

# 2-SELMER GROUPS OF QUADRATIC TWISTS OF ELLIPTIC CURVES

GEORGE BOXER AND PETER DIAO

ABSTRACT. In this paper we investigate families of quadratic twists of elliptic curves. Addressing a speculation of Ono, we identify a large class of elliptic curves for which the parities of the “algebraic parts” of the central values  $L(E^{(d)}/\mathbb{Q}, 1)$ , as  $d$  varies, have essentially the same multiplicative structure as the coefficients  $a_d$  of  $L(E/\mathbb{Q}, s)$ . We achieve this by controlling the 2-Selmer rank (à la Mazur and Rubin) when the Tamagawa numbers do not already dictate the parity.

## 1. INTRODUCTION

Let  $E/\mathbb{Q}$  be an elliptic curve and let  $L(E/\mathbb{Q}, s)$  be its  $L$ -function. The famous conjecture of Birch and Swinnerton-Dyer predicts that

$$L(E/\mathbb{Q}, 1) = \begin{cases} \frac{|\text{III}(E/\mathbb{Q})|\Omega_E \prod_p c_p}{|E_{\text{Tor}}|^2} & \text{if } \text{rank}(E/\mathbb{Q}) = 0 \\ 0 & \text{if } \text{rank}(E/\mathbb{Q}) > 0, \end{cases}$$

where  $|\text{III}(E/\mathbb{Q})|$  denotes the order of the Shafarevich-Tate group (which we will temporarily assume is finite,)  $c_p$  denotes the Tamagawa number at  $p$ ,  $\Omega_E$  denotes the period of  $E$ , and  $|E_{\text{Tor}}|$  is the size of the group of rational torsion points of  $E$ . For convenience we define:

$$L^{\text{alg}}(E/\mathbb{Q}, 1) := \frac{L(E/\mathbb{Q}, 1)}{\Omega_E}, \tag{1.1}$$

$$L^{\text{BSD}}(E/\mathbb{Q}, 1) := \begin{cases} \frac{|\text{III}(E/\mathbb{Q})|\prod_p c_p}{|E_{\text{Tor}}|^2} & \text{if } \text{rank}(E/\mathbb{Q}) = 0 \\ 0 & \text{if } \text{rank}(E/\mathbb{Q}) > 0. \end{cases} \tag{1.2}$$

The Birch and Swinnerton-Dyer conjecture predicts that  $L^{\text{alg}} = L^{\text{BSD}}$ . We consider elliptic curves over  $\mathbb{Q}$  without  $\mathbb{Q}$ -rational 2-torsion and investigate the parity of these quantities (even if they aren't integers) in families of quadratic twists. If  $E/\mathbb{Q}$  is an elliptic curve and  $d \neq 1$  is a squarefree integer, then recall that the quadratic twist of  $E^{(d)}/\mathbb{Q}$  of  $E$  by  $d$  is the unique elliptic curve over  $\mathbb{Q}$  that is not isomorphic to  $E$  but becomes isomorphic to  $E$  over  $\mathbb{Q}(\sqrt{d})$ . The question of how  $\text{rank}(E^{(d)}/\mathbb{Q})$  varies with  $d$  is an extremely important one and is the subject of many conjectures. Perhaps the most notable is Goldfeld's conjecture which predicts that  $E^{(d)}/\mathbb{Q}$  has rank 0 half the time and rank 1 half the time.

This problem has been studied by Ono and Skinner [OS, O], using Waldspurger's theory to study the nonvanishing of central values of  $L$ -functions by investigating the power of 2 dividing  $L^{\text{alg}}$ . More recently it has been studied in the work of Mazur and Rubin [MR] from the point of view of controlling 2-Selmer ranks, which can essentially

be interpreted as studying the parity of  $L^{\text{BSD}}$ . In principle, by combining these two works one can hope to prove the “Birch and Swinnerton-Dyer conjecture mod 2” for many elliptic curves in a family of quadratic twists.

Our work is motivated by the beautiful example of  $E = X_0(11)$ . Let

$$f(z) = \sum_{n=1}^{\infty} a_n q^n = \eta(z)^2 \eta(11z)^2 = q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2$$

be the weight 2 level 11 modular form associated to  $X_0(11)$ , where  $q = e^{2\pi iz}$ . By the theory of Shimura, Waldspurger, and Kohnen, there is a weight 3/2 modular form  $F = \sum_{n=1}^{\infty} B_n q^n$  associated to  $E$  whose Fourier coefficients encode the central  $L$ -values of negative quadratic twists of  $E$ . More precisely we have Kohnen’s formula

$$L(E^{(-d)}/\mathbb{Q}, 1) = \frac{\pi \langle f, f \rangle B_D^2}{2 \langle F, F \rangle \sqrt{D}}, \quad \text{for } (d, 11) = 1 \quad (1.3)$$

where  $D = -\text{disc}(\mathbb{Q}(\sqrt{-d}))$  and the  $\langle \cdot, \cdot \rangle$  are the relevant Petersson inner products for  $\Gamma_0(11)$  and  $\Gamma_0(44)$ . In this case,  $F$  has the following nice description [Sh]. We have that  $B_n = \widehat{B}_{4n}$ , where  $\widehat{B}_n$  is defined by

$$\widehat{F}(z) = \sum_{n=1}^{\infty} \widehat{B}_n q^n = \theta(11z) \eta(2z) \eta(22z) = \left( \sum_{n=-\infty}^{\infty} q^{11n^2} \right) \left( q \prod_{n=1}^{\infty} (1 - q^{2n}) (1 - q^{22n}) \right).$$

Since  $\widehat{F} \equiv f \pmod{2}$ , with a little work we see from Kohnen’s formula (1.3) that for  $d > 0$  squarefree with  $(d, 11) = 1$ , the parity of  $L^{\text{alg}}(E^{(-d)}/\mathbb{Q}, 1)$  has a very nice description:

$$L^{\text{alg}}(E^{(-d)}, 1) \equiv a_d \pmod{2}. \quad (1.4)$$

Using the arithmetic description of  $f$ , we have that for  $d$  odd and squarefree,  $a_d$  is odd if and only if for every prime  $p$  dividing  $d$ ,  $E$  has no rational 2-torsion modulo  $p$ .

This leads to two natural questions:

### Questions.

- (1) *Can one directly prove (1.4) for  $L^{\text{BSD}}(E^{(-d)}, 1)$ ?*
- (2) *Is this an example of a general phenomenon? In particular does the Birch and Swinnerton-Dyer conjecture predict (1.4) for a general class of elliptic curves?*

We answer these questions for certain curves which we now define. We call an elliptic curve  $E/\mathbb{Q}$  *good* if it satisfies all of the following:

- (1) The 2-Selmer rank of  $E$  is 0.
- (2) The discriminant  $\Delta$  of  $E$  is negative.
- (3) If  $p$  is any prime for which  $E$  has bad reduction, then  $E$  has multiplicative reduction at  $p$  and  $v_p(\Delta)$  is odd.
- (4)  $E$  has good reduction at 2 and the reduction of  $E \pmod{2}$  has  $j$ -invariant 0.

**Remark.** *Condition (4) is equivalent to  $E$  having a minimal model*

$$E : y^2 + y = x^3 + a_2 x^2 + a_4 x + a_6.$$

*Furthermore note that this implies that the reduction of  $E \pmod{2}$ ,  $\tilde{E}(\mathbb{F}_2)$ , has no 2-torsion.*

**Remark.** *There are many good elliptic curves. For example, an elliptic curve is good if it has 2-Selmer rank 0,  $v_2(j) > 0$ , and discriminant that is negative, squarefree, and prime to 2.*

In the course of this paper, the following condition arises sufficiently often that we give it a name. If  $E/\mathbb{Q}$  is an elliptic curve, we shall refer to a squarefree integer  $d$  as *2-trivial* for  $E$  if  $E$  has no rational 2-torsion mod  $p$  for every odd prime  $p|d$ . For good  $E$ , such as  $X_0(11)$ , we prove the following theorem for 2-trivial integers.

**Theorem 1.1.** *Let  $E/\mathbb{Q}$  be a good elliptic curve. If  $d$  is a squarefree 2-trivial integer with  $(d, \Delta) = 1$ , then*

$$\dim_{\mathbb{F}_2}(\text{Sel}_2(E^{(d)})) = \begin{cases} 0 & \text{if } d \text{ is odd} \\ 1 & \text{if } d \text{ is even.} \end{cases}$$

*In particular for such odd  $d$  we have that  $\text{rank}(E^{(d)}/\mathbb{Q}) = 0$ .*

**Remark.** *Mazur and Rubin [MR, Prop. 4.2] show that for an arbitrary elliptic curve  $E/\mathbb{Q}$  with 2-Selmer rank 0, if  $0 < d \equiv 1 \pmod{8\Delta}$  is a 2-trivial squarefree integer then  $E^{(d)}/\mathbb{Q}$  has 2-Selmer rank 0 as well. We show that with some assumptions on  $E/\mathbb{Q}$ , we can control the 2-Selmer of  $E^{(d)}/\mathbb{Q}$  for all  $d$  2-trivial squarefree integers prime to  $\Delta$ .*

**Remark.** *If we consider the set  $C_r(X)$  of square free integers  $|d| < X$  with  $r$  prime factors, as considered in [OS], then the Chebotarev density theorem implies that for an elliptic curve  $E$  with no rational 2-torsion,*

$$\#\{d \in C_r(X) \mid d \text{ is 2-trivial for } E\} \gg_r |C_r(X)|.$$

*Since the implied constants tend to 0 as  $r \rightarrow +\infty$ , this result falls short of proving that a positive proportion of quadratic twists have rank 0. On the other hand we still have*

$$\#\{0 < d < X \mid d \text{ is squarefree and 2-trivial for } E\} \gg \frac{X}{(\log X)^{1-\alpha}}$$

*for some  $\alpha > 0$ .*

It is important to relate Theorem 1.1 to the parity of  $L^{\text{BSD}}(E^{(d)}, 1)$  for all  $d$  square-free (positive or negative.)

**Theorem 1.2.** *Let  $E/\mathbb{Q}$  be a good elliptic curve, and let  $a_n$  be defined by*

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

*If  $d$  is a squarefree integer, then*

$$\begin{cases} L^{\text{BSD}}(E^{(d)}, 1) \equiv a_{|d|} \pmod{2} & \text{if } (d, \Delta) = 1 \\ L^{\text{BSD}}(E^{(d)}, 1) \equiv 0 \pmod{2} & \text{if } (d, \Delta) > 1. \end{cases}$$

**Remark.** *Strictly speaking, the statement of this theorem presumes the conjectural finiteness of  $|\text{III}(E/\mathbb{Q})|$ . However we can define the parity of  $|\text{III}(E/\mathbb{Q})|$  in order to avoid this issue. We say that  $|\text{III}(E/\mathbb{Q})|$  has odd order if and only if its 2-part is trivial. Thus when suitably interpreted, this theorem can be stated unconditionally.*

This paper is structured as follows. In Section 2 we recall the work of Mazur and Rubin, and derive conditions which imply the conclusion of Theorem 1.1. We carry out calculations in Section 3 to obtain Theorem 1.1. The deduction of Theorem 1.2 from Theorem 1.1 amounts to calculating Tamagawa numbers which is done in Section 4.

## 2. PRELIMINARIES

We now recall the recent work of Mazur and Rubin [MR] which allows us to prove the following key criterion.

**Theorem 2.1.** *Let  $E/\mathbb{Q}$  be a good elliptic curve. If  $d$  is a squarefree 2-trivial integer with  $(d, \Delta) = 1$ , then the following are true:*

- (1) *If  $d \equiv 1 \pmod{4}$  then  $\dim_{\mathbb{F}_2}(\text{Sel}_2(E^{(d)})) = 0$ .*
- (2) *Otherwise, we have*

$$\dim_{\mathbb{F}_2}(\text{Sel}_2(E^{(d)}/\mathbb{Q})) \leq \dim_{\mathbb{F}_2}(E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)), \quad (2.1)$$

and

$$\dim_{\mathbb{F}_2}(\text{Sel}_2(E^{(d)}/\mathbb{Q})) \equiv \dim_{\mathbb{F}_2}(E(\mathbb{Q}_2)/N_{\mathbb{Q}_2}^{\mathbb{Q}_2(\sqrt{d})}E(\mathbb{Q}_2(\sqrt{d}))) \pmod{2}. \quad (2.2)$$

**2.1. Mazur and Rubin revisited.** The problem of calculating Mordell-Weil groups reduces to calculating orders of 2-Selmer groups and 2-torsion in the Shafarevich-Tate group. Under the standard 2-descent this is easiest when  $E$  has full rational 2-torsion. The approach of Mazur and Rubin for studying the 2-Selmer rank of quadratic twists is more versatile as it works without assumption on the 2-torsion.

We restrict attention to  $\mathbb{Q}$  even though most of this discussion holds for a general number field. Let  $v$  be a place of  $\mathbb{Q}$ . There is a short exact sequence of  $\text{Gal}(\overline{\mathbb{Q}_v}/\mathbb{Q}_v)$ -modules

$$0 \rightarrow E(\overline{\mathbb{Q}_v})[2] \rightarrow E(\overline{\mathbb{Q}_v}) \xrightarrow{2} E(\overline{\mathbb{Q}_v}) \rightarrow 0.$$

Taking Galois cohomology one obtains the Kummer map  $\delta$

$$0 \rightarrow E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) \xrightarrow{\delta} H^1(\mathbb{Q}_v, E[2]).$$

Following [MR] we denote the image of the Kummer map by  $H_f^1(\mathbb{Q}_v, E[2])$ . For each  $v$  there is a localization map

$$\text{loc}_v : H^1(\mathbb{Q}, E[2]) \rightarrow H^1(\mathbb{Q}_v, E[2]),$$

and the 2-Selmer group  $\text{Sel}_2(E/\mathbb{Q})$  is defined to be the subgroup of  $H^1(\mathbb{Q}, E[2])$  of elements whose images under  $\text{loc}_v$  are in  $H_f^1(\mathbb{Q}_v, E[2])$  for all  $v$ .

Now let  $E^{(d)}$  be a quadratic twist of  $E$ . There is a natural isomorphism of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -modules  $E[2] \cong E^{(d)}[2]$ . This suggests a natural way of studying how the 2-Selmer group varies in quadratic twists: we can view both  $\text{Sel}_2(E/\mathbb{Q})$  and  $\text{Sel}_2(E^{(d)}/\mathbb{Q})$  as

living in the same space  $H^1(\mathbb{Q}, E[2])$ , but cut out by different local conditions. Thus the question of how the 2-Selmer group varies in families of quadratic twists can be reduced to studying how these local conditions change. This is the point of view taken in [MR].

In fact, if  $E$  and  $E^{(d)}$  are as above, then there is a finite set of places  $T$  of  $\mathbb{Q}$ , depending on  $d$  (see Proposition 2.4 below,) such that for all places  $v$  not in  $T$ ,

$$H_f^1(\mathbb{Q}_v, E[2]) = H_f^1(\mathbb{Q}_v, E^{(d)}[2]).$$

Now following [MR, Def 3.1] we define two additional subgroups of  $H^1(\mathbb{Q}, E[2])$  cut out by local conditions. We define the relaxed 2-Selmer group  $\mathcal{S}^T$  to be the subgroup of  $H^1(\mathbb{Q}, E[2])$  of elements whose images under  $\text{loc}_v$  are in  $H_f^1(\mathbb{Q}_v, E[2])$  for all places  $v$  outside of  $T$ . Additionally we define the strict 2-Selmer group  $\mathcal{S}_T$  to be the subgroup of  $\mathcal{S}^T$  of elements which additionally are killed by  $\text{loc}_v$  for all places  $v$  in  $T$ . More succinctly there are exact sequences

$$0 \rightarrow \mathcal{S}^T \rightarrow H^1(\mathbb{Q}, E[2]) \rightarrow \bigoplus_{v \notin T} H^1(\mathbb{Q}_v, E[2]) / H_f^1(\mathbb{Q}_v, E[2]). \quad (2.3)$$

$$0 \rightarrow \mathcal{S}_T \rightarrow \mathcal{S}^T \rightarrow \bigoplus_{v \in T} H^1(\mathbb{Q}_v, E[2]). \quad (2.4)$$

By definition we have

$$\mathcal{S}_T \subset \text{Sel}_2(\mathbb{E}/\mathbb{Q}) \subset \mathcal{S}^T, \quad \text{and} \quad \mathcal{S}_T \subset \text{Sel}_2(\mathbb{E}^{(d)}/\mathbb{Q}) \subset \mathcal{S}^T.$$

In light of this the following result bounds the 2-Selmer rank of  $E^{(d)}$ .

**Proposition 2.2** ([MR, Lemma 3.2]). *If  $T$ ,  $\mathcal{S}_T$ , and  $\mathcal{S}^T$  are as above, then*

$$\dim_{\mathbb{F}_2}(\mathcal{S}^T / \mathcal{S}_T) = \sum_{v \in T} \dim_{\mathbb{F}_2}(H_f^1(K_v, E[2])).$$

Then the following congruence of Kramer provides a ‘‘local formula’’ for comparing the parity of the 2-Selmer rank of a curve  $E$  and its quadratic twist  $E^{(d)}$ .

**Theorem 2.3** (Kramer [Kr]). *We have that*

$$\dim_{\mathbb{F}_2}(\text{Sel}_2(E^{(d)}/\mathbb{Q})) \equiv \dim_{\mathbb{F}_2}(\text{Sel}_2(E/\mathbb{Q})) + \sum_v \delta_v(E, d) \pmod{2},$$

where the sum is taken over all places of  $\mathbb{Q}$  and the local factor  $\delta_v(E, d)$  is defined by

$$\delta_v(E, d) = \dim_{\mathbb{F}_2}(E(\mathbb{Q}_v) / N_{\mathbb{Q}_v}^{\mathbb{Q}_v(\sqrt{d})} E(\mathbb{Q}_v(\sqrt{d}))).$$

In view of these results, we recall the following criteria for the equality of  $H_f^1(\mathbb{Q}_v, E[2])$  and  $H_f^1(\mathbb{Q}_v, E^{(d)}[2])$ , and the triviality of  $\delta_v(E, d)$ .

**Proposition 2.4** ([MR, Lemma 2.5]). *Let  $E^{(d)}$  be a quadratic twist of  $E/\mathbb{Q}$  and let  $F = \mathbb{Q}(\sqrt{d})$  be the corresponding quadratic extension. Let  $v$  be a place of  $\mathbb{Q}$  satisfying at least one of the following conditions:*

- (1)  $v$  is a finite place where  $E$  has good reduction and  $F/\mathbb{Q}$  is unramified.
- (2)  $v$  is a finite place where  $E$  has multiplicative reduction and  $\text{ord}_v(\Delta_E)$  is odd, and  $F/\mathbb{Q}$  is unramified at  $v$ .

- (3)  $v$  is the real place and  $\Delta_E < 0$ .
- (4)  $v$  is a finite place other than 2 and  $E(\mathbb{Q}_v)[2] = 0$ .

Then  $H_f^1(\mathbb{Q}_v, E[2]) = H_f^1(\mathbb{Q}_v, E^{(d)}[2])$  and  $\delta_v(E, d) = 0$ .

**2.2. Proof of Theorem 2.1.** We claim for all places  $v$  of  $\mathbb{Q}$ , other than the prime 2, that  $H_f^1(\mathbb{Q}_v, E[2]) = H_f^1(\mathbb{Q}_v, E^{(d)}[2])$  and  $\delta_v(E, d) = 0$ . We consider three cases. If  $v$  is the real place, then this follows from the fact that  $\Delta < 0$  and case 3 of Proposition 2.4. If  $v$  is a finite place of multiplicative reduction, then by assumption  $\text{ord}_v(\Delta)$  is odd and  $\mathbb{Q}(\sqrt{d})$  is unramified at  $v$  (since  $(d, \Delta) = 1$ ) and so this follows from case 2 of Proposition 2.4. Now assume that  $v \neq 2$  is a finite place of good reduction, corresponding to the prime  $p$ . If  $v$  is unramified in  $\mathbb{Q}(\sqrt{d})$  then this follows from case 1 of Proposition 2.4. Finally if  $v$  ramifies in  $\mathbb{Q}(\sqrt{d})$  then  $p$  divides  $d$  and so by assumption,  $E$  has no two torsion mod  $p$  and thus this follows from case 4 of Proposition 2.4.

To prove the first statement of the theorem, observe that if  $d \equiv 1 \pmod{4}$ , then 2 does not ramify in  $\mathbb{Q}(\sqrt{d})$ , and since  $E$  has good reduction at 2, Proposition 2.4 implies that  $H_f^1(\mathbb{Q}_2, E[2]) = H_f^1(\mathbb{Q}_2, E^{(d)}[2])$ . Thus the local conditions defining  $\text{Sel}_2(E/\mathbb{Q})$  and  $\text{Sel}_2(E^{(d)}/\mathbb{Q})$  agree, so  $\dim_{\mathbb{F}_2}(\text{Sel}_2(E^{(d)}/\mathbb{Q})) = 0$ .

Now we prove the second statement. Note that (2.2) follows immediately from Kramer's Theorem 2.3 and from the fact that  $\dim_{\mathbb{F}_2}(\text{Sel}_2(E/\mathbb{Q})) = 0$ . As for (2.1), the local conditions defining  $\text{Sel}_2(E/\mathbb{Q})$  and  $\text{Sel}_2(E^{(d)}/\mathbb{Q})$  agree at all places except for  $v = 2$ . Thus with the notation as above, we can take  $T = \{2\}$  and consider the corresponding strict and relaxed 2-Selmer groups. Since  $\mathcal{S}_T \subset \text{Sel}_2(E/\mathbb{Q}) = 0$ , Proposition 2.2 implies that

$$\dim_{\mathbb{F}_2}(\mathcal{S}^T/\mathcal{S}_T) = \dim_{\mathbb{F}_2}(\mathcal{S}^T) = \dim_{\mathbb{F}_2}(E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)).$$

Since  $\text{Sel}_2(E^{(d)}/\mathbb{Q}) \subset \mathcal{S}^T$ , the result follows.  $\square$

### 3. PROOF OF THEOREM 1.1

In view of Theorem 2.1, we see that the proof of Theorem 1.1 is reduced to the calculation of the dimension of  $E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)$  and the local factors  $\delta_2(E, d)$ . In this direction we first prove,

**Proposition 3.1.** *Let  $E/\mathbb{Q}_2$  be an elliptic curve with good reduction at 2 with  $E \pmod{2}$  having  $j$ -invariant 0. Then we have*

$$\dim_{\mathbb{F}_2}(E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)) = 1.$$

*Proof.* Let  $E$  have a minimal model

$$E : y^2 + y = x^3 + a_2x^2 + a_4x + a_6.$$

We recall a few standard facts about elliptic curves over local fields (see [S1, p. 174]). There is an exact sequence

$$0 \rightarrow E_1(\mathbb{Q}_2) \rightarrow E(\mathbb{Q}_2) \rightarrow \tilde{E}(\mathbb{F}_2) \rightarrow 0,$$

where  $\tilde{E}$  is the reduction of  $E \bmod 2$ . Since  $\tilde{E}(\mathbb{F}_2)$  is finite and has order prime to 2, there is an isomorphism

$$E(\mathbb{Q}_2)/2E(\mathbb{Q}_2) \cong E_1(\mathbb{Q}_2)/2E_1(\mathbb{Q}_2).$$

The group  $E_1(\mathbb{Q}_2)$  has a description in terms of the formal group of  $E$ . More precisely, there is a formal power series with coefficients in  $\mathbb{Z}_2$

$$F(z_1, z_2) = z_1 + z_2 - a_1 z_1 z_2 - a_2(z_1^2 z_2 + z_1 z_2^2) + \cdots$$

that endows the set  $2\mathbb{Z}_2$  with a group structure  $\mathcal{F}(2\mathbb{Z}_2)$ . Then there is an isomorphism of groups  $E_1(\mathbb{Q}_2) \cong \mathcal{F}(2\mathbb{Z}_2)$ . Furthermore by [S1, p. 126] the subgroup  $\mathcal{F}(4\mathbb{Z}_2)$  is isomorphic to  $4\mathbb{Z}_2$  under addition. In particular this implies that  $2\mathcal{F}(4\mathbb{Z}_2) = \mathcal{F}(8\mathbb{Z}_2)$ . Now given an arbitrary element  $c_1 2 + d$  of  $2\mathbb{Z}_2$ , with  $c_1 \in \{0, 1\}$  and  $d \in 4\mathbb{Z}_2$ , we have, by the formal group law

$$2 \cdot (c_1 2 + d) = 4c_1 + O(2^3).$$

Thus  $2\mathcal{F}(2\mathbb{Z}_2) = \mathcal{F}(4\mathbb{Z}_2)$  and the result follows.  $\square$

**Remark.** *The assumption that the reduction of  $E \bmod 2$  has  $j$ -invariant 0 is essential here. If  $E/\mathbb{Q}_2$  had good reduction and the reduction mod 2 had  $j$ -invariant 1 then we would have  $\dim_{\mathbb{F}_2}(E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)) > 1$ .*

**Remark.** *An alternative way to prove Proposition 3.1 is to use the standard fact that  $E(\mathbb{Q}_2) \cong \mathbb{Z}_2 \times E(\mathbb{Q}_2)_{\text{Tor}}$  and then observe that the assumptions of the proposition imply that  $E(\mathbb{Q}_2)$  has no 2-torsion by [Se, Prop. 12].*

Turning to the local  $\delta$  factors we have the following.

**Proposition 3.2.** *Let  $E/\mathbb{Q}_2$  be an elliptic curve with good reduction at 2 with  $E \bmod 2$  having  $j$ -invariant 0. If  $K/\mathbb{Q}_2$  is a ramified quadratic extension, then*

$$\dim_{\mathbb{F}_2}(E(\mathbb{Q}_2)/N_{\mathbb{Q}_2}^K E(K)) = \begin{cases} 0 & \text{if } K = \mathbb{Q}_2(\sqrt{d}) \text{ with } d = 3, 7 \\ 1 & \text{if } K = \mathbb{Q}_2(\sqrt{d}) \text{ with } d = 2, 6, 10, 14. \end{cases}$$

*Proof.* Let  $E$  have a minimal model

$$E : y^2 + y = x^3 + a_2 x^2 + a_4 x + a_6.$$

For brevity we denote  $N_{\mathbb{Q}_2}^K$  by  $N$ . We have a commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & E_1(K) & \longrightarrow & E(K) & \longrightarrow & \tilde{E}(\mathbb{F}_2) \longrightarrow 0 \\ & & \downarrow N & & \downarrow N & & \downarrow 2 \\ 0 & \longrightarrow & E_1(\mathbb{Q}_2) & \longrightarrow & E(\mathbb{Q}_2) & \longrightarrow & \tilde{E}(\mathbb{F}_2) \longrightarrow 0, \end{array}$$

from which we obtain an isomorphism  $E(\mathbb{Q}_2)/NE(K) \cong E_1(\mathbb{Q}_2)/NE_1(K)$ . Let  $\pi$  denote a uniformizer for  $K$  and let  $\mathcal{O}_K$  denote its ring of integers. Then again by [S1, p. 126] we have isomorphisms  $\mathcal{F}(\pi^3 \mathcal{O}_K) \cong \pi^3 \mathcal{O}_K$  and  $\mathcal{F}(4\mathbb{Z}_2) \cong 4\mathbb{Z}_2$ . Furthermore

these isomorphisms are given by the same convergent power series with coefficients in  $\mathbb{Q}_2$ . Thus there is a commutative diagram

$$\begin{array}{ccc} \mathcal{F}(\pi^3 \mathcal{O}_K) & \xrightarrow{N} & \mathcal{F}(4\mathbb{Z}_2) \\ \downarrow & & \downarrow \\ \pi^3 \mathcal{O}_K & \xrightarrow{\text{Tr}_{\mathbb{Q}_2}^K} & 4\mathbb{Z}_2. \end{array}$$

Since  $\text{Tr} \pi^3 \mathcal{O}_K = 8\mathbb{Z}_2$ , we have  $\mathcal{F}(8\mathbb{Z}_2) \subset N\mathcal{F}(\pi \mathcal{O}_K)$ . Now consider the element  $2 \in \mathcal{F}(\pi \mathcal{O}_K)$ . Using the formal group law we compute its norm

$$N(2) = F(2, 2) = 4 - O(2^3).$$

Thus  $N\mathcal{F}(\pi^2 \mathcal{O}_K) = \mathcal{F}(4\mathbb{Z}_2)$ .

To complete the proposition it remains to compute  $N(\pi)$ . Now we split into two cases. First suppose  $K = \mathbb{Q}_2(\sqrt{d})$  with  $d = 3, 7$ . Then we can take  $\pi = 1 + \sqrt{d}$ . By the formal group law we have

$$N(\pi) = F(\pi, \bar{\pi}) = \pi + \bar{\pi} + O(\pi^3) = 2 + O(2^2).$$

Thus in this case  $N\mathcal{F}(\pi \mathcal{O}_K) = \mathcal{F}(2\mathbb{Z}_2)$  as required. Now if we have  $K = \mathbb{Q}_2(\sqrt{d})$  with  $d = 2, 6, 10, 14$  we can take  $\pi = \sqrt{d}$  and we have

$$N(\pi) = F(\pi, \bar{\pi}) = \pi + \bar{\pi} + O(\pi^3) = 0 + O(2^2).$$

Thus in this case  $N\mathcal{F}(\pi \mathcal{O}_K) = \mathcal{F}(4\mathbb{Z}_2)$  which has index 2 in  $\mathcal{F}(2\mathbb{Z}_2)$ , completing the proof.  $\square$

*Proof of Theorem 1.1.* Let  $d$  prime to  $\Delta$  be a squarefree, 2-trivial integer for  $E$ . If  $d \equiv 1 \pmod{4}$  then the result is immediate from the first part of Theorem 2.1. Otherwise, the second part of Theorem 2.1 implies that  $\dim_{\mathbb{F}_2}(\text{Sel}_2(E^{(d)})) \leq \dim_{\mathbb{F}_2} E(\mathbb{Q}_2)/2E(\mathbb{Q}_2) = 1$  with the second equality following from Proposition 3.1. Thus  $\dim_{\mathbb{F}_2}(\text{Sel}_2(E^{(d)}))$  is determined by its parity, which is computed as a result of Theorem 2.1 and Proposition 3.2.  $\square$

#### 4. PROOF OF THEOREM 1.2

The proof of theorem 1.2 uses the following calculation of Tamagawa numbers for quadratic twists.

**Proposition 4.1.** *Let  $E/\mathbb{Q}$  be a good elliptic curve and, let  $d$  be a squarefree integer. The following are true:*

- (1) *If  $(d, \Delta) = 1$ , then the Tamagawa factor  $\prod_p c_p(E^{(d)})$  is odd if and only if  $d$  is 2-trivial for  $E$ .*
- (2) *If  $(d, \Delta) > 1$ , then the Tamagawa factor  $\prod_p c_p(E^{(d)})$  is even.*

*Proof.* First we prove (1). If  $p$  is a prime of bad reduction then by assumption  $p$  is odd and  $E$  has multiplicative reduction at  $p$  and  $v_p(\Delta_E)$  is odd. Then since  $(d, \Delta) = 1$ ,  $E^{(d)}$  retains multiplicative reduction at  $p$  and  $v_p(\Delta_E) = v_p(\Delta_{E^{(d)}})$  and so the Tamagawa factor  $c_p(\Delta_{E^{(d)}})$  is odd (it is either 1 or  $v_p(\Delta_E)$  depending on whether or not  $E^{(d)}$  has split or non-split multiplicative reduction at  $p$  [S2, p. 366].)

Next we consider the prime 2. We claim that  $c_2$  is always 1. By assumption,  $E$  has a minimal Weierstrass model of the form

$$E : y^2 + y = x^3 + a_2x^2 + a_4x + a_6.$$

First suppose  $d$  is even and make the change of variables

$$x = \frac{x'}{d}, \quad y = \frac{y'}{d^{3/2}} - \frac{1}{2}.$$

This yields a Weierstrass equation for  $E^{(d)}$

$$E^{(d)} : y^2 = x^3 + a'_2x^2 + a'_4x + a'_6$$

with coefficients

$$\begin{aligned} a'_2 &= da_2 \\ a'_4 &= d^2a_4 \\ a'_6 &= d^3 \left( a_6 + \frac{1}{4} \right) \end{aligned}$$

Since  $d$  is even, the  $a'_i$  are integers and we apply Tate's algorithm. Since  $a'_6 \equiv 2 \pmod{4}$  the algorithm terminates at step 3 of [S2, p. 366] and we see that  $E^{(d)}$  has Kodaira symbol II at 2 and  $c_2 = 1$ .

Now suppose  $d$  is odd. This time make the change of variables

$$x = \frac{x'}{4d}, \quad y = \frac{y'}{8d^{3/2}} + \frac{1}{2d^{3/2}} - \frac{1}{2}$$

to obtain a Weierstrass equation for  $E^{(d)}$  of the form

$$E^{(d)} : y^2 + 8y = x^3 + a'_2x^2 + a'_4x + a'_6$$

with coefficients

$$\begin{aligned} a'_2 &= 4da_2 \\ a'_4 &= 16d^2a_4 \\ a'_6 &= 64d^3a_6 + 16(d^3 - 1). \end{aligned}$$

If  $d \equiv 1 \pmod{4}$  then  $64|a'_6$  and we can make the change of variables  $x = 4x'$ ,  $y = 8y'$  to see that  $E^{(d)}$  has good reduction at 2 and thus  $c_2 = 1$ . On the other hand if  $d \equiv 3 \pmod{4}$  then 32 is the largest power of 2 dividing  $a'_6$  and following Tate's algorithm we end up in step 10 of [S2, p. 368] and thus  $E^{(d)}$  has Kodaira symbol II\* at 2 and  $c_2 = 1$ .

If  $p$  is an odd prime of good reduction and  $(p, d) = 1$  then  $E^{(d)}$  has good reduction at  $p$  and so  $c_p = 1$ . If  $p$  divides  $d$  then we can easily compute  $c_p$  using Tate's algorithm. Since  $p$  is odd,  $E$  has a model which is minimal at  $p$  of the form  $y^2 = f(x)$ . Then the quadratic twist of  $E$  by  $d$  is given by the equation  $E^{(d)} : y^2 = d^3f(x/d)$ . Following Tate's algorithm we end up in step 6 of [S2, p. 367] and it tells us that  $E^{(d)}$  has Kodaira symbol I\*\_0 at  $p$  and  $c_p$  is equal to 1 plus the number of roots of the polynomial  $(d')^3f(x/d')$  where  $d' = d/p$ . But this is just the number of 2-torsion of  $E^{(d')}$  mod  $p$  which is the same as the number of 2-torsion of  $E$  mod  $p$ . The claim follows.

Now we prove (2). Take any  $p | (\Delta, d)$ . Then  $E$  has multiplicative reduction at  $p$ . Let  $n = v_p(\Delta)$ . Then by [S2, p. 365],  $E^{(d)}$  has Kodaira symbol  $I_n^*$  at  $p$  and by [S2, p. 367],  $c_p = 2$  or  $4$ . Thus the Tamagawa product for  $E^{(d)}$  is even as claimed.  $\square$

*Proof of Theorem 1.2.* First we characterize the parity of  $a_{|d|}$  for  $d$  squarefree. Since  $E$  is assumed to have good reduction at  $2$ , and has no  $2$ -torsion modulo  $2$ ,  $a_2$  is even. Thus for  $d$  even,  $a_{|d|}$  is even by multiplicativity. On the other hand if  $d$  is odd then  $a_{|d|}$  is odd if and only if  $d$  is  $2$ -trivial for  $E$ .

Now we consider  $L^{\text{BSD}}(E^{(d)}, 1)$ . In the case that  $(d, \Delta) > 1$  then either  $\text{rank}(E^{(d)}) > 0$ , or  $\text{rank}(E^{(d)}) = 0$  and part (2) of Proposition 4.1 implies that the Tamagawa factor for  $E^{(d)}$  is even. Either way  $L^{\text{BSD}}(E^{(d)}, 1)$  is even.

Now assume  $(d, \Delta) = 1$ . We split into two cases. First suppose  $d$  is not  $2$ -trivial. Then either  $\text{rank}(E^{(d)}) > 0$  and  $L^{\text{BSD}}(E^{(d)}, 1) = 0$  or  $\text{rank}(E^{(d)}) = 0$  and  $L^{\text{BSD}}(E^{(d)}, 1)$  is still even as the Tamagawa product is even by Proposition 4.1.

Now suppose  $d$  is  $2$ -trivial. If  $d$  is odd then by Theorem 1.1  $E^{(d)}$  has  $2$ -Selmer rank  $0$ . Thus  $\text{rank}(E^{(d)}) = 0$  and  $|\text{III}(E^{(d)})|$  is odd. Furthermore the Tamagawa product is odd by Proposition 4.1 and so  $L^{\text{BSD}}(E^{(d)}, 1)$  is odd in this case. Finally if  $d$  is even then by Theorem 1.1  $E^{(d)}$  has  $2$ -Selmer rank  $1$ . Thus either the rank of  $E^{(d)}$  is  $1$ , or  $|\text{III}(E^{(d)})|$  is even, and either way  $L^{\text{BSD}}(E^{(d)}, 1)$  is even (of course conjecturally only the first situation can occur.)  $\square$

## REFERENCES

- [Kr] K. Kramer, *Arithmetic of elliptic curves upon quadratic extensions*, Trans. Amer. Math. Soc. **264** (1981) 121-135.
- [MR] B. Mazur and K. Rubin, *Ranks of Twists of Elliptic Curves and Hilbert's Tenth Problem*, Preprint available at <http://arxiv.org/0904.3709>.
- [O] K. Ono, *Nonvanishing of quadratic twists of modular  $L$ -functions with applications for elliptic curves*, J. reine Angew. Math., **533** (2001), 81-97.
- [OS] K. Ono, C. Skinner, *Non-vanishing of quadratic twists of modular  $L$ -functions*. Invent. Math. **134** (1998) 651-660.
- [Se] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*. Invent. Math. **15** (1972) 259-331.
- [Sh] T. Shintani, *On construction of holomorphic cusp forms of half integral weight.*, Nagoya Math. J. **58** (1975), 83-126.
- [S1] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, New York: Springer-Verlag (1986).
- [S2] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **151**, New York: Springer-Verlag (1994).

MAILBOX 2704, FRIST CENTER. PRINCETON, NJ 08544.  
*E-mail address:* [gboxer@princeton.edu](mailto:gboxer@princeton.edu)

MAILBOX 2868, FRIST CENTER. PRINCETON, NJ 08544.  
*E-mail address:* [pdiao@princeton.edu](mailto:pdiao@princeton.edu)