12, p. 42]. We further mention that in [12] the case of $k = \mathbb{Q}$ is considered. But the equivalence of the two definitions of the Selmer groups considered over the cyclotomic extension of a more general number field can be proved similarly. For any subset Σ_0 of Σ not containing the primes of k lying above p, the imprimitive Selmer group $\mathrm{Sel}^{\Sigma_0}(E/k_{\mathrm{cyc}})$ associated to the set Σ_0 is defined similarly by ignoring the local Galois cohomology groups at primes in the set Σ_0. The Selmer group $\mathrm{Sel}^{\Sigma_0}(E[p]/k_{\mathrm{cyc}})$ associated to the residual representation $E[p]$ is analagously defined by replacing the group E_{p^∞} by $E[p]$ and $E_{p^\infty}/F^+E_{p^\infty}$ by $(E_{p^\infty}/F^+E_{p^\infty})[p]$.

Let E_1 and E_2 be two elliptic curves defined over k with good ordinary reduction at the primes above p, and such that $E_1[p] \cong E_2[p]$ as a $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$-module. Let N_1 and N_2 be the conductor of E_1 and E_2 respectively and $\bar{N}$ denote the prime to p part of the conductor of $E_1[p]$. For the rest of the section, the set Σ will denote the finite set of primes v of k such that v satisfies one of the following four conditions: (i) $v|N_1N_2$, (ii) $v|m$, (iii) $v|p$, (iv) v is an infinite prime of k. We shall also assume that m is coprime to N_1N_2.

Definition 3.1. Let $\Sigma(E_j)$ denote the subset of Σ of primes v such that $v \nmid \bar{N}$ and E_j has split multiplicative reduction at v for $j = 1, 2$. In the case $p = 3$, we shall further assume that $\Sigma(E_j)$ also contains the finite primes v of k which satisfy the following conditions: (i) $v \mid N_j/\bar{N}$, (ii) E_j has additive reduction at v and (iii) the local Tamagawa number c_v is not a 3-adic unit.

Let Σ_0 be a subset of $\Sigma(E_1) \cup \Sigma(E_2)$.

The following well known lemma will be crucial for what follows.

Lemma 3.2. *Let M be a discrete $\mathbb{Z}_p[[\Gamma_k]] \cong \mathbb{Z}_p[[X]]$-module such that its Pontryagin dual $\widehat{M}$ is a finitely generated and torsion $\mathbb{Z}_p[[\Gamma_k]]$-module. Let*

$f(X)$ be a generator of the characteristic ideal of $\widehat{M}$. If M^Γ is finite, then $\chi(\Gamma_k, M)$ exists and we have

$$f(0) = \chi(\Gamma_k, M).$$

Proof. See [9, Lemma 4.2] □

Remark 3.3. We remark that in particular the above lemma says that if $\chi(\Gamma_k, M)$ exists, then it is always an integer. Further, it follows from this lemma and the structure of the torsion $\mathbb{Z}_p[[\Gamma_k]]$-module $\widehat{M}$, that if $\chi(\Gamma_k, M) = 1$, then M is finite. In particular, if $\chi(k_{\mathrm{cyc}}/k, E_1; \Sigma_0) = 1$ then $\mathrm{Sel}^{\Sigma_0}(E_1/k_{\mathrm{cyc}})$ is finite. In fact, the finiteness of $\mathrm{Sel}^{\Sigma_0}(E_1/k_{\mathrm{cyc}})$ implies that $\mathrm{Sel}^{\Sigma}(E_1/k_{\mathrm{cyc}}) = 0$ (cp. [9, Prop. 4.14]).

Theorem 3.4. *Suppose that*

(a) $E_1(k)[p] = 0$.
(b) $\Sigma(E_2) \subset \Sigma_0 \subset \Sigma(E_1) \cup \Sigma(E_2)$.

If $\chi(F_\infty/k, E_1; \Sigma_0) = 1$, then $\Sigma_0 = \varnothing$ and

$$\chi(F_\infty/k, E_2; \Sigma_0) = \chi(F_\infty/k, E_1) = \chi(F_\infty/k, E_2) = 1.$$

Proof. Suppose that $\chi(F_\infty/k, E_1; \Sigma_0) = 1$. As the cyclotomic Euler characteristic is integral, Corollary 2.8 along with the hypothesis $\chi(F_\infty/k, E_1; \Sigma_0) = 1$, implies that $\chi(k_{\mathrm{cyc}}/k, E_1; \Sigma_0) = 1$ and $\Sigma_3(E_1) = \varnothing$. Recall that $\Sigma_3(E_j)$ for $j = 1, 2$, is defined (see Definition 2.4) as the set of finite primes v of k such that $v|m$ and the corresponding reduced curve at v has a rational point of order p. Note that $L_v(E_2, 1)$ is not a p-adic unit if and only if the reduced curve at v has a point of order p (see Lemma 2.5). Thus for every $v|m$, we have that $L_v(E_1, 1)$ is a p-adic unit. Since $E_1[p] \cong E_2[p]$ and m is coprime to N_1N_2, we get that for every $v|m$, $P_v(E_1, T) \equiv P_v(E_2, T) \bmod p$. This implies that $L_v(E_2, 1)$ is also a p-adic unit. This implies that $\Sigma_3(E_2) = \varnothing$.

Since $\chi(k_{\mathrm{cyc}}/k, E_1; \Sigma_0) = 1$, from Remark 3.3 we have that $\mathrm{Sel}^{\Sigma_0}(E_1/k_{\mathrm{cyc}}) = 0$. We shall show that $\mathrm{Sel}^{\Sigma_0}(E_2/k_{\mathrm{cyc}}) = 0$ as well. To do this, it is convenient to use the second definition of the Selmer group. Consider the natural map

$$\mathrm{Sel}^{\Sigma_0}(E_j[p]/k_{\mathrm{cyc}}) \xrightarrow{a_j} \mathrm{Sel}^{\Sigma_0}(E_j/k_{\mathrm{cyc}})[p].$$

It follows from the proof of [12, Prop. 2.8] that a_j is injective for $j = 1, 2$. Since $\mathrm{Sel}^{\Sigma_0}(E_1/k_{\mathrm{cyc}}) = 0$, we get that $\mathrm{Sel}^{\Sigma_0}(E_1/k_{\mathrm{cyc}})[p] = 0$ and therefore $\mathrm{Sel}^{\Sigma_0}(E_1[p]/k_{\mathrm{cyc}}) = 0$. This implies that $\mathrm{Sel}^{\Sigma_0}(E_2[p]/k_{\mathrm{cyc}}) = 0$. Let $v \in \Sigma \setminus \Sigma_0$ be a finite prime of k such that $v \nmid p$. Assume that w is a prime of k_{cyc} lying above v. Consider the map

$$H^1(k_{w,cyc}, E_2[p]) \xrightarrow{g_w} \longrightarrow H^1(k_{w,cyc}, E_{2,p^\infty})[p].$$

The kernel of g_w is given by $H^0(k_{w,cyc}, E_{2,p^\infty})/p$. We claim that g_w is injective, and prove this statement by considering the following different cases:
a) Suppose that E_2 has good reduction at v. Then it follows from the proof of [8, Lemma 4.1.2] that $H^0(k_{w,cyc}, E_{2,p^\infty})$ is divisible, and g_w is injective.

b) If E_2 has nonsplit multiplicative reduction at v, then $H^0(k_{w,cyc}, E_{2,p^\infty}) = 0$ (see [13, Prop. 5.1(iii)]) and again g_w is injective for such primes.
c) Next, suppose that E_2 has additive reduction at v. We have two further subcases here, depending on whether $v \nmid N_2/\bar{N}$ and $v \mid N_2/\bar{N}$. Assume first that $v \nmid N_2/\bar{N}$. We then have $\mathrm{ord}_v(N_2) = \mathrm{ord}_v(\bar{N})$ and the conclusion follows from [8, Prop. 4.1.2]. Suppose now that $v \mid N_2/\bar{N}$ and either $p \geq 5$, or $p = 3$ and the local Tamagawa number c_v is a 3-adic unit. The vanishing of $H^0(k_{w,cyc}, E_{p^\infty})$ then follows by [13, Prop. 5.1(iii)], and hence g_w is injective. Finally, we are left with the case $p = 3$ and c_v is not a 3-adic unit. In this case, the prime v belongs to Σ_0 which is a contradiction, since we have started with v in $\Sigma \setminus \Sigma_0$. Hence the claim is proved.

We now consider the case when $v|p$. Consider the map

$$H^1(k^{ur}_{w,cyc}, E_{2,p^\infty}/F_v^+ E_{2p^\infty}[p]) \xrightarrow{g_w} H^1(k^{ur}_{w,cyc}, E_{2,p^\infty}/F_v^+ E_{2,p^\infty})[p].$$

We have $H^0(k^{ur}_{w,cyc}, E_{2,p^\infty}/F_v^+ E_{2,p^\infty}) = E_{2,p^\infty}/F_v^+ E_{2,p^\infty}$, which is a divisible group . Thus g_w is injective, and this shows that a_2 is surjective. Therefore $\mathrm{Sel}^{\Sigma_0}(E_2/k_{\mathrm{cyc}})[p] = 0$, as $\mathrm{Sel}^{\Sigma_0}(E_2[p]/k_{\mathrm{cyc}}) = 0$. This implies that the Euler characteristic $\chi(F_\infty/k, E_2; \Sigma_0) = 1$. It also follows from Lemma 2.6 that $\chi(F_\infty/k, E_1) = \chi(F_\infty/k, E_2) = 1$.

Let us now show that Σ_0 is empty in this case. We prove this by showing that $\Sigma(E_2) = \varnothing$ and $\Sigma_0 \cap \Sigma(E_1)$ is empty. Note first that when $p \geq 5$, the set $\Sigma(E_2)$ does not contain a prime of additive reduction. If $v \in \Sigma(E_2)$, and E_2 has split multiplicative reduction at v, then v is in $\Sigma_1(E_2)$. But $\chi(F_\infty/k, E_2, \Sigma_0) = 1$ along with Lemma 2.5 then yields a contradiction. Next suppose that $p = 3$ and E_2 has additive reduction at v. Then as v is in $\Sigma(E_2)$, c_v is not a 3-adic unit. The triviality of $\chi(F_\infty/k, E_2, \Sigma_0)$ then implies that $\chi(F_{\mathrm{cyc}}/k, E_2) = 1$. Hence it follows from the explicit formula for the Euler characteristic of Selmer group (cp. [3, Thm. 3.3]) that c_v is a 3-adic unit. This is again a contradiction and we thus obtain that $\Sigma(E_2) = \varnothing$. By a similar argument we have that $\Sigma(E_1) \cap \Sigma_0$ is empty. Thus we get that Σ_0 is empty, since by assumption $\Sigma_0 \subset \Sigma(E_1) \cup \Sigma(E_2)$.

□

Remark 3.5. In hypothesis (b) above, if the subset $\Sigma(E_2)$ of Σ_0 is replaced by $\Sigma(E_1)$, then the conclusion is that $\chi(F_\infty/k, E_1; \Sigma_0) = 1$, if $\chi(F_\infty/k, E_2, \Sigma_0) = 1$. In particular, whenever Σ_0 contains either $\Sigma(E_1)$ or $\Sigma(E_2)$, and the corresponding imprimitive Euler characteristic is one, then we obtain that

$$\chi(F_\infty/k, E_1) = \chi(F_\infty/k, E_2) = 1.$$

The next corollary is a consequence of the symmetry of relation $E_1[p] \cong E_2[p]$.

Corollary 3.6. *Suppose that*

(a) $E_1(k)[p] = 0$.
(b) $\Sigma_0 = \Sigma(E_1) \cup \Sigma(E_2)$.

Then $\chi(F_\infty/k, E_1; \Sigma_0) = 1$ *if and only if* $\chi(F_\infty/k, E_2; \Sigma_0) = 1$. *Moreover if* $\chi(F_\infty/k, E_1; \Sigma_0) = 1$ *then* $\Sigma_0 = \varnothing$.

Proof. The assertion is clear from the above remark. □

Next we consider an application of Theorem 3.4 in the case $p = 3$. Let E_1 and E_2 be elliptic curves defined over $\mathbb{Q}$ with good ordinary reduction at 3. Put $K = K_1 = \mathbb{Q}(\mu_3)$ and $F = F_1 = K(m^{1/3})$.

Let $k \subset F$ be a field extension of $\mathbb{Q}$. To keep track of field extensions, we shall add the superscript k to the finite set of primes Σ and write it as Σ^k. Similarly we shall write Σ_0^k to denote the corresponding subset Σ_0 of Σ. The sets $\Sigma^k(E_j)$ for $j = 1, 2$ are defined as in Definition 3.1, and we define Σ_3^k as the set of primes v in k such that $v \mid m$, $v \nmid p$ and (any of) the reduced curve has a point of order p in the residue field $\mathbb{F}_v$. Note that if E_1 has a point of order p in $\mathbb{F}_v$ for a prime $v|m$ and $v \nmid p$, then the same is true for E_2.

We continue to assume that m is coprime to N_1N_2, so that the reduction type of E_1 and E_2 does not change in F_∞. In particular, this assumption implies that the sets $\Sigma^k(E_j)$ contain precisely those primes of k which divide the primes in the set $\Sigma^{\mathbb{Q}}(E_j)$ for every $k \subset F_\infty$. Since F/K is a p-extension, we have that the set Σ_3^F contains the primes lying above the primes in the set Σ_3^K.

Let $\Delta_{\mathbb{Q}(\mu_3)}$ denote the fundamental discriminant of $\mathbb{Q}(\mu_3)$. For a number field $k \subset F$, let $L_S(E_j/k, s)$ denote the imprimitive L-function associated to E_j for $j = 1, 2$ over k, where we have removed the local L-factors at the primes in the set S, for the usual L-function $L(E_j, s)$ associated to E_j. Suppose that τ is a two dimensional representation of $\mathrm{Gal}(F/\mathbb{Q})$ with coefficients in $\mathbb{Z}_p$. Then $L_S(E_j, \tau, s)$ denote the twist of the corresponding imprimitive L-function. Let $\Omega_{E_j}^+$ and $\Omega_{E_j}^-$ denote the Néron periods associated to E_j.

Lemma 3.7. *Suppose that one of the following conditions hold: i) There is a prime* v *of* $\mathbb{Q}$ *such that* E_1 *has nonsplit multiplicative reduction at* v*, ii) There is a prime* v *of* K *such that* E_1 *has additive reduction at* v *and* c_v *is a 3-adic unit, iii)* $E_1[3]$ *is an irreducible* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$*-module and* $\bar{N}$ *is squarefree. Then we have that* $H^0(F, E_1[3]) = 0$.

Proof. If i) holds, then as the reduction type does not change in K, there exists a prime in K, which we again denote by v, such that E_1 has nonsplit multiplicative reduction at v. By [13, Prop. 5.1(iii)], $E_{1,3^\infty}(K) = 0$. Further, it is clear from the proof of [13, Prop. 5.1(iii)] that if v is a prime of K where E_1 has additive reduction then $E_{1,3^\infty}(K_v) \neq 0$ if and only if c_v is not a 3-adic unit. If hypothesis ii) holds then c_v is 3-adic unit and therefore $E_{1,3^\infty}(K) = 0$. If iii) holds, then noting that $\mathbb{Q}(\mu_3) = \mathbb{Q}(\sqrt{-3})$, it follows from [6, Lemma 3.24], that the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{-3}))$-module $E_1[p]$ is irreducible. Therefore $H^0(K, E_1[p]) = 0$. Since F/K is a degree 3 extension, we have that $H^0(F, E_1[3]) = 0$. □

Now, suppose that $\Sigma_0^K = \Sigma^K(E_1) \cup \Sigma^K(E_2)$. We show that when $\Sigma_0 = \varnothing$, then under additional hypotheses, if an algebraic special value of the complex

L-function of E_1 over $K = \mathbb{Q}(\mu_3)$ is a 3-adic unit, then the same holds true for the corresponding special value of E_2 over K.

Let $\sigma = \mathbf{1} \oplus \epsilon$ be the Artin representation given by the sum of the trivial character and the nontrivial character of $\mathrm{Gal}(\mathbb{Q}(\mu_3)/\mathbb{Q})$. Let $P_p(E_j, \sigma, T)$, $j = 1, 2$ (resp. $P_p(\sigma, T)$) be the characteristic polynomial associated to the twist of E_j by σ, (resp. to σ) at the prime p. Denote by u_j and w_j respectively the p-adic unit root and non p-adic unit root of the characteristic polynomial $P_p(E_j, T)$. Let $\Omega^+_{E_j}$ and $\Omega^-_{E_j}$ be the Néron periods associated to elliptic curve E_j. Put,

$$\mathcal{L}_j(\sigma) := \epsilon_p(\sigma) \times u_j^{-v_p(N_\sigma)} \times \frac{P_p(\sigma, u_j^{-1})}{P_p(\sigma, w_j^{-1})} \times \frac{L_{\{p,q|m\}}(E_j, \sigma, 1)}{\Omega^+_{E_j}\Omega^-_{E_j}}, \tag{4}$$

where $\epsilon_p(\sigma)$ denotes the local epsilon factor of σ as in [5] and N_σ denotes the conductor of σ. Further $L_{\{p,q|m\}}(E_j, \sigma, s)$ is the twisted L-function $L(E_j, \sigma, s)$ with local L-factors at the primes dividing p and m removed. We mention that $\mathcal{L}_j(\sigma)$ is denoted by $\mathcal{L}_{E_j}(\sigma)$ in [5], and by $R(\sigma)$ in [1].

Theorem 3.8. *Suppose that*

(a) $E_1[3]$ *is an irreducible* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-module.*
(b) Σ_0^K *is empty.*
(c) $\bar{N}$ *is squarefree, and* $N_1/\bar{N}$ *(resp.* $N_2/\bar{N}$*) and* $\bar{N}$ *are coprime.*
(d) $\chi(F_\infty/\mathbb{Q}(\mu_3), E_1) = 1$.

Then $\frac{L(E_1/\mathbb{Q}(\mu_3),1)\sqrt{|\Delta_{\mathbb{Q}(\mu_3)}|}}{\Omega^+_{E_1}\Omega^-_{E_1}}$ *is a* 3*-adic unit if and only if* $\frac{L(E_2/\mathbb{Q}(\mu_3),1)\sqrt{|\Delta_{\mathbb{Q}(\mu_3)}|}}{\Omega^+_{E_2}\Omega^-_{E_2}}$ *is a* 3*-adic unit. Moreover if* $\frac{L(E_1/\mathbb{Q}(\mu_3),1)\sqrt{|\Delta_{\mathbb{Q}(\mu_3)}|}}{\Omega^+_{E_1}\Omega^-_{E_1}}$ *is a* 3*-adic unit, then* $L(E_1/F, 1)$ *and* $L(E_2/F, 1)$ *do not vanish, where we recall that* $F = \mathbb{Q}(\mu_3, m^{1/3})$.

Proof. From Lemma 3.7 and assumption (a) it follows that $E_j(F)[3] = 0$ for $j = 1, 2$. Since $\chi(F_\infty/\mathbb{Q}(\mu_3), E_1) = 1$ it follows from Corollary 3.6 that $\chi(F_\infty/\mathbb{Q}(\mu_3), E_j) = 1$ for $j = 1, 2$. This implies that $\mathrm{Sel}(E_j/F_\infty) = 0$, and hence $\chi(F_\infty/F, E_j) = 1$ (see Corollary 2.8). By Remark 3.3 we get that $\mathrm{Sel}(E_j/F_{\mathrm{cyc}}) = 0$ for $j = 1, 2$. From Lemma 3.7 and assumption (a) we have that $E(F)[3] = 0$. Using the exact formula for the Euler characteristic of $\mathrm{Sel}(E/F_{\mathrm{cyc}})$ and vanishing of the group $E(F)[3]$, we obtain that $\tilde{E}(\mathbb{F}_3)[p] = 0$, where $\tilde{E}$ is the reduced curve at a prime $v|3$, and $\mathbb{F}_v$ is the residue field at v. To simplify notation, put

$$\mathcal{L}_j := \frac{L(E_j/\mathbb{Q}(\mu_3), 1)\sqrt{|\Delta_{\mathbb{Q}(\mu_3)}|}}{\Omega^+_{E_j}\Omega^-_{E_j}},\ j = 1, 2. \tag{5}$$

From Theorem 3.4, we get that $\chi(F_\infty/\mathbb{Q}(\mu_3), E_1) = \chi(F_\infty/\mathbb{Q}(\mu_3), E_2) = 1$. It is easily seen that $\chi(F_\infty/\mathbb{Q}(\mu_3), E_1) = 1$ implies that the local Euler factor $L_v(E_1/\mathbb{Q}(\mu_3), 1)$ is a 3-adic unit for a prime $v \mid m$ such that $v \nmid p$. A similar assertion holds for $L_v(E_2/\mathbb{Q}(\mu_3), 1)$ at a prime $v \mid m$ such that $v \nmid p$. Using

this fact, and the vanishing of $\tilde{E}(\mathbb{F}_3)[3]$, it is shown in the proof (See top of p. 619) of [1, Thm. A.1], that

(6) $\mathcal{L}_j$ is a 3-adic unit if and only if $\mathcal{L}_j(\sigma)$ is a 3-adic unit.

On the other hand, under the hypotheses of the theorem, it follows from (cp. [18, Lemma 5.3]), that $\mathcal{L}_1(\sigma)$ is a 3-adic unit if and only if $\mathcal{L}_2(\sigma)$ is a 3-adic unit. Thus we conclude that $\mathcal{L}_1$ is a 3-adic unit if and only if $\mathcal{L}_2$ is. The final assertion follows from Theorem A.1 of [1]. □

Corollary 3.9. *If the assumptions of Theorem 3.8 hold and the Birch and Swinnerton-Dyer conjecture is true for E_1 over $\mathbb{Q}(\mu_3)$, then $E_1(F)$ and $E_2(F)$ are finite, and the complex L-functions associated to E_1 and E_2 over F do not vanish at 1. In particular the analytic rank equals the algebraic rank for both E_1 and E_2 over F.*

Proof. The assumptions of Theorem 3.8 and Corollary 3.6 imply that $\chi(F_\infty/\mathbb{Q}(\mu_3), E_j) = 1$ for $j = 1, 2$. Thus we have that $\mathrm{Sel}(E_j/F_\infty) = 0$ for $j = 1, 2$ (see [14, Prop. 4.12]). We once again mention that in [14] it is assumed that $p \geq 5$. But a similar result hold for $p = 3$ under the assumption that N_1N_2 is coprime to m. Thus it follows that $E_1(F)$ and $E_2(F)$ are finite. Since the Birch and Swinnerton-Dyer conjecture hold for E_1 over $\mathbb{Q}(\mu_3)$ and $\chi(F_\infty/\mathbb{Q}(\mu_3), E_1) = 1$, from [5, Prop. 5.13(a)] it follows that $\mathcal{L}_1(\sigma)$ is a 3-adic unit. From (6) we have that $\mathcal{L}_1$ is 3-adic unit. Now the assertion follows from Theorem 3.8.

□

Remark 3.10. Note that the above theorem has been proved using (6). We emphasize that even though E_1 is congruent to E_2 mod 3, it is not necessary that $\mathcal{L}_1(\sigma)$ and $\mathcal{L}_2(\sigma)$ are congruent mod 3. We shall illustrate this later with numerical examples.

4. Congruence for dihedral extensions

In this section, we discuss how the results in [18] allow us to prove a version of Theorems 3.4 and 3.8 for certain dihedral extensions. Let p be an odd prime, and let now $K = \mathbb{Q}(\sqrt{-d})$ be a totally imaginary quadratic extension of $\mathbb{Q}$, and let F be an extension of degree p^n over K such that $F/\mathbb{Q}$ is a dihedral extension. Let $\mathfrak{f}_{F/K}$ be the conductor of F/K, and D be the fundamental discriminant of $K/\mathbb{Q}$. Assume that $\mathfrak{f}_{F/K}$ is prime to D', where D' denotes the prime to p part of D. We shall assume that $\mathfrak{m} := D \cdot \mathrm{Norm}_{\mathrm{K}/\mathbb{Q}}\mathfrak{f}_\chi$ is coprime to N_1N_2. This integer $\mathfrak{m}$ will now play the role of m that was considered in the False Tate extension. Let $k \subset F$ be a field extension of $\mathbb{Q}$. As before, let Σ^k be a finite set of primes of k containing the prime divisors of p, the primes dividing $\mathfrak{m}$, the prime divisors of N_1N_2 and the infinite primes. Let $\Sigma_0^k \subset \Sigma^k$ be a finite set of finite primes of K such that if $v \mid p$ then $v \notin \Sigma_0^k$. The sets $\Sigma^k(E_j)$ is defined as in Definition 3.1, and we define Σ_3^k as the set of primes v

in k such that $v \mid \mathfrak{m}$, $v \nmid p$ and (any of) the reduced curve has a point of order p in the residue field $\mathbb{F}_v$. Now suppose that

$$\Sigma_0^k = \Sigma^k(E_1) \cup \Sigma^k(E_2) \cup \Sigma_3^k. \tag{7}$$

Theorem 4.1. *Let $k \subset F$ where F is a dihedral extension of $\mathbb{Q}$ of degree $2p^n$. Assume that $E_1(K)[p] = 0$. Then $\chi(k_{\mathrm{cyc}}/k, E_1; \Sigma_0^k) = 1$ if and only if $\chi(k_{\mathrm{cyc}}/k, E_2; \Sigma_0^k) = 1$.*

Proof. The key point is to note that $\chi(k_{\mathrm{cyc}}/k, E_1; \Sigma_0^k) = 1$, is equivalent to the vanishing of the Selmer group $\mathrm{Sel}^{\Sigma_0^k}(E_1/k_{\mathrm{cyc}})$ (see Remark 3.3). Arguing as in the proof of Theorem 3.4, it can be seen that $\mathrm{Sel}^{\Sigma_0^k}(E_1/k_{\mathrm{cyc}})$ vanishes if and only if $\mathrm{Sel}^{\Sigma_0^k}(E_2/k_{\mathrm{cyc}})$ vanishes. □

In order to prove the analog of Theorem 3.8, we first establish the following lemma. Consider the Artin representation $\sigma = \mathbf{1} \oplus \epsilon$, where ϵ is the nontrivial character of $\mathrm{Gal}(K/\mathbb{Q})$. Let $P_p(E_j, \sigma, T)$, $j = 1, 2$, (resp. $P_p(\sigma, T)$) be the characteristic polynomial associated to the twist of E_j by σ, (resp. to σ) at the prime p. Denote by u_j (resp. w_j) the p-adic unit root (resp. non p-adic unit root) of the characteristic polynomial $P_p(E_j, T)$.

Lemma 4.2. *Suppose that $\tilde{E}_j(\mathbb{F}_v)[p]$, $j = 1, 2$, is trivial for the primes v of K dividing p. Then*

$$\frac{P_p(\sigma, u_j^{-1})}{P_p(\sigma, w_j^{-1})} P_p(E_j, \sigma, 1/p)$$

is a p-adic unit.

Proof. There are three cases:

Case i): p is ramified in K. In this case, $P_p(\sigma, T) = (1 - T)$ and the proof is similar to that in [5, Lemma 5.14].

Case ii): p splits in K. We then have $P_p(\sigma, T) = (1 - T)^2$ and the proof is again similar to *loc.cit.*

Case iii): p is inert in K. We have $P_p(\sigma, T) = (1 - T)(1 + T)$. By a computation similar to *loc.cit.*, it is easily seen that up to a p-adic unit, we have

$$P_p(\sigma, u_j^{-1}) = (1 - a_p(j) + p)(1 + a_p(j) + p), \text{ and } P_p(\sigma, w_j^{-1}) = 1/p^2,$$

where $a_p(j)$ is the p-th Fourier coefficient of the modular form associated to the curve E_j. Further, $P_p(E_j, \sigma, T) = P_p(E_j, T) P_p(E_j, \epsilon, T)$. Since p is inert in K we have that $\epsilon(\mathrm{Fr}_p) = -1$, where Fr_p is the Frobenius at p. Thus we have that,

$$P_p(E_j, \sigma, 1/p) = \frac{(1 + a_p(j) + p)(1 - a_p(j) + p)}{p^2}.$$

Therefore, up to a p-adic unit, we get

$$\frac{P_p(\sigma, u_j^{-1})}{P_p(\sigma, w_j^{-1})} P_p(E_j, \sigma, 1/p) = ((1 - a_p(j) + p) \cdot (1 + a_p(j) + p))^2,$$

Since $L_p(E_j,\sigma,s) = P_p(E_j,\sigma,1/p^s)^{-1}$, we have for $j=1,\,2$,

$$((1-a_p(j)+p)\cdot(1+a_p(j)+p))^2 = p^4 \times (L_p(E_j,\sigma,1))^{-2}.$$

Let v be the unique prime of K above p. Then by the Artin formalism, we have

$$L_p(E_j,\sigma,1)^{-1} = L_v(E_j/K,1)^{-1} = \frac{|\tilde{E}_j(\mathbb{F}_v)|}{\mathrm{Norm}_{K/\mathbb{Q}}(p)} = \frac{|\tilde{E}_j(\mathbb{F}_v)|}{p^2}.$$

Therefore, we obtain

$$\frac{P_p(\sigma,u_j^{-1})}{P_p(\sigma,w_j^{-1})} P_p(E_j,\sigma,1/p) = |\tilde{E}_j(\mathbb{F}_v)|^2$$

up to a p-adic unit. The conclusion now follows from the hypothesis.

□

Analogous to the proof of Theorem 3.8, we have the L-values $\mathcal{L}_j$ (cp. (5)) and the twisted p-adic L-values $\mathcal{L}_j(\sigma)$ (which is denoted by $R(\sigma)$ in [18]). The following is now the analog of Theorem 3.8.

Theorem 4.3. *Suppose that*

(a) $E_1[p]$ *is an irreducible* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$*-module and* $E(K)[p]=0$.
(b) $\Sigma_0^K = \varnothing$.
(c) $\bar{N}$ *is squarefree, and* $N_1/\bar{N}$ *(resp.* $N_2/\bar{N}$*) is coprime to* $\bar{N}$.
(d) $\chi(K_{\mathrm{cyc}}/K,E_1)=1$.

Then $\chi(F_{\mathrm{cyc}}/F,E_j)=1,\ j=1,\,2$, *and the* L*-value* $\frac{L(E_1/K,1)\sqrt{|\Delta_K|}}{\Omega^+_{E_1}\Omega^-_{E_1}}$ *is a* p*-adic unit if and only if* $\frac{L(E_2/K,1)\sqrt{|\Delta_K|}}{\Omega^+_{E_2}\Omega^-_{E_2}}$. *Moreover, if* $\frac{L(E_1/K,1)\sqrt{|\Delta_K|}}{\Omega^+_{E_1}\Omega^-_{E_1}}$ *is a* p*-adic unit, then* $L(E_1/F,1)$ *and* $L(E_2/F,1)$ *do not vanish.*

Proof. As in the proof of Theorem 3.8, assumptions (b), (d) and Theorem 4.1 allow us to conclude that $\chi(K_{\mathrm{cyc}}/K,E_j)=1$ for $j=1,2$. This in particular implies that the Selmer groups $\mathrm{Sel}(K_{\mathrm{cyc}}/k,E_j)$ vanish for $j=1,2$, and hence the μ-invariant and λ-invariant are both zero for E_1 and E_2. We remark that the assumption $(\mathfrak{m},N_1N_2)=1$ implies that the primes in F of bad reduction are unramified. Further, under assumption (b), we see that if v is a prime of K such that $v|\mathfrak{m}$ and $v\nmid p$, then $\tilde{E}_j(\mathbb{F}_v)[p]=0$. Since F/K is a p-extension, a similar conclusion holds for the primes of F dividing $\mathfrak{m}$. This implies that $\Sigma_0^F=\varnothing$, and by [13, Thm. 3.1], we obtain that the λ and μ-invariants for $\mathrm{Sel}(F_{\mathrm{cyc}}/F,E_j)$ are also zero. In particular, the Selmer groups $\mathrm{Sel}(F_{\mathrm{cyc}}/F,E_j)$ vanish and we have $\chi(F_{\mathrm{cyc}}/F,E_j)=1,\ j=1,\,2$.

Since, $\chi(K_{\mathrm{cyc}}/K,E_j)=1$ for $j=1,2$, using the assumption $E(K)[p]=0$, it follows from the formula for the Euler characteristic of $\mathrm{Sel}(K_{\mathrm{cyc}}/K,E_j)$ that $\tilde{E}_j(\mathbb{F}_v)[p]=0$ for all primes $v|p$ of K. From Lemma 4.2, we then see that $\frac{P_p(\sigma,u_j^{-1})}{P_p(\sigma,w_j^{-1})}\cdot P_p(E_j,\sigma,1/p)$ is a p-adic unit. Using this fact, assertion (6) can be proved in this case as well by a method similar to the proof [1, Thm. A.1].

The conclusion now follows by an argument analogous to that in Theorem 3.8. This completes the proof of the theorem. □

Finally we remark that we need the extra assumption in the above theorem that $E(K)[p] = 0$. If $K = \mathbb{Q}(\mu_3)$ and $p = 3$ then the assumption that $E_1[3]$ is an irreducible $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-module implies that $E(F)[p] = E(K)[p] = 0$(see Lemma 3.7). We do not have an analog of Lemma 3.7 for a more general quadratic imaginary extension K.

5. Numerical examples

The following numerical examples illustrate the results proved in this article, especially Theorem 3.8. We are very grateful to Tim Dokchitser for his help with the numerical computations.

Let E_1 be the elliptic curve $11A3$ and E_2 be the elliptic curve $77C1$ in Cremona's tables. Since there exists no 3-isogeny of E_1 over $\mathbb{Q}$, we have that $E_1[3]$ is an irreducible module over $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. By Lemma 3.7, $E_j(F)[3] = 0$ for $j = 1\,, 2$. We have $\Sigma(E_1) = \phi$, and the elliptic curve E_2 has nonsplit multiplicative reduction at 7 (cp. [5, Table 3-77C1]). Thus $\Sigma(E_2) = \phi$. We also have $\mathrm{Sel}(E_1/K_{\mathrm{cyc}}) = 0$ (cp. [5]), and $\chi(K_{\mathrm{cyc}}/K, E_j) = 1$ for $j = 1$, 2 by Corollary 3.6. Let m be an integer coprime to 3 and 77 such that if $v|m$, then the local L-factor $L_v(E_1/K, 1)$ is a 3-adic unit. Then we get that the Euler characteristic $\chi(F_\infty/\mathbb{Q}(\mu_3), E_1) = 1$. From [14], we conclude that $\mathrm{Sel}(E_j/F_\infty) = 0$, for $j = 1$, 2. This implies that $\chi(F_\infty/\mathbb{Q}(\mu_3, m^{1/p}), E_j) = 1$. It is known that $\frac{L(E_1/\mathbb{Q}(\mu_p),1)\sqrt{|\Delta_{\mathbb{Q}(\mu_p)}|}}{\Omega^+_{E_1}\Omega^-_{E_1}}$ is a 3-adic unit, as can be checked using the tables in [5]). Thus the assertion of the above theorem holds for E_2.

The above example is obtained using the result on congruence between modular forms by raising the level [7]. We next consider the elliptic curves 203A1 and 203C1 from Cremona's tables, and $p = 3$. In this case, Tim Dokchitser has computed (using the Néron period) that $\mathcal{L}_1(\sigma) = 1 \bmod 3$ and $\mathcal{L}_2(\sigma) = 2 \bmod 3$ for $m = 2,\ 5$. Using this, it can be shown that $\mathcal{L}_1$ is a 3-adic unit if and only if $\mathcal{L}_2$ is a 3-adic unit. This example also illustrates Remark 3.10.

Here is another pair of elliptic curves namely $E_1 = 158C1$ and $E_2 = 158E2$, for which the special values are 3-adic units over $\mathbb{Q}(\mu_3)$. The residual representations at $p = 3$ are again irreducible with conductor equal to 158. Hence $\Sigma_0 = \varnothing$. Further $|\tilde{E}(\mathbb{F}_p)|$ is a 3-adic unit. We are grateful to T. Dokchitser for confirming computationally that $\mathcal{L}_j(\sigma)$ is indeed a 3-adic unit for $j = 1$, 2. By Lemma 4.2, we get that $\mathcal{L}_j$ is a 3-adic unit for $j = 1$, 2.

The pair of elliptic curves 106A1 and 106C1 are congruent mod 3. It turns out that the values $\mathcal{L}_j(\sigma)$ for $j = 1$, 2 for $m = 7$ are simultaneously non-3-adic units. Using this, it can be shown that $\mathcal{L}_j$ are also non-3-adic units. In fact, in this case, the reduced curves $\tilde{E}_1$ and $\tilde{E}_2$ have a point of order 3 at the prime 3, and therefore on using the formula for the Euler characteristic of the corresponding Selmer groups over F_∞ (see [14]), one obtains that the Euler characteristics are nontrivial.

Consider the following pair of elliptic curves E_1 and E_2 where $E_1 = 235A1$ and $E_2 = 235B1$, which are congruent mod 3. However, E_1 has rank 1 and E_2 has rank 0. Thus $\chi(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}, E_2)$ exists but $\chi(\mathbb{Q}_{\mathrm{cyc}}/\mathbb{Q}, E_1)$ is not defined. In this case, the set Σ_0 is nonempty as the prime $5 \nmid \bar{N}_j$ for $j = 1, 2$, and E_1 has split multiplicative reduction at 5. This shows that our hypotheses are in fact essential. The pair of elliptic curves $E_1 = 11A1$ and $E_2 = 121C1$ which are congruent mod 3, also does not satisfy the hypothesis of Theorem 3.8. In this case it turns out that if we take $m = 3$ and $K = \mathbb{Q}(\mu_3)$ then $\mathcal{L}_1(\sigma)$ is a 3-adic unit. On the other hand $\mathcal{L}_2(\sigma) = 0$.

Finally, we remark that Rubin and Silverberg have shown that there are infinitely many elliptic curves E defined over $\mathbb{Q}$ with a given Galois module structure on $E[p]$ for $p = 3$ and $p = 5$ (see [17]). Using the level raising technique of [7], one knows that such congruences for Hecke eigenforms exist for all odd primes. We believe that our methods should carry over for Hecke eigenforms of weight 2 ordinary at p in general.

References

[1] T. Bouganis, Special values of L-functions and false Tate curve extensions, J. Lond. Math. Soc. (2) **82** (2010), no. 3, 596–620. MR2739058 (2012g:11120)

[2] J. H. Coates and S. Howson, Euler characteristics and elliptic curves. II, J. Math. Soc. Japan **53** (2001), no. 1, 175–235. MR1800527 (2001k:11215)

[3] J. Coates and R. Sujatha, *Galois cohomology of elliptic curves*, Tata Institute of Fundamental Research Lectures on Mathematics, **88**, Published by Narosa Publishing House, New Delhi, 2000. MR1759312 (2001b:11046)

[4] J. Coates, P. Schneider and R. Sujatha, Links between cyclotomic and GL_2 Iwasawa theory, Doc. Math. **2003**, Extra Vol., 187–215 (electronic). MR2046599 (2005c:11134)

[5] T. Dokchitser and V. Dokchitser, Computations in non-commutative Iwasawa theory, Proc. Lond. Math. Soc. (3) **94** (2007), no. 1, 211–272. MR2294995 (2008g:11106)

[6] H. Darmon, F. Diamond, and R. Taylor, Fermat's last theorem, in *Current developments in mathematics, 1995 (Cambridge, MA)*, 1–154, Int. Press, Cambridge, MA. MR1474977 (99d:11067a)

[7] F. Diamond, Congruences between modular forms: raising the level and dropping Euler factors, Proc. Nat. Acad. Sci. U.S.A. **94** (1997), no. 21, 11143–11146. MR1491976 (98m:11033)

[8] M. Emerton, R. Pollack, and T. Weston, Variation of Iwasawa invariants in Hida families, Invent. Math. **163** (2006), no. 3, 523–580. MR2207234 (2007a:11059)

[9] R. Greenberg, Iwasawa theory for elliptic curves, in *Arithmetic theory of elliptic curves (Cetraro, 1997)*, 51–144, Lecture Notes in Math., 1716, Springer, Berlin. MR1754686 (2002a:11056)

[10] R. Greenberg, Introduction to Iwasawa theory for elliptic curves, in *Arithmetic algebraic geometry (Park City, UT, 1999)*, 407–464, IAS/Park City Math. Ser., 9, Amer. Math. Soc., Providence, RI. MR1860044 (2003a:11067)

[11] R. Greenberg, On the structure of Selmer groups. Preprint (available on homepage).

[12] R. Greenberg and V. Vatsal, On the Iwasawa invariants of elliptic curves, Invent. Math. **142** (2000), no. 1, 17–63. MR1784796 (2001g:11169)

[13] Y. Hachimori and K. Matsuno, An analogue of Kida's formula for the Selmer groups of elliptic curves, J. Algebraic Geom. **8** (1999), no. 3, 581–601. MR1689359 (2000c:11086)

[14] Y. Hachimori and O. Venjakob, Completely faithful Selmer groups over Kummer extensions, Doc. Math. **2003**, Extra Vol., 443–478 (electronic). MR2046605 (2005b:11072)

[15] K. Kato, p-adic Hodge theory and values of zeta functions of modular forms, Astérisque No. **295** (2004), ix, 117–290. MR2104361 (2006b:11051)
[16] B. Mazur, Rational points of abelian varieties with values in towers of number fields, Invent. Math. **18** (1972), 183–266. MR0444670 (56 #3020)
[17] K. Rubin and A. Silverberg, Families of elliptic curves with constant mod p representations, in *Elliptic curves, modular forms, & Fermat's last theorem* (Hong Kong, 1993), 148–161, Ser. Number Theory, I, Int. Press, Cambridge, MA, 1995. MR1363500 (96j:11078)
[18] S. Shekhar and R. Sujatha, Congruence formula for certain dihedral twists. To appear in Transactions of AMS.
[19] V. Vatsal, Canonical periods and congruence formulae, Duke Math. J. **98** (1999), no. 2, 397–419. MR1695203 (2000g:11032)

Received March 24, 2013; accepted August 22, 2013

Sudhanshu Shekhar
Ruprecht-Karls-Universität Heidelberg, Mathematisches Institut
Im Neuenheimer Feld 288, 69120 Heidelberg
E-mail: sudhanshu@mathi.uni-heidelberg.de

R. Sujatha
Mathematics Department
1984, Mathematics Road, University of British Columbia
Vancouver, Canada V6T1Z2.
E-mail: sujatha@math.ubc.ca