

# 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.

## 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<sup>1</sup> and a quadratic extension  $K$  of  $k$ . Next, fix a character  $\rho$  of  $\text{Gal}(\bar{k}/K)$  of order  $p^n$  and let  $\tau_\rho = \text{ind}_{K/k} \rho$  and  $\tau_1 = \text{ind}_{K/k} 1$  be the induced representations<sup>2</sup> from  $\text{Gal}(\bar{k}/K)$  to  $\text{Gal}(\bar{k}/k)$ . With  $\rho$  we define  $L = \bar{k}^{\ker(\rho)}$ , a cyclic extension  $L/K$  of degree  $p^n$ , and we assume  $\rho$  is such that  $L/k$  is Galois and that the non-trivial element  $c \in \text{Gal}(K/k)$  acts on  $g \in \text{Gal}(L/k)$  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  $\text{Gal}(L_w/k_u) \leq \text{Gal}(L/k)$ , and we set  $\tau_{\rho,u}$  (resp.  $\tau_{1,u}$ ) to be  $\tau_\rho$  (resp.  $\tau_1$ ) restricted to  $\text{Gal}(L_w/k_u)$ .

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

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

with  $W(E/k_u, \tau_u) \in \{\pm 1\}$  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  $\delta_v$ , for each prime  $v$  of  $K$ , which relate the  $\rho$ -part and 1-part of the pro- $p$ -Selmer module  $\mathcal{S}_p(E/L)$  (see §2.2)

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

---

2010 *Mathematics Subject Classification*. Primary 11G05; Secondary 11G07, 11G40.

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.

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

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

Defining  $\gamma_u$  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

$$(1.3) \quad \text{ord}_{s=1} \Lambda(E/k, \rho, s) - \text{ord}_{s=1} \Lambda(E/k, 1, s) \equiv \sum_u \gamma_u \pmod{2}.$$

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  $\delta_v$  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  $\omega_u$  for the standard valuation on  $k_u$  and  $c_6$  for the constant appearing in a simplified Weierstrass model for  $E/k_u$  (see [17, §III.1]). For  $\tau$  a representation of  $\text{Gal}(\bar{k}_u/k_u)$  with real-valued character, we call  $W(E/k_u, \tau) \in \{\pm 1\}$  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  $\tau$  has finite image, set  $\mathfrak{c}(\tau) := \det(\tau)(-1)$  and for two representations  $\tau$  and  $\tau'$  of  $\text{Gal}(\bar{k}_u/k_u)$  with finite image define  $\langle \tau, \tau' \rangle := \langle \text{tr}(\tau), \text{tr}(\tau') \rangle$ , with the right-hand side the usual inner product on characters.

Let  $H$  be the unramified quadratic extension of  $k_u$  and  $\eta$  the unramified quadratic character of  $\text{Gal}(\bar{k}_u/k_u)$ , i.e. the character of  $\text{Gal}(\bar{k}_u/k_u)$  with kernel  $\text{Gal}(\bar{k}_u/H)$ . For  $e = 3, 4$ , or  $6$  and  $q \equiv -1 \pmod{e}$ , where  $q = \#(k_u/u)$ , let  $\varphi_e$  be a tamely ramified character of  $\text{Gal}(\bar{k}_u/H)$  of exact order  $e$  and such that  $\sigma_e = \text{ind}_{H/k} \varphi_e$  is irreducible and symplectic. For  $\theta$  the unramified quadratic character of  $\text{Gal}(\bar{k}_u/H)$  set  $\hat{\sigma}_e := \text{ind}_{H/k_u} (\varphi_e \theta)$ , which is a dihedral representation of  $\text{Gal}(\bar{k}_u/k_u)$  (see p. 316-318 of [13]).

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

$$\sigma_{E/k_u, \ell} : \text{Gal}(\bar{k}_u/k_u) \rightarrow \text{GL}(V_\ell(E)^*),$$

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  $\text{Gal}(\bar{k}_u/k_u)$  and denote  $\ell$  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

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

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

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

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

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

**2.2. Arithmetic Local Constants.** Let  $\text{Sel}_{p^\infty}(E/K)$  be the  $p^\infty$ -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  $\text{Sel}_{p^\infty}(E/K)$

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

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

$$\delta_v := \dim_{\mathbb{F}_p} E(K_v)/(E(K_v) \cap N_{L_w/L'_w} E(L_w)) \pmod{2}.$$

**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*

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

*Proof.* Following the notation of [9, §3], let  $R$  be the maximal order in the cyclotomic field of  $p^n$ -roots of unity, so  $R$  has a unique prime  $\mathfrak{p}$  above  $p$ . Define  $\mathcal{I} := \mathfrak{p}^{n-1}$  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  $R \subset \text{End}_K(A)$ . We then have

$$\begin{aligned} \dim_{\bar{\mathbb{Q}}_p} \mathcal{S}_p(E/L)^\rho &= \text{corank}_{R \otimes \mathbb{Z}_p} \text{Sel}_{p^\infty}(A/K), \\ \dim_{\bar{\mathbb{Q}}_p} \mathcal{S}_p(E/L)^1 &= \text{corank}_{\mathbb{Z}_p} \text{Sel}_{p^\infty}(E/K). \end{aligned}$$

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

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

□

### 3. LOCAL COMPUTATIONS

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

### 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  $\text{Gal}(L_w/k_u) = \text{Gal}(L_w/K_v)$ . 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  $\langle \psi, \tau \rangle \equiv 0 \pmod{2}$  for  $\psi = 1, \eta, \chi$ , or  $\hat{\sigma}_e$ , and by Theorem 2.1, we have  $W(E/k_u, \tau) = 1$ . Applying Lemma 5.1 of [9] for  $\delta_v$  finishes the claim.  $\square$

**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

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

viewing  $\text{Gal}(K_v/k_u)$  as the  $v$ -decomposition subgroup of  $\text{Gal}(L/k)$ . 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  $\delta_v$  the claim follows.  $\square$

**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  $\det(\tau_{\rho,u}) \equiv \det(\tau_{1,u}) \pmod{\mathfrak{p}}$  for some  $\mathfrak{p} \mid p$ . Fixing a basis for the spaces of  $\rho$  and  $1$  respectively, we have  $\rho \equiv 1 \pmod{\mathfrak{p}}$  since  $L/K$  is a cyclic  $p$ -power extension. This implies  $\tau_{\rho,u} \equiv \tau_{1,u} \pmod{\mathfrak{p}}$  (component-wise), viewed as matrices with function-valued entries, and  $\det(\tau_{\rho,u}) \equiv \det(\tau_{1,u}) \pmod{\mathfrak{p}}$ .  $\square$

**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.  $L_w \neq K_v$ .

#### 3.3.1. 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  $\mu$  the character associated to the extension  $K_v/k_u$ . When  $E$  has split multiplicative reduction at  $u$ ,  $\chi = 1 \not\cong \mu$  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.  $\square$

3.3.2. *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  $\text{Gal}(L_w/K_v)$ -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  $E \xrightarrow{\varphi} E'$  is an isomorphism over  $H$ . As before, we have a  $\text{Gal}(HL_w/k_u)$ -isomorphism

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

with  $q \in k^\times$ . Let  $\text{Gal}(HL_w/L_w) = \langle \sigma \rangle$  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  $\text{Gal}(HL_w/L_w)$ -modules<sup>3</sup>. The map obtained by precomposing  $\lambda$  with  $\varphi$  restricts to

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

If  $q \notin N_{HL_w/L_w}$  then we also have  $((HL_w^\times)/q^{\mathbb{Z}})^- \cong (HL_w^\times)^-$ . If  $q \in N_{HL_w/L_w}$  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  $E(L'_w) \rightarrow (HL'_w)^\times$ .

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

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

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

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

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

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

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

**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.

3.4.1. *Analytic.* Denote  $\ell$  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  $\ell \geq 5$ . For  $\tau = \tau_{\rho,u}$  or  $\tau = \tau_{1,u}$ , we have  $\langle 1, \tau \rangle + \langle \eta, \tau \rangle \equiv 0 \pmod{2}$ , using that  $K_v/k_u$  is unramified for the latter.

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

<sup>3</sup>For example, restriction of  $\sigma$  gives  $\text{Gal}(HL_w/L_w) \cong \text{Gal}(HL'_w/L'_w)$ , providing  $HL'_w$  a  $\text{Gal}(HL_w/L_w)$ -module structure.

of  $\text{Gal}(K_1/k_u)$  for some extension  $K_1/K_v$ .

Consider  $\tau = \tau_{\rho,u}$ . Lifting  $\hat{\sigma}_e$  and  $\tau$  to some appropriate extension  $K_2/k_u$ , since  $\tau$  is irreducible, we see  $\langle \hat{\sigma}_e, \tau \rangle = 1$  if and only if  $\hat{\sigma}_e \cong \tau$ . Restricting  $\tau$  and  $\hat{\sigma}_e$  to  $\text{Gal}(K_2/K_v)$ , these representations decompose as  $\tau = \rho \oplus \rho^c$  and  $\hat{\sigma}_e = \varphi_e \oplus \varphi_e^c$ . The order of  $\rho$  is a power of  $p \geq 5$  and the order of  $\varphi_e$  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  $\langle \hat{\sigma}_e, \tau \rangle = 0$ .  $\square$

**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  $\ell \geq 5$ , 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  $\psi$  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.  $\square$

**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  $\epsilon$ -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.  $\square$

### 3.4.2. 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

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

with  $\kappa$ , 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  $\ell$ -group  $T$ .
- (2)  $|E(K_v)/E_0(K_v)| \leq 4$ .

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  $\delta_v \equiv 0$ .  $\square$

For  $\mathcal{K}$  a finite extension of  $k_u$ , denote  $\tilde{E}$  for the reduction of  $E$  at the prime of  $\mathcal{K}$ . If  $\kappa$  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  $E^k \rightarrow E^M$  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  $\Gamma = \text{Gal}(M/K_v)$  and  $H = \text{Gal}(L_w/L'_w)$ , and note that

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

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

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

Since  $\Gamma$  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  $\delta_v \equiv 0$ .  $\square$

#### 4. MAIN RESULT

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

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

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

**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  $\gamma_u \equiv \sum_{v \mid u} \delta_v \pmod{2}$ .

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

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

*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  $\delta_v$  and  $\gamma_u$ , 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  $\delta_v$  and Proposition 3.5 for  $\gamma_u$ . Case (b) is covered by Proposition 3.7 for  $\delta_v$  and Proposition 3.6 for  $\gamma_u$ .

For case (c), first consider  $v \mid 6$ . We apply Proposition 3.10 for  $\gamma_u$ , and since  $v \nmid p$ , we can apply Proposition 3.11 for  $\delta_v$ . When  $v \mid p$  the condition that  $E$  acquires ordinary, non-anomalous reduction allows us to apply Proposition 3.12 for  $\delta_v$ . In

this case,  $v \nmid 6$  and so for  $\gamma_u$  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.  $\square$

## 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\[math.NT\]](https://arxiv.org/abs/1002.0554v1), preprint.
- [2] T. Dokchitser and V. Dokchitser. Regulator Constants and the Parity Conjecture. *Invent. Math.*, 178(1):23–71, 2009.
- [3] T. Dokchitser and V. Dokchitser. On the Birch-Swinnerton-Dyer quotients modulo squares. *Annals of Mathematics*, 172(1):567–596, 2010.
- [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*, 323:609–623, 2002.
- [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.*, 18:183–266, 1972.
- [9] B. Mazur and K. Rubin. Finding large Selmer rank via an arithmetic theory of local constants. *Annals of Mathematics*, 166(2):581–614, 2007.
- [10] B. Mazur, K. Rubin, and A. Silverberg. Twisting Commutative Algebraic Groups. *Journal of Algebra*, 314(1):419–438, 2007.
- [11] D. Rohrlich. Variation of the root number in families of elliptic curves. *Composito Mathematica*, 87:119–151, 1993.
- [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*, 100:311–349, 1996.
- [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):492–517, 1968.
- [16] J. Silverman. The Néron Fiber of Abelian Varieties with Potential Good Reduction. *Math. Ann.*, 264:1–3, 1983.
- [17] J. Silverman. *Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 1986.

Mathematics Department  
 College of St. Benedict and St. John’s University  
 Email: [schetty@csbsju.edu](mailto:schetty@csbsju.edu)