Functiones et Approximatio
54.2 (2016), 241–250
doi: 10.7169/facm/2016.54.2.7

COMPARING LOCAL CONSTANTS OF ORDINARY ELLIPTIC CURVES IN DIHEDRAL EXTENSIONS

Sunil Chetty

Abstract: We establish, for a substantial class of elliptic curves, that the arithmetic local constants introduced by Mazur and Rubin agree with quotients of analytic root numbers.

Keywords: elliptic curves, rank, Selmer groups, parity conjecture.

1. Introduction

Let E/k be an elliptic curve over a number field k. Fix a rational prime $p > 3$ for which E is ordinary[1] and a quadratic extension K of k. Next, fix a character ρ of $\mathrm{Gal}(\overline{k}/K)$ of order p^n and let $\tau_\rho = \mathrm{ind}_{K/k}\,\rho$ and $\tau_1 = \mathrm{ind}_{K/k}\,1$ be the induced representations[2] from $\mathrm{Gal}(\overline{k}/K)$ to $\mathrm{Gal}(\overline{k}/k)$. With ρ we define $L = \overline{k}^{\ker\rho}$, a cyclic extension L/K of degree p^n, and we assume ρ is such that L/k is Galois and that the non-trivial element $c \in \mathrm{Gal}(K/k)$ acts on $g \in \mathrm{Gal}(L/k)$ via conjugation as $cgc^{-1} = g^{-1}$. Following [9] we refer to such extensions L/k as dihedral.

Let v denote a prime of K, u the prime of k below v, w a prime of L above v, and denote k_u, K_v and L_w for the completions at u, v, and w. We consider $\mathrm{Gal}(L_w/k_u) \leqslant \mathrm{Gal}(L/k)$, and we set $\tau_{\rho,u}$ (resp. $\tau_{1,u}$) to be τ_ρ (resp. τ_1) restricted to $\mathrm{Gal}(L_w/k_u)$.

For a self-dual complex representation τ of $\mathrm{Gal}(L/k)$, one has a conjectural functional equation for the completed L-function $\Lambda(E/k,\tau,s)$ (see [12, §21])

$$\Lambda(E/k,\tau,s) = \left(\prod_u W(E/k_u,\tau_u)\right)\Lambda(E/k,\tau,2-s), \tag{1.1}$$

This material is based upon work supported by the National Science Foundation under grant DMS-0457481. The author would like to thank Karl Rubin for his many helpful conversations on this material and reading of initial drafts of this paper.

2010 Mathematics Subject Classification: primary: 11G05; secondary: 11G07, 11G40

[1] There is, to date and to our knowledge, only one result [9, Theorem 5.7] at supersingular primes analogous to our considerations.

[2] Context will determine the field of values. See [7, §5] for a discussion of this.

with $W(E/k_u,\tau_u)\in\{\pm1\}$ and the product taken over places u of k. Even though the functional equation is conjectural, the $W(E/k_u,\tau_u)$ can often be made explicit.

In [9] Mazur and Rubin define constants δ_v, for each prime v of K, which relate the ρ-part and 1-part of the pro-p-Selmer $\mathrm{Gal}(\bar{k}/K)$-module $\mathcal{S}_p(E/L)$ (see §2.2)

$$\dim_{\overline{\mathbb{Q}}_p}\mathcal{S}_p(E/L)^\rho-\dim_{\overline{\mathbb{Q}}_p}\mathcal{S}_p(E/L)^1\equiv\sum_v\delta_v \mod 2. \tag{1.2}$$

Defining γ_u by $(-1)^{\gamma_u}=W(E/k_u,\tau_{\rho,u})/W(E/k_u,\tau_{1,u})$, for each prime u of k, the invariance of $\Lambda(E/k,\tau,s)$ under induction (see [12, §8]) and (1.1) give

$$\mathrm{ord}_{s=1}\Lambda(E/k,\tau_\rho,s)-\mathrm{ord}_{s=1}\Lambda(E/k,\tau_1,s)\equiv\sum_u\gamma_u \mod 2. \tag{1.3}$$

With the Shafarevic-Tate and Birch-Swinnerton-Dyer Conjectures in mind, the left-hand sides of (1.2) and (1.3) are equal, and so we aim to show in as many cases as possible that $\gamma_u=\sum_{v|u}\delta_v$.

Our main new result is Theorem 4.1, and it yields a new proof of a case of a relative version of the Parity Conjecture, Corollary 4.2. This Corollary is already known by different methods via work by de la Rochefoucauld in [1], Dokchitser and Dokchitser in [3] and [2], and can also be recovered from work by Greenberg in [5, §13]. Our calculations of δ_v in bad reduction also provide a new extension of the results of [9, §7-8] regarding growth in rank of $\mathcal{S}_p(E)$ over dihedral L/K, for example by relaxing the conditions in Theorem 8.5 of [9].

2. Local constants of elliptic curves

In this section we recall the relevant parts of [13] and [9].

2.1. Analytic local constants

We denote ω_u for the standard valuation on k_u and c_6 for the constant appearing in a simplified Weierstrauss model for E/k_u (see [17, §III.1]). For τ a representation of $\mathrm{Gal}(\overline{k}_u/k_u)$ with real-valued character, we call $W(E/k_u,\tau)\in\{\pm1\}$ the analytic local root number for the pair $(E/k_u,\tau)$. We call the constants $\gamma_u\in\mathbb{Z}/2\mathbb{Z}$ defined as quotients of local root numbers in §1 the analytic local constants.

When τ has finite image, set $\mathfrak{c}(\tau):=\det\tau(-1)$ and for two representations τ and τ' of $\mathrm{Gal}(\overline{k}_u/k_u)$ with finite image define $\langle\tau,\tau'\rangle:=\langle\mathrm{tr}(\tau),\mathrm{tr}(\tau')\rangle$, with the right-hand side the usual inner product on characters.

Let H be the unramified quadratic extension of k_u and η the unramified quadratic character of $\mathrm{Gal}(\overline{k}_u/k_u)$, i.e. the character of $\mathrm{Gal}(\overline{k}_u/k_u)$ with kernel $\mathrm{Gal}(\overline{k}_u/H)$. For $e=3,\ 4$, or 6 and $q\equiv-1 \mod e$, where $q=\#(k_u/u)$, let ϕ_e be a tamely ramified character of $\mathrm{Gal}(\overline{k}_u/H)$ with $\phi_e|_{\mathcal{O}_H^\times}$ of exact order e and such that $\sigma_e=\mathrm{ind}_{H/k}\phi_e$ is irreducible and symplectic. For θ the unramified quadratic character of $\mathrm{Gal}(\overline{k}_u/H)$ set $\hat{\sigma}_e:=\mathrm{ind}_{H/k_u}(\phi_e\theta)$, which is a dihedral representation of $\mathrm{Gal}(\overline{k}_u/k_u)$ (see p. 316-318 of [13]).

Define a representation σ_{E/k_u} by applying the results of [12, §4] to

$$\sigma_{E/k_u,\ell} : \mathrm{Gal}(\overline{k}_u/k_u) \to \mathrm{GL}(V_\ell(E)^*),$$

where $V_\ell(E)^*$ is the dual of $V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$. From

$$W(E/k_u, \tau) = W(\sigma_{E/k_u} \otimes \tau),$$

Rohrlich proves the following formulae.

Theorem 2.1 (Theorem 2 of [13]). *Suppose $\tau = \bar{\tau}$ is a 2-dimensional representation of $\mathrm{Gal}(\overline{k}_u/k_u)$ and denote ℓ for the residue characteristic of k_u.*

(i) *If $\ell = \infty$ then $W(E/k_u, \tau) = (-1)^{dim\ \tau} = 1$.*
(ii) *If $\ell < \infty$ and E has good reduction over k_u then $W(E/k_u, \tau) = \mathfrak{c}(\tau)$.*
(iii) *If $\ell < \infty$ and $\omega_u(j) < 0$ then*

$$W(E/k_u, \tau) = \mathfrak{c}(\tau)(-1)^{\langle \chi, \tau \rangle}$$

where χ is the character associated to the extension $k_u(\sqrt{-c_6})$.

(iv) *If $5 \leqslant \ell < \infty$, $\omega_u(j) \geqslant 0$, and $e = \frac{12}{gcd(\omega_u(\Delta_E),12)}$*

$$W(E/k_u, \tau) = \begin{cases} \mathfrak{c}(\tau) & \text{if } q \equiv 1 \mod e \\ \mathfrak{c}(\tau)(-1)^{\langle 1,\tau\rangle + \langle \eta,\tau\rangle + \langle \hat{\sigma}_e,\tau\rangle} & \text{if } e > 2,\ q \equiv -1 \mod e. \end{cases}$$

Proposition 2.2 (Proposition 7 of [13]). *If $\sigma_{E/k_u} = \psi \oplus \psi^{-1}$ for some character ψ of $k_u^\times$ and τ is as in Theorem 2.1, then $W(E/k_u, \tau) = \mathfrak{c}(\tau)$.*

2.2. Arithmetic local constants

Let $\mathrm{Sel}_{p^\infty}(E/K)$ be the p^∞-Selmer group of E (see [9, §2] or [4, §2]). Define the pro-p Selmer group of E over K as the Pontrjagin dual of $\mathrm{Sel}_{p^\infty}(E/K)$

$$\mathcal{S}_p(E/K) := \mathrm{Hom}(\mathrm{Sel}_{p^\infty}(E/K), \mathbb{Q}_p/\mathbb{Z}_p),$$

and consider it as a $\bar{\mathbb{Q}}_p$-module by tensoring with $\bar{\mathbb{Q}}_p$.

When $L_w \neq K_v$, let L'_w be the unique subfield of L_w containing K_v with $[L_w : L'_w] = p$, and otherwise let $L'_w := L_w = K_v$.

Definition 2.3 (Corollary 5.3 of [9])**.** For each prime v of K, define the arithmetic local constant $\delta_v = \delta(v, E, \rho) \in \mathbb{Z}/2\mathbb{Z}$ to be

$$\delta_v := \dim_{\mathbb{F}_p} E(K_v)/(E(K_v) \cap \mathrm{N}_{L_w/L'_w} E(L_w)) \mod 2.$$

Theorem 2.4 (Theorem 6.4 of [9]). *If S is a set of primes of K containing all primes above p, all primes ramified in L/K, and all primes where E has bad reduction, then*

$$\dim_{\overline{\mathbb{Q}}_p} \mathcal{S}_p(E/L)^\rho - \dim_{\overline{\mathbb{Q}}_p} \mathcal{S}_p(E/L)^1 \equiv \sum_{v \in S} \delta_v \mod 2.$$

Proof. Following the notation of [9, §3], let R be the maximal order in in the cyclotomic field of p^n-roots of unity, so R has a unique prime $\mathfrak{p}$ above p. Define $\mathcal{I} := \mathfrak{p}^{p^{n-1}}$ and define the $\mathcal{I}$-twist of E by $A := \mathcal{I} \otimes E$ (in the sense of [10] and [9]), an abelian variety with $R \subset \mathrm{End}_K(A)$. We then have

$$\dim_{\overline{\mathbb{Q}}_p} \mathcal{S}_p(E/L)^\rho = \mathrm{corank}_{R\otimes\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(A/K),$$
$$\dim_{\overline{\mathbb{Q}}_p} \mathcal{S}_p(E/L)^1 = \mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(E/K).$$

Thus the conclusion above is equivalent to Theorem 6.4 of [9]

$$\mathrm{corank}_{R\otimes\mathbb{Z}_p} \mathrm{Sel}_{p^\infty}(A/K) - \mathrm{corank}_{Z_p} \mathrm{Sel}_{p^\infty}(E/K) \equiv \sum_{v\in S} \delta_v \mod 2. \quad \blacksquare$$

3. Local computations

We keep the setting and notation of Theorem 2.1 and §1. Recall that c is the non-trivial element of $\mathrm{Gal}(K/k)$.

3.1. Preliminary calculations

Proposition 3.1. *If $v^c \neq v$, then $\gamma_u \equiv \delta_v + \delta_{v^c} \equiv 0$.*

Proof. When $v \neq v^c$, we have $\mathrm{Gal}(L_w/k_u) = \mathrm{Gal}(L_w/K_v)$. It follows that $\tau_{\rho,u} = \rho \oplus \rho^{-1}$ and $\tau_{1,u} = 1 \oplus 1$, so $\det \tau(-1) = 1$ for $\tau = \tau_{\rho,u}$ or $\tau = \tau_{1,u}$. Also $\langle \psi, \tau \rangle \equiv 0 \mod 2$ for $\psi = 1$, η, χ, or $\hat{\sigma}_e$, and by Theorem 2.1, we have $W(E/k_u, \tau) = 1$. Applying Lemma 5.1 of [9] for δ_v finishes the claim. $\blacksquare$

Proposition 3.2. *If $v^c = v$, v is unramified in L/K then $\gamma_u \equiv \sum_{v|u} \delta_v \equiv 0$.*

Proof. In this case, v splits completely in L/K by [9, 6.5(i)], i.e. for every prime w of L lying above v, $L_w = K_v$. Now, we have

$$\tau_{\rho,u}, \tau_{1,u} : \mathrm{Gal}(L_w/k_u) = \mathrm{Gal}(K_v/k_u) \to \mathrm{GL}_2(\mathbb{C})$$

viewing $\mathrm{Gal}(K_v/k_u)$ as the v-decomposition subgroup of $\mathrm{Gal}(L/k)$. One sees by direct calculation (see for example [14, §5.3]) that $\tau_{\rho,u} \cong \tau_{1,u}$, and by applying Corollary 5.3 of [9] for δ_v the claim follows. $\blacksquare$

3.2. Good reduction

In the case of good reduction, the arithmetic local constant has been determined by Mazur and Rubin in [9].

Theorem 3.3 (Theorem 5.6 and 6.6 of [9]). *If v is a prime of K with $v \nmid p$, $v = v^c$, v is ramified in L/K, and E has good reduction at v, then $\delta_v \equiv 0$.*

Theorem 3.4 (Theorem 6.7 of [9]). *If $v \mid p$ and E has good ordinary reduction at v, then $\delta_v \equiv 0$.*

For the corresponding situation on the analytic side:

Proposition 3.5. *If E has good reduction over K_v then $\gamma_u \equiv 0$.*

Proof. By Theorem 2.1(ii), it suffices to see $\det \tau_{\rho,u} \equiv \det \tau_{1,u} \mod \mathfrak{p}$ for some $\mathfrak{p} \mid p$. Fixing a basis for the spaces of ρ and 1 respectively, we have $\rho \equiv 1 \mod \mathfrak{p}$ since L/K is a cyclic p-power extension. This implies $\tau_{\rho,u} \equiv \tau_{1,u} \mod \mathfrak{p}$ (component-wise), viewed as matrices with function-valued entries, and $\det \tau_{\rho,u} \equiv \det \tau_{1,u} \mod \mathfrak{p}$. ∎

3.3. Potential multiplicative reduction

Here, in view of Propositions 3.1-3.2, we assume $v^c = v$ and v ramifies in L/K, i.e. $L_w \neq K_v$.

Analytic

Proposition 3.6. *If E/k_u has potential multiplicative reduction, then $\gamma_u \equiv 0$ if and only if E does not have split multiplicative reduction over K_v.*

Proof. Applying the arguments of Proposition 3.5, it remains to determine $\langle \chi, \tau \rangle$. If E has split multiplicative reduction at u, $\chi = 1$ and since $L_w \neq K_v$, $\dim \tau = 2$. We have $\tau = \tau_{1,u} = 1 \oplus \mu$, with μ the character associated to the extension K_v/k_u. When E has split multiplicative reduction at u, $\chi = 1 \ncong \mu$ and so $\langle \chi, \tau \rangle = 1$. For the other cases, $\chi \cong \mu$ if and only if K_v/k_u is the quadratic extension over which E acquires split multiplicative reduction. ∎

Arithmetic

Proposition 3.7. *If E has potential multiplicative reduction over k_u, then $\delta_v \equiv 0$ if and only if E does not have split multiplicative reduction over K_v.*

Proof. Let H be the quadratic extension over which E attains split multiplicative reduction. If $H = K_v$, there is a $q \in k_u^\times$ such that $E(L_w) \cong L_w^\times / q^{\mathbb{Z}}$ as $\mathrm{Gal}(L_w/K_v)$-modules, and with the isomorphism defined over K_v (loc. cit. [17]). This case is Lemma 8.4 of [9].

Suppose now that $H \neq K_v$. Define E' to be the quadratic twist of E associated to H/k_u, so that E' has split multiplicative reduction at u, and $E \overset{\phi}{\to} E'$ is an isomorphism over H. As before, we have a $\mathrm{Gal}(HL_w/k_u)$-isomorphism

$$\lambda : E'(HL_w) \to HL_w^\times / q^{\mathbb{Z}},$$

with $q \in k^\times$. Let $\mathrm{Gal}(HL_w/L_w) = \langle \sigma \rangle$ and define the minus-part of $HL_w^\times$ to be

$$(HL_w^\times)^- := \{ z \in HL_w^\times \ : \ z^\sigma = z^{-1} \}$$

and similarly for all other $\mathrm{Gal}(HL_w/L_w)$-modules[3]. The map obtained by precomposing λ with ϕ restricts to

$$E(L_w) \xrightarrow{\phi} E'(HL_w)^- \xrightarrow{\lambda} ((HL_w^\times)/q^{\mathbb{Z}})^-.$$

If $q \notin \mathrm{N}_{HL_w/L_w}$ then we also have $((HL_w^\times)/q^{\mathbb{Z}})^- \cong (HL_w^\times)^-$. If $q \in \mathrm{N}_{HL_w/L_w}$ then the projection of $(HL_w^\times)^-$ has index 2 in $((HL_w^\times)/q^{\mathbb{Z}})^-$, hence prime to p. Both cases will be similar, so we proceed with the former. One has a similar situation with $E(L'_w) \to (HL'^\times_w)^-$.

Since these maps commute with $N := \mathrm{N}_{HL_w/HL'_w}$, the snake lemma gives

$$[E(L'_w) : N(E(L_w))] = [(HL'^\times_w)^- : N((HL_w^\times)^-)].$$

We claim that this index is 1, implying $E(K_v) \subseteq E(L'_w) = N(E(L_w))$ and hence

$$\dim_{\mathbb{F}_p} E(K_v)/(E(K_v) \cap \mathrm{N}_{L_w/L'_w} E(L_w)) = 0.$$

To see that the index is 1, we note that local class field theory gives an injection

$$((HL'_w)^\times)^-/N((HL_w^\times)^-) \hookrightarrow \mathrm{Gal}(HL_w/HL'_w) = \mathrm{Gal}(L_w/L'_w)^-.$$

Since we know that σ conjugates $\mathrm{Gal}(L_w/L'_w)$ trivially, $\mathrm{Gal}(L_w/L'_w)^-$ is trivial. ■

3.4. Potential good reduction

Again, we assume $v^c = v$ and v ramifies in L/K, so $L_w \neq K_v$ as before.

Analytic

Denote ℓ for the common residue characteristic of k_u, K_v, L_w, and suppose E/k_u has additive and potential good reduction. Throughout we set H to be the unique unramified quadratic extension of k_u.

Proposition 3.8. *Suppose $v \nmid 6$. If $v \nmid p$ or K_v/k_u is unramified then $\gamma_u \equiv 0$.*

Proof. Here, we use the notation of Theorem 2.1, and from $v \nmid 6$, we have $\ell \geqslant 5$. For $\tau = \tau_{\rho,u}$ or $\tau = \tau_{1,u}$, we have $\langle 1, \tau\rangle + \langle \eta, \tau\rangle \equiv 0 \mod 2$, using that K_v/k_u is unramified for the latter.

In this setting $\hat{\sigma}_e$ is the representation of $\mathrm{Gal}(\bar{k}_u/k_u)$ induced from a character $\hat{\phi}_e$ of order $e = 3$, 4, or 6 (see [13, p. 332]). Hence, we may view $\hat{\sigma}_e$ as a representation of $\mathrm{Gal}(K_1/k_u)$ for some extension K_1/K_v.

Consider $\tau = \tau_{\rho,u}$. Lifting $\hat{\sigma}_e$ and τ to some appropriate extension K_2/k_u, since τ is irreducible, we see $\langle \hat{\sigma}_e, \tau\rangle = 1$ if and only if $\hat{\sigma}_e \cong \tau$. Restricting τ and $\hat{\sigma}_e$ to $\mathrm{Gal}(K_2/K_v)$, these representations decompose as $\tau = \rho \oplus \rho^c$ and $\hat{\sigma}_e = \phi_e \oplus \phi_e^c$. The order of ρ is a power of $p \geqslant 5$ and the order of ϕ_e is 3, 4, or 6, so $\langle \hat{\sigma}_e, \tau\rangle = 0$. For $\tau = \tau_{1,u}$, we have $\tau = 1 \oplus \eta$ and so $\langle \hat{\sigma}_e, \tau\rangle = 0$. ■

[3]For example, restriction of σ gives $\mathrm{Gal}(HL_w/L_w) \cong \mathrm{Gal}(HL'_w/L'_w)$, providing HL'_w a $\mathrm{Gal}(HL_w/L_w)$-module structure.

Proposition 3.9. *Suppose $v \nmid 6$ and K_v/k_u is ramified. If E acquires good reduction over an abelian extension of k_u, then $\gamma_u \equiv 0$.*

Proof. Here $\ell \geqslant 5$, so we are in case (iii) of Theorem 2.1, and the condition that E acquires good reduction over an abelian extension of k_u is equivalent to (see [11, Prop 2]) $\mathcal{W}(M/k_u)$ being abelian, where M is the minimal extension of k_u^{ur} over which E acquires good reduction, and in turn to $\sigma_{E/k_u} = \psi \oplus \psi^{-1}$ for some character ψ of $k_u^\times$. This gives

$$W(E/k_u, \tau) = \mathfrak{c}(\tau) = \det \tau(-1).$$

Applying Proposition 3.5 then gives the result. ∎

Proposition 3.10. *If $v \mid 6$ then $\gamma_u \equiv 0$.*

Proof. This is case 2(b) of [1]. De la Rochefoucauld proves this in terms of ϵ-factors as Rohrlich's formula (Theorem 2.1 above) do not apply when E is wildly ramified (see [6, §4]). We note that the dihedral setting is essential in his proof. ∎

Arithmetic

Proposition 3.11. *If $v \nmid p$ and E has additive reduction over K_v then $\delta_v \equiv 0$.*

Proof. If E has additive reduction, then

$$E_0(K_v)/E_1(K_v) \cong \tilde{E}_{ns}(\kappa) \cong \kappa^+, \tag{3.1}$$

with κ, the residue field of K_v, a finite field of characteristic $\ell \neq p$. We recall two facts (see §VII.3 and §VII.6 of [17]),

(1) $E_1(K_v) \cong \mathbb{Z}_\ell^r \oplus T$ for some finite ℓ-group T.
(2) $|E(K_v)/E_0(K_v)| \leqslant 4$.

Since $p \nmid 6\ell$ these two facts yield

$$E(K_v)/pE(K_v) \cong E_0(K_v)/pE_0(K_v) \cong E_1(K_v)/pE_1(K_v) = 0,$$

showing that $E(K_v)$ has no p-subgroups and so $\delta_v \equiv 0$. ∎

For $\mathcal{K}$ a finite extension of k_u, denote $\tilde{E}$ for the reduction of E at the prime of $\mathcal{K}$. If κ is the residue field of $\mathcal{K}$ and E has good ordinary reduction over $\mathcal{K}$ then we say that E has *anomalous* reduction over $\mathcal{K}$ if $\tilde{E}(\kappa)[p] \neq 0$, and we say E has *non-anomalous* reduction otherwise (see [9, App. B], also [8, §1.b]).

Proposition 3.12. *If $v \mid p$, E has additive reduction over K_v, and E attains good, ordinary, non-anomalous reduction over a Galois extension M/K_v, then $\delta_v \equiv 0$.*

Proof. Since E has potential good reduction, M can be chosen so that $[M : K_v]$ is prime to p (see [15, §2] and [16, p.2]). Let E^k denote a model for E defined over k_u, and let E^M denote a model of E defined over M for which E has good, ordinary, non-anomalous reduction. We have an isomorphism $E^k \to E^M$ defined over M, giving $E^k(\mathcal{M}) \cong E^M(\mathcal{M})$, where $\mathcal{M} = ML_w$, and similarly for $\mathcal{M}' = ML'_w$. We denote $\Gamma = \mathrm{Gal}(M/K_v)$ and $H = \mathrm{Gal}(L_w/L'_w)$, and note that

$$\mathrm{Gal}(M/K_v) \cong \mathrm{Gal}(\mathcal{M}'/L'_w) \cong \mathrm{Gal}(\mathcal{M}/L_w), \qquad \mathrm{Gal}(L_w/L'_w) \cong \mathrm{Gal}(\mathcal{M}/\mathcal{M}').$$

By Propositions B.2 and B.3 of [9], we have that $N_H : E^M(\mathcal{M}) \to E^M(\mathcal{M}')$ is surjective, and hence $N_H : E^k(\mathcal{M}) \to E^k(\mathcal{M}')$ is surjective also. From this and $N_\Gamma \circ N_H = N_H \circ N_\Gamma$ we have

$$\begin{aligned}[E^k(L'_w) : N_\Gamma(E^k(\mathcal{M}'))] &= [E^k(L'_w) : N_\Gamma \circ N_H(E^k(\mathcal{M}))] \\ &= [E^k(L'_w) : N_H \circ N_\Gamma(E^k(\mathcal{M}))].\end{aligned} \tag{3.2}$$

Since Γ has order prime to p and

$$|\Gamma| \cdot E^k(L'_w) \subset N_\Gamma(E^k(\mathcal{M}')) \subset E^k(L'_w),$$

the first term in (3.2) is prime to p. Since H has order p and

$$N_H \circ N_\Gamma(E^k(\mathcal{M})) \subset N_H(E^k(L_w)) \subset E^k(L'_w),$$

the last term in (3.2) is divisible by some power of p when $N_H(E^k(L_w)) \neq E^k(L'_w)$. Since this is impossible, we must have $N_H(E^k(L_w)) \supset E^k(K_v)$ and $\delta_v \equiv 0$. ■

4. Main result

Recall E/k is an elliptic curve ordinary at p. Also recall that γ_u is defined by

$$(-1)^{\gamma_u} = W(E/k_u, \tau_{\rho,u})/W(E/k_u, \tau_{1,u}).$$

Define $\mathfrak{S} = \{$primes v of $K : v^c = v$, v ramifies in L/K, and $v \mid 6p\}$.

Theorem 4.1. *Fix primes u of k and v of K with $v \mid u$. If $v \in \mathfrak{S}$ suppose that one of the following holds:*

(a) *E has good reduction at v.*
(b) *E has potential multiplicative reduction at v,*
(c) *E has additive, potential good reduction at v, and acquires good, non-anomalous reduction over an abelian extension of k_u when $v \mid p$.*

Then $\gamma_u \equiv \sum_{v|u} \delta_v \mod 2$.

Corollary 4.2. *If E/k satisfies the hypothesis of Theorem 4.1, then* mod 2

$$\dim_{\overline{\mathbb{Q}}_p} \mathcal{S}_p(E/L)^\rho - \dim_{\overline{\mathbb{Q}}_p} \mathcal{S}_p(E/L)^1 \equiv \mathrm{ord}_{s=1} \Lambda(E/k, \rho, s) - \mathrm{ord}_{s=1} \Lambda(E/k, 1, s).$$

Proof of 4.1. Let v, v^c the primes of K above u. If $v \notin \mathfrak{S}$ then $v^c \neq v$, v is unramified in L/K, or $v \nmid 6p$. If $v^c \neq v$ then we use Proposition 3.1, and if $v^c = v$ is unramified in L/K, Proposition 3.2 gives the claim. For the remainder we may assume $v^c = v$.

In the case $v \nmid 6p$, we have $v \nmid 6$ and $v \nmid p$. If E has good reduction at v then Theorem 3.3 shows $\delta_v \equiv 0$, and Proposition 3.5 gives $\gamma_u \equiv 0$. If E has potential multiplicative reduction then Proposition 3.7 and Proposition 3.6, for δ_v and γ_u, respectively, give the result. Lastly, if E has potential good reduction, then we apply Proposition 3.11 and Proposition 3.8.

For $v \in \mathfrak{S}$, case (a) follows from Theorem 3.4 for δ_v and Proposition 3.5 for γ_u. Case (b) is covered by Proposition 3.7 for δ_v and Proposition 3.6 for γ_u.

For case (c), first consider $v \mid 6$. We apply Proposition 3.10 for γ_u, and since $v \nmid p$, we can apply Proposition 3.11 for δ_v. When $v \mid p$ the condition that E acquries ordinary, non-anomalous reduction allows us to apply Proposition 3.12 for δ_v. In this case, $v \nmid 6$ and so for γ_u we use Proposition 3.8 when K_v/k_u is unramified or the 'abelian' condition and Proposition 3.9 when K_v/k_u is ramified. ■

References

[1] T. De la Rochefoucauld, *Invariance of the parity conjecture for p-Selmer groups of elliptic curves in a D_{2p^n}-extension*, arXiv:1002.0554v1 [math.NT], preprint.

[2] T. Dokchitser and V. Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math. **178**(1) (2009), 23–71.

[3] T. Dokchitser and V. Dokchitser, *On the Birch-Swinnerton-Dyer quotients modulo squares*, Annals of Mathematics **172**(1) (2010), 567–596.

[4] R. Greenberg, *Introduction to Iwasawa theory*, in B. Conrad and K. Rubin, editors, Arithmetic Algebraic Geometry, volume 9 of Park City Mathematics Series, American Mathematical Society, 2001.

[5] R. Greenberg, *Iwasawa theory, projective modules, and modular representations*, http://www.math.washington.edu/ greenber/personal.html, preprint.

[6] S. Kobayashi, *The local root number of elliptic curves with wild ramification*, Mathematische Annalen **323** (2002), 609–623.

[7] B. Mazur, *An Arithmetic Theory of Local Constants*, http://www.cirm.univ-mrs.fr/videos/2006/exposes/17w2/Mazur.pdf.

[8] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Inventiones Math. **18** (1972), 183–266.

[9] B. Mazur and K. Rubin, *Finding large Selmer rank via an arithmetic theory of local constants*, Annals of Mathematics **166**(2) (2007), 581–614.

[10] B. Mazur, K. Rubin, and A. Silverberg, *Twisting commutative algebraic groups*, Journal of Algebra **314**(1) (2007), 419–438.

[11] D. Rohrlich, *Variation of the root number in families of elliptic curves*, Composito Mathematica **87** (1993), 119–151.

[12] D. Rohrlich, *Elliptic Curves and the Weil-Deligne Group*, in Elliptic Curves and Related Topics, volume 4 of CRM Proceedings and Lecture Notes, pages 125–157, Amer. Math. Soc. 1994.

[13] D. Rohrlich, *Galois theory, elliptic curves, and root numbers*, Composito Mathematica **100** (1996), 311–349.

[14] J-P. Serre, *Linear Representations of Finite Groups*, volume 67 of Graduate Texts in Mathematics, Springer, 1979.

[15] J-P. Serre and J. Tate, *Good Reduction of Abelian Varieties*, Annals of Mathematics **88**(3) (1968), 492–517.

[16] J. Silverman, *The Néron fiber of abelian varieties with potential good reduction*, Math. Ann. **264** (1983), 1–3.

[17] J. Silverman, *Arithmetic of Elliptic Curves*, volume 106 of Graduate Texts in Mathematics, Springer, 1986.

Address: Sunil Chetty: Mathematics Department, College of St. Benedict and St. John's University.

E-mail: schetty@csbsju.edu

Received: 10 October 2010; **revised:** 4 January 2016