

The Tate-Shafarevich Group in Families of  
Elliptic Curves

Jy-Ying Janet Chen

Senior Honors Thesis  
Department of Mathematics  
Stanford University

## **Acknowledgments**

I would like to thank my advisor, Professor Karl Rubin, for all of the help and advice he has given me throughout this project.

# 1 Introduction

It has been conjectured that the Tate-Shafarevich group  $\text{III}$  of an elliptic curve  $E$  over  $\mathbb{Q}$  is always finite. Assuming the truth of this conjecture, it now makes sense to try to describe the order of  $\text{III}$ . In this paper, we will investigate the distribution of the order of  $\text{III}$  for families of quadratic twists. In particular, given an elliptic curve  $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$  with twists  $E_d : y^2 = x^3 + a_2dx^2 + a_4d^2x + a_6d^3$ , we are interested in seeing, for primes  $p$ , how often  $\#\text{III}(E_d/\mathbb{Q})$  is divisible by  $p$ .

Birch and Swinnerton-Dyer formulated a conjecture relating the order of the Tate-Shafarevich group to the behavior of the  $L$ -series of the elliptic curve at 1. In section 2 of this paper, we will use their conjecture and a theorem of Waldspurger to compute the conjectured order of the Tate-Shafarevich group for several million quadratic twists of three elliptic curves. In section 3, we will use the Birch and Swinnerton-Dyer Conjecture to further study the 2-part of the Tate-Shafarevich group in two families of quadratic twists. Finally, in section 4, we will use other methods to verify, in certain cases, that the 2-part of the Tate-Shafarevich group agrees with the conjectured order discussed in section 3.

Throughout the paper, we will focus our discussion on curves of analytic rank 0. In this case, it is known that  $\text{III}(E/\mathbb{Q})$  is finite ([11, Theorems 4.2.8 and 4.7.3]).

## 2 Distribution of the Conjectured Order of $\text{III}$

First, we will describe the results of computing the conjectured order of  $\text{III}$  for some families of quadratic twists. We will use two conjectures of Birch and Swinnerton-Dyer (see, for example, [11, Chapter 4]). In general, finding the actual order of  $\text{III}$  is difficult, so it is not feasible to compute the distribution of the actual order of  $\text{III}$ .

Recall that the analytic rank of an elliptic curve is the order of vanishing of its  $L$ -series  $L(E, s)$  at  $s = 1$ .

**Conjecture 2.1.** (*BSD I*) *If  $E$  is an elliptic curve over  $\mathbb{Q}$ , then the rank of  $E$  is the same as the analytic rank of  $E$ .*

In particular, BSD I implies that  $L(E, 1) \neq 0$  iff  $E$  has rank 0.

For an elliptic curve  $E$  with minimal equation  $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ , let

$$\Omega(E) = \int_{E(\mathbb{R})} \frac{dx}{|2y + a_1x + a_3|} \in \mathbb{R}.$$

Let  $c_p = \#(E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p))$  where  $E_0(\mathbb{Q}_p) = \{P \in E(\mathbb{Q}_p) : P \text{ reduces to a}$

non-singular point on the reduction of  $E \bmod p$ ).

Then, assuming BSD I, the second Birch and Swinnerton-Dyer conjecture gives the following for curves of rank 0:

**Conjecture 2.2.** (BSD II) *Suppose  $E$  is an elliptic curve over  $\mathbb{Q}$  of rank 0. Then,*

$$L(E, 1) = \frac{\Omega(E) \# \text{III}(E/\mathbb{Q}) \prod_{p|\Delta(E)} c_p}{\#(E(\mathbb{Q})_{\text{tors}})^2}.$$

The quantities  $\Omega(E)$ ,  $\Delta(E)$ ,  $c_p$ , and  $\#(E(\mathbb{Q})_{\text{tors}})$  can be computed efficiently by the computer program PARI (see [3] for descriptions of several algorithms used by PARI). So, the only additional quantity that we need to be able to compute efficiently is  $L(E, 1)$ . To do this, we will use a result of Waldspurger. First, we need to state some definitions; see [1] for more details.

Let

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

Let  $\chi_t$  be the Dirichlet character corresponding to  $\mathbb{Q}(\sqrt{t})/\mathbb{Q}$ . If  $N$  is a natural number divisible by 4 and  $\psi$  is a Dirichlet character mod  $N$ , let  $S_{3/2}(N, \psi)$  denote the complex vector space of cusp forms of weight  $3/2$  with respect to  $\Gamma_0(N)$  and with character  $\psi$  (see [10] for more precise definitions). Let  $S_0(N, \psi)$  be the subspace of  $S_{3/2}(N, \psi)$  generated by forms  $F$  of the following type: there is a  $t \in \mathbb{N}$  and a quadratic character  $\chi$  with conductor  $r$  such that

$$N = 4r^2t, \quad \psi = \chi \cdot \chi_{-t}, \quad \text{and} \quad F = \sum_{m=1}^{\infty} \chi(m) m q^{tm^2}.$$

We will define orthogonality on  $S_{3/2}(N, \psi)$  by the following Hermitian form:

$$\langle F, G \rangle = \frac{1}{C(N)} \int_{\mathbb{H}/\Gamma_0(N)} F(x+iy) G(x-iy) y^{-\frac{1}{2}} dx dy$$

where  $\mathbb{H}$  is the upper half plane of  $\mathbb{C}$ . Given

$$F = \sum_{n=1}^{\infty} a_n q^n \in S_{3/2}(N, \chi_t) \cap S_0(N, \chi_t)^\perp,$$

let

$$S(F) = \sum_{m=1}^{\infty} b_m q^m$$

where  $b_m$  satisfies

$$\sum_{m=1}^{\infty} b_m m^{-s} = \left( \sum_{i=1}^{\infty} \begin{pmatrix} -1 \\ i \end{pmatrix} \psi(i) i^{-s} \right) \left( \sum_{j=1}^{\infty} a_{j^2} j^{-s} \right).$$

In [1] we find the following theorem:

**Theorem 2.3.** (Waldspurger) *Suppose that  $E/\mathbb{Q}$  is a modular elliptic curve with corresponding cusp form  $f_E$ ; suppose also that  $F \in S_{3/2}(N, \chi_t) \cap S_0(N, \chi_t)^\perp$  with  $S(F) = f_E$  and*

$$F = \sum_{n=1}^{\infty} a_n q^n.$$

*If  $d$  and  $d_0$  are square free natural numbers with*

$$d \equiv d_0 \pmod{\prod_{p|N} \mathbb{Q}_p^{\times 2}}$$

*and  $dd_0$  is relatively prime to  $N$ , then*

$$L(E_{-td}, 1) \sqrt{da_{d_0}^2} = L(E_{-td_0}, 1) \sqrt{d_0 a_d^2}.$$

Note that it has recently been shown that every elliptic curve over  $\mathbb{Q}$  is modular ([11, Theorem 4.2.8]).

For some of our examples, we will also need to define  $\Theta(f)$ . If  $f$  is a quadratic form, let

$$\Theta(f) = \sum_{n=1}^{\infty} b_n q^n$$

where

$$b_n = \frac{1}{2} \#\{(z_1, z_2) \in \mathbb{Z}^2 : f(z_1, z_2) = n\}.$$

Now, we will study the distribution of the conjectured order of III for some families of quadratic twists  $E_d$ . We will always take  $d$  to be a square-free positive integer.

## 2.1 $y^2 = x^3 - d^2x$

First, consider the family  $E_d : y^2 = x^3 - d^2x$ . Using Waldspurger's Theorem, Tunnell proved in [13] that

$$L(E_d, 1) = \frac{k_d(n_d - 2m_d)^2 L(E_1, 1)}{4\sqrt{d}} \tag{2.1}$$

where

$$k_d = \begin{cases} 1, & d \text{ is odd} \\ 2, & d \text{ is even} \end{cases},$$

$n_d = \#\{(x, y, z) \in \mathbb{Z}^3 : x^2 + 2k_d y^2 + 8z^2 = d/k_d\}$ , and  $m_d = \#\{(x, y, z) \in \mathbb{Z}^3 : x^2 + 2k_d y^2 + 32z^2 = d/k_d\}$ . Also, we have the following fact:

**Proposition 2.4.**  $\Omega(E_d) = \Omega(E_1)/\sqrt{d}$ .

**Proof.** The discriminant of  $y^2 = x^3 - d^2x$  is  $2^6d^6$ . Recall that  $d$  is square-free. If  $d$  is odd, then  $y^2 = x^3 - d^2x$  is a minimal equation for  $E_d$  by [12, VII, Remark 1.1]. If  $d$  is even, then  $d = 2k$  for some odd  $k$ ; then,  $y^2 = x^3 - d^2x$  has discriminant  $2^{12}k^6$ . Assume that  $y^2 = x^3 - d^2x$  is not minimal. Then, there is a change of variables which produces a minimal equation. Since this change of variables fixes the point  $[0, 1, 0]$  on the curve and preserves the Weierstrass form of the equation, it must have the form  $x = u^2x' + r$ ,  $y = u^3y' + u^2sx' + t$  for  $u, r, s, t \in \overline{\mathbb{Q}}$ ; under this change of variables, the new curve will have discriminant  $u^{-12}(2^{12}k^6)$ . By [12, Proposition VII.1.3], we may take  $u, r, s, t \in \mathbb{Z}$  with  $u > 0$ . So,  $u$  must be 2, and the change of variables  $x = 4x' + r$ ,  $y = 8y' + 4sx' + t$  gives a minimal equation for some  $r, s, t \in \mathbb{Z}$ . Under this transformation, we get a curve  $y'^2 + a_1x'y' + a_3y' = x'^3 + a_2x'^2 + a_4x' + a_6$  where

$$\begin{aligned} 2a_1 &= 2s \\ 4a_2 &= 3r - s^2 \\ 8a_3 &= 2t \\ 16a_4 &= -4k^2 + 3r^2 - 2st \\ 64a_6 &= -4rk^2 + r^3 - t^2 \end{aligned}$$

Since  $y'^2 + a_1x'y' + a_3y' = x'^3 + a_2x'^2 + a_4x' + a_6$  is minimal,  $a_i \in \mathbb{Z}$  for each  $i$ . Then  $16a_4 = -4k^2 + 3r^2 - 2st$  implies that  $-4k^2 + 3r^2 - 2st \equiv 0 \pmod{16}$ . In particular,  $r$  must be even. Then, since  $4a_2 = 3r - s^2$ ,  $3r - s^2 \equiv 0 \pmod{4}$ , and it must be the case that  $r \equiv 0 \pmod{4}$  and  $s$  is even. Also,  $t = 4a_3$ , so  $2st \equiv 0 \pmod{16}$ . Then,  $-4k^2 + 3r^2 - 2st \equiv 0 \pmod{16}$  implies that  $-4k^2 + 3r^2 \equiv 0 \pmod{16}$ . This occurs iff  $4k^2 \equiv 3r^2 \equiv 0 \pmod{16}$ , a contradiction since  $k$  is odd. So,  $y^2 = x^3 - d^2x$  must be minimal for all  $d$ .

By definition,

$$\begin{aligned} \Omega(E_d) &= \int_{E_d(\mathbb{R})} \frac{dx}{|2y|} \\ &= \int_{-d}^0 \frac{dx}{\sqrt{x^3 - d^2x}} + \int_d^\infty \frac{dx}{\sqrt{x^3 - d^2x}} \\ &= \frac{1}{\sqrt{d}} \int_{-1}^0 \frac{dx}{\sqrt{x^3 - x}} + \frac{1}{\sqrt{d}} \int_1^\infty \frac{dx}{\sqrt{x^3 - x}} \\ &= \frac{\Omega(E_1)}{\sqrt{d}} \end{aligned}$$

so  $\Omega(E_d) = \Omega(E_1)/\sqrt{d}$ . □

Birch and Swinnerton-Dyer proved in [2] that  $L(E_1, 1)/\Omega(E_1) = 1/8$ . Combining these results, the conjectured order of III is

$$\frac{k_d(n_d - 2m_d)^2 \#(E_d(\mathbb{Q})_{\text{tors}})^2}{32 \prod_{p|\Delta(E_d)} c_p} \quad (2.2)$$

The quantities in this formula are easy to compute, and we were in fact able to compute the conjectured order of  $\text{III}(E_d/\mathbb{Q})$  for  $E_d$  of rank 0 with  $1 \leq d \leq 38,000,000$ . This table summarizes the results:

$p$	Fraction of $d$ with $\#\text{III}(E_d/\mathbb{Q})$ divisible by $p$
2	0.50095
3	0.31713
5	0.15963
7	0.09879
11	0.04927
13	0.03716
17	0.02290
19	0.01837
23	0.01241
29	0.00742
31	0.00633
37	0.00406

Also, 0.08898 of the  $E_d$  have trivial Tate-Shafarevich groups. Now, if we consider only twists by prime  $d$ , we have the following results:

$p$	Fraction of $d$ with $\#\text{III}(E_d/\mathbb{Q})$ divisible by $p$
2	0.49195
3	0.34697
5	0.19394
7	0.13134
11	0.07679
13	0.06281
17	0.04473
19	0.03800
23	0.02911
29	0.02049
31	0.01849
37	0.01386

In this case, 0.02732 of the  $E_d$  have trivial Tate-Shafarevich groups.

## 2.2 $y^2 = x^3 - 4dx^2 + 16d^3$

Now, consider the elliptic curve  $E : y^2 + y = x^3 - x^2$ , a curve of conductor 11. For simplicity, we will work with the equivalent Weierstrass equation  $y^2 = x^3 - 4x^2 + 16$ . Let  $E_d$  denote the twist  $y^2 = x^3 - 4dx^2 + 16d^3$ .

By [1, Example 3.1], we may take the  $F$  in Waldspurger's Theorem to be  $G \cdot H$ , where  $G = \Theta(X^2 + 11Y^2) - \Theta(3X^2 + 2XY + 4Y^2)$  and

$$H = \sum_{n=-\infty}^{\infty} q^{11n^2}.$$

In particular, for any  $d$ , let

$$n_d = \#\{(x, y, z) \in \mathbb{Z}^3 : x^2 + 11y^2 + 11z^2 = d\} \quad (2.3)$$

and

$$m_d = \#\{(x, y, z) \in \mathbb{Z}^3 : 3x^2 + 2xy + 4y^2 + 11z^2 = d\} \quad (2.4)$$

Then,

$$F = \sum_{d=1}^{\infty} a_d q^d \in S_{3/2}(44, \chi_1) \cap S_0(44, \chi_1)^\perp$$

where

$$a_d = \frac{n_d - m_d}{2}.$$

By Waldspurger's Theorem, if  $d$  and  $d_0$  are square-free natural numbers with  $d \equiv d_0 \pmod{\mathbb{Q}_2^{\times 2} \times \mathbb{Q}_{11}^{\times 2}}$  and  $dd_0$  is relatively prime to 44, then  $L(E_{-d}, 1)\sqrt{d}a_d^2 = L(E_{-d_0}, 1)\sqrt{d_0}a_{d_0}^2$ . Notice that this choice of  $F$  imposes two restraints. First, it only allows us to compute  $L(E_{-d}, 1)$  efficiently; it does not give us a way to compute  $L(E_d, 1)$ . Second, it only gives us information about  $d$  relatively prime to 44. We will only consider such  $d$  from now on.

Let  $d_0 = 1$ . It is easy to check that  $a_{d_0} = 1$  and  $L(E_{-1}, 1) = \Omega(E_{-1})$ . Then, if  $d \equiv 1 \pmod{8}$  and  $d$  is a quadratic residue mod 11,  $L(E_{-d}, 1)\sqrt{d} = a_d^2 \Omega(E_{-1})$ ; equivalently,

$$L(E_{-d}, 1) = \frac{a_d^2 \Omega(E_{-1})}{\sqrt{d}}.$$

Similarly, it is easy to check using various values of  $d_0$  that the following is true:

**Proposition 2.5.** *Suppose  $d$  is odd and a quadratic residue mod 11. If  $d \equiv 1 \pmod{4}$ , then*

$$L(E_{-d}, 1) = \frac{a_d^2 \Omega(E_{-1})}{\sqrt{d}}.$$

*If  $d \equiv 3 \pmod{4}$ , then*

$$L(E_{-d}, 1) = \frac{2a_d^2 \Omega(E_{-1})}{\sqrt{d}}.$$

We will show in Proposition 3.5 that, if  $d \equiv 1 \pmod{4}$ , then  $\Omega(E_{-d}) = \Omega(E_{-1})/\sqrt{d}$ ; if  $d \equiv 3 \pmod{4}$ , then  $\Omega(E_{-d}) = 2\Omega(E_{-1})/\sqrt{d}$ . Combining these results with BSD II, we find that the conjectured order of  $\text{III}(E_{-d}/\mathbb{Q})$  is

$$\frac{a_d^2 \#(E_{-d}(\mathbb{Q})_{\text{tors}})^2}{\prod_{p|\Delta(E_{-d})} c_p} \quad (2.5)$$

when  $d$  is a quadratic residue mod 11.

On the other hand, suppose that  $d$  is not a quadratic residue mod 11. Observe that  $x^2 + 11y^2 + 11z^2 \equiv x^2 \pmod{11}$ , so  $x^2 + 11y^2 + 11z^2 = d$  has no solutions, and  $n_d = 0$ . Similarly,  $3x^2 + 2xy + 4y^2 + 11z^2 \equiv (5x + 9y)^2 \pmod{11}$ , so  $m_d = 0$ . Therefore,  $a_d = 0$ . In this case, Waldspurger's Theorem tells us nothing about  $L(E_{-d}, 1)$ . However, we will use the functional equation of  $L(E_{-d}, s)$  to show that  $L(E_{-d}, 1) = 0$ .

In the special case  $s = 1$ , the functional equation in [11, Theorem 4.2.9] shows that  $L(E_{-d}, 1) = \omega_{E_{-d}} L(E_{-d}, 1)$  where  $\omega_{E_{-d}} \in \{\pm 1\}$ . To find  $\omega_{E_{-d}}$ , we use the following fact from [11, Section 4.3]. Let  $N_E$  denote the conductor of  $E$ . Let  $D$  be a square-free integer,  $\psi_D$  denote the Dirichlet character associated to  $\mathbb{Q}(\sqrt{D})$ , and

$$N_{\psi_D} = \begin{cases} D, & D \equiv 1 \pmod{4} \\ 4D, & D \equiv 2, 3 \pmod{4} \end{cases}.$$

Then, if  $(N_E, N_{\psi_D}) = 1$ , we have  $\omega_{E_D} = \psi_D(-N_E)\omega_E$ .

Recall that  $N_E = 11$ , so if  $d \not\equiv 0 \pmod{11}$ , then  $(N_E, N_{\psi_{-d}}) = 1$ . Using PARI, we find that  $L(E, 1) \neq 0$ , so  $L(E, 1) = \omega_E L(E, 1)$  where  $\omega_E \in \{\pm 1\}$  implies that  $\omega_E = 1$ . Therefore,  $\omega_{E_{-d}} = \psi_{-d}(-11) = \psi_d(11)$ . Since  $d$  is not a square mod 11,  $\psi_d(11) = -1$ , so  $\omega_{E_{-d}} = -1$ . Then,  $L(E_{-d}, 1) = -L(E_{-d}, 1)$ , so  $L(E_{-d}, 1) = 0$ . Thus, if  $d$  is not a quadratic residue mod 11,  $E_{-d}$  has positive analytic rank.

We computed the conjectured order of  $\text{III}(E_{-d}/\mathbb{Q})$  for  $E_{-d}$  of rank 0 with  $1 \leq d \leq 13,000,000$  and  $d$  relatively prime to 44. The following table summarizes the results:

$p$	Fraction of $E_{-d}$ with $\#\text{III}$ divisible by $p$
2	0.32894
3	0.33473
5	0.21143
7	0.11861
11	0.06582
13	0.05225
17	0.03510
19	0.02945
23	0.02150
29	0.01413
31	0.01248
37	0.00884

In this case, 0.06593 of the twists had  $\#\text{III}(E_{-d}/\mathbb{Q}) = 1$ . The following table lists the same information, but with only prime  $d$  considered:

$p$	Fraction of $E_{-d}$ with $\#\text{III}$ divisible by $p$
2	0.15329
3	0.34643
5	0.22586
7	0.13156
11	0.07667
13	0.06302
17	0.04439
19	0.03803
23	0.02902
29	0.02018
31	0.01831
37	0.01333

Here, 0.06532 of the curves had trivial Tate-Shafarevich groups.

### 2.3 $y^2 = x^3 + dx^2 - 8d^2x + 16d^3$

The last family of quadratic twists we will consider comes from the elliptic curve  $E : y^2 + xy + y = x^3 - x$ , which has conductor 14. We will use the simpler Weierstrass equation  $E : y^2 = x^3 + x^2 - 8x + 16$ , which has twists  $E_d : y^2 = x^3 + dx^2 - 8d^2x + 16d^3$ . By [1, Example 3.6.2], we may take the  $F$  in Waldspurger's Theorem to be  $G \cdot H \in S_{3/2}(56, \chi_1) \cap S_0(56, \chi_1)^\perp$ , where  $G = \Theta(X^2 + 14Y^2) - \Theta(2X^2 + 7Y^2)$  and

$$H = \sum_{n=-\infty}^{\infty} q^{14n^2}.$$

In particular, for any  $d$ , let

$$n_d = \#\{(x, y, z) \in \mathbb{Z}^3 : x^2 + 14y^2 + 14z^2 = d\},$$

$$m_d = \#\{(x, y, z) \in \mathbb{Z}^3 : 2x^2 + 7y^2 + 14z^2 = d\}.$$

Also, let

$$a_d = \frac{n_d - m_d}{2}.$$

By Waldspurger's Theorem, if  $d \equiv d_0 \pmod{\mathbb{Q}_2^{\times 2} \times \mathbb{Q}_7^{\times 2}}$  and  $dd_0$  is relatively prime to 56, then  $L(E_{-d}, 1)\sqrt{da_{d_0}^2} = L(E_{-d_0}, 1)\sqrt{d_0a_d^2}$ . In particular, we will only consider  $d$  relatively prime to 56.

Observe that  $x^2 + 14y^2 + 14z^2 \equiv x^2 \pmod{7}$ , and  $2x^2 + 7y^2 + 14z^2 \equiv (3x)^2 \pmod{7}$ , so if  $d$  is not a square mod 7, then  $n_d = m_d = 0$ . Furthermore, it is easy to check that there are no  $x, y, z$  such that  $x^2 + 14y^2 + 14z^2 \equiv 3 \pmod{8}$

or  $2x^2 + 7y^2 + 14z^2 \equiv 3 \pmod{8}$ , so if  $d \equiv 3 \pmod{8}$ , then  $n_d = m_d = 0$ . Thus, if  $d$  is not a square mod 7, or  $d \equiv 3 \pmod{8}$ , then  $a_d = 0$ . Unlike the family of twists discussed in section 2.2, it is not in general true that  $L(E_{-d}, 1) = 0$  in these instances; for example,  $L(E_{-3}, 1) \neq 0$ . So, we are not able to efficiently compute  $\#\text{III}(E_{-d}/\mathbb{Q})$  for all  $E_{-d}$  with  $d$  relatively prime to 56; rather, we can only compute  $\#\text{III}(E_{-d}/\mathbb{Q})$  when  $a_d \neq 0$ .

We can show a result analogous to Proposition 2.5, that if  $a_d \neq 0$ , then

$$L(E_{-d}, 1) = \frac{a_d^2 \Omega(E_{-1}, 1)}{\sqrt{d}}.$$

Using this, we computed the conjectured order of  $\text{III}(E_{-d}/\mathbb{Q})$  for  $1 \leq d \leq 18,000,000$  such that  $d$  is relatively prime to 56 and  $a_d \neq 0$ . We find that 0.06054 of the curves of rank 0 have trivial Tate-Shafarevich groups. The other results are summarized here:

$p$	Fraction of $E_{-d}$ with $\#\text{III}$ divisible by $p$
2	0.56244
3	0.38305
5	0.15741
7	0.09689
11	0.04724
13	0.03565
17	0.02131
19	0.01700
23	0.01115
29	0.00629
31	0.00534
37	0.00326

If we consider only prime  $d$ , then we have the following:

$p$	Fraction of $E_{-d}$ with $\#\text{III}$ divisible by $p$
2	0.65116
3	0.39831
5	0.17071
7	0.10871
11	0.05640
13	0.04359
17	0.02718
19	0.02225
23	0.01506
29	0.00871
31	0.00779
37	0.00470

In this case, 0.03089 of the curves have trivial Tate-Shafarevich groups.

## 2.4 Observations

First, notice with the second and third families of quadratic twists, there is a significant difference between the fraction of twists with even order when considering all twists and just twists by primes. This suggests that the conjectured order of  $\text{III}(E_{-d}/\mathbb{Q})$  is related to the factorization of  $d$ .

In general, we expect the density of trivial Tate-Shafarevich groups to be 0 in a family of quadratic twists. Our data seems to support this claim; for instance, in the first example, if we only consider  $d$  such that  $1 \leq d \leq 1,000,000$ , then 0.17285 of the curves have trivial Tate-Shafarevich groups. As we take larger upper bounds for  $d$ , this density decreases. However, the convergence of the density occurs very slowly, so it is difficult to determine whether the density of trivial Tate-Shafarevich groups is actually 0. The slow rate of convergence also makes it difficult to approximate the probability that a prime  $p$  divides the conjectured order of  $\text{III}$ .

In [4], Delaunay gives a heuristic assumption for Tate-Shafarevich groups of elliptic curves defined over  $\mathbb{Q}$ . Based on the heuristic assumption, Delaunay concludes that, if we take the isomorphism classes of elliptic curves  $E$  of rank 0 defined over  $\mathbb{Q}$ , assumed to be ordered by the conductor  $N(E)$ , then the probability that a prime  $p$  divides  $\#\text{III}$  is equal to

$$f_0(p) = 1 - \prod_{k=1}^{\infty} (1 - (1/p)^{2k-1}).$$

In particular,

$$\begin{aligned} f_0(2) &\sim 0.580566 \\ f_0(3) &\sim 0.360995 \\ f_0(5) &\sim 0.20666 \\ f_0(7) &\sim 0.145408 \end{aligned}$$

From our three examples, it seems clear that the heuristic assumption cannot be applied to families of quadratic twists without modification; in fact, the values of  $f_0(2)$  suggested by our data vary widely among the three families studied. On the other hand, it is not clear whether the values of  $f_0(p)$  for  $p > 2$  are reasonable for families of quadratic twists.

It is in fact not surprising that the value of  $f_0(2)$  predicted by [4] does not match the values suggested by our data. If we consider the isomorphism classes of all elliptic curves of rank 0 over  $\mathbb{Q}$ , as Delaunay does, there does not seem to be a strong relationship between  $\text{III}$  for one curve and  $\text{III}$  for another. However, in

a family of quadratic twists  $E_d$ ,  $E[2]$  and  $E_d[2]$  are isomorphic as  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ -modules, so  $H^1(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E[2]) = H^1(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E_d[2])$ . Since  $S_2(E_d/\mathbb{Q})$ , the 2-part of the Selmer group, is contained in  $H^1(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E_d[2])$ , this indicates that the 2-parts of Selmer groups for various twists of the same curve should be related. By [12, Theorem X.4.2], there is an exact sequence

$$0 \longrightarrow E_d(\mathbb{Q})/2E_d(\mathbb{Q}) \xrightarrow{\phi} S_2(E_d/\mathbb{Q}) \xrightarrow{\psi} \text{III}(E_d/\mathbb{Q})[2] \longrightarrow 0,$$

so the 2-parts of Tate-Shafarevich groups for various twists of the same curve should also be related.

### 3 The Conjectured 2-Part of III

In this section, we will use the Birch and Swinnerton-Dyer conjectures to explain and refine some of the results from the previous section. We will focus on the 2-part of  $\text{III}(E_{-d}/\mathbb{Q})$ . As we mentioned in section 2.3, the family  $y^3 = x^3 + dx^2 - 8d^2x + 16d^3$  is somewhat unsuitable for study since our choice of  $F$  does not allow us to find the value of the  $L$ -series at 1 for all twists of rank 0. Therefore, we will concentrate on studying the other two families of quadratic twists.

#### 3.1 $y^2 = x^3 - p^2x$

We will consider the family of curves  $E_p : y^2 = x^3 - p^2x$  for odd primes  $p$ . Recall from equation (2.2) and section 2.1 that the conjectured order of  $\text{III}(E_p/\mathbb{Q})$  is

$$\frac{(n_p - 2m_p)^2 \#(E_p(\mathbb{Q})_{\text{tors}})^2}{32 \prod_{q|\Delta(E_p)} c_q} \quad (3.6)$$

where

$$\begin{aligned} n_p &= \#\{(x, y, z) \in \mathbb{Z}^3 : x^2 + 2y^2 + 8z^2 = p\}, \\ m_p &= \#\{(x, y, z) \in \mathbb{Z}^3 : x^2 + 2y^2 + 32z^2 = p\}. \end{aligned}$$

It is easy to check that  $\Delta(E_p) = 64p^6$ .

**Proposition 3.1.**  $c_2 = 2$  and  $c_p = 4$ .

**Proof.** First, we will show that  $c_2 = 2$ . Observe that  $E_p$  reduced modulo 2 is  $y^2 = x^3 - x$ , which has exactly one singular point,  $(1, 0)$ . Then, since  $p$  is an odd prime,  $(p, 0) \in E(\mathbb{Q}_2) - E_0(\mathbb{Q}_2)$ . Let  $P = (x, y) \in E(\mathbb{Q}_2) - E_0(\mathbb{Q}_2)$ . Let  $\tilde{P}$  denote the reduction of  $P \pmod{2}$ ; since  $P \notin E_0(\mathbb{Q}_2)$ ,  $\tilde{P} = (1, 0)$ . In particular,

$\tilde{P}$  is singular, so  $x \equiv 1 \pmod{2}$ . We will show that  $P \in (p, 0) + E_0(\mathbb{Q}_2)$ . By the addition law on the elliptic curve,

$$P + (p, 0) = (x, y) + (p, 0) = \left( p \frac{x+p}{x-p}, \frac{-2p^2y}{(x-p)^2} \right).$$

Since  $x \equiv 1 \pmod{2}$  and  $p$  is odd, either  $x \equiv p \pmod{4}$  or  $x \equiv p+2 \pmod{4}$ . If  $x \equiv p \pmod{4}$ , then  $\widetilde{P + (p, 0)} = O$ . If  $x \equiv p+2 \pmod{4}$ , then  $\widetilde{P + (p, 0)} = (0, 0)$ . In either case,  $P + (p, 0) \in E_0(\mathbb{Q}_2)$ , so  $P \in (p, 0) + E_0(\mathbb{Q}_2)$ . Therefore,  $c_2 = \#(E(\mathbb{Q}_2)/E_0(\mathbb{Q}_2)) = 2$ .

Now, we will show that  $c_p = 4$ . Observe that  $E_p$  reduced modulo  $p$  is  $y^2 = x^3$ , which has the singular point  $(0, 0)$ . Then,  $(0, 0), (p, 0), (-p, 0) \in E(\mathbb{Q}_p) - E_0(\mathbb{Q}_p)$ . It is easy to check that these three points are elements of distinct cosets of  $E_0(\mathbb{Q}_p)$ , so  $c_p \geq 4$ . By [12, Corollary C.15.2.1],  $c_p \leq 4$ . Therefore,  $c_p = 4$ .  $\square$

Applying the previous proposition to equation (3.6) gives the conjectured order

$$\#\text{III}(E_p/\mathbb{Q}) = \frac{\#(E_p(\mathbb{Q})_{\text{tors}})^2 (n_p - 2m_p)^2}{256}.$$

Observe that  $E_p(\mathbb{Q})[2] = \{O, (0, 0), (p, 0), (-p, 0)\}$ . Using the duplication formula and the fact that points of finite order have integer coordinates, we can check that  $E_p(\mathbb{Q})$  has no points of order 4, so  $E_p(\mathbb{Q})_{\text{tors}} = 4k$  for some odd integer  $k$ . Then, the conjectured order of  $\text{III}(E_p/\mathbb{Q})$  is

$$\frac{k^2 (n_p - 2m_p)^2}{16}.$$

In particular, the conjectured order of  $\text{III}(E_p/\mathbb{Q})$  is odd iff  $n_p - 2m_p \equiv 4 \pmod{8}$ .

Observe that  $x^2 + 2y^2 + 8z^2, x^2 + 2y^2 + 32z^2 \equiv x^2 + 2y^2 \equiv 0, 1, 2, 3 \pmod{8}$ . In particular, if  $p \equiv 5, 7 \pmod{8}$ , then  $n_p = m_p = 0$ , so,  $L(E_p, 1) = 0$  by equation (2.1). In this case,  $E_p$  has positive analytic rank. Since we are only interested in curves of analytic rank 0, we will only consider  $p \equiv 1, 3 \pmod{8}$ .

**Proposition 3.2.** *If  $E_p$  has analytic rank 0, then the conjectured order of  $\text{III}(E_p/\mathbb{Q})$  is odd iff  $p \equiv 3 \pmod{8}$ .*

**Proof.** If  $(x, y, z)$  is a solution to  $x^2 + 2y^2 + 32z^2 = p$ , then so are all of the elements of  $\{(\pm x, \pm y, \pm z)\}$ . Then, the set of solutions to  $x^2 + 2y^2 + 32z^2 = p$  can be partitioned into sets of the form  $\{(\pm x, \pm y, \pm z)\}$ . Since  $p$  is prime, if  $x^2 + 2y^2 + 32z^2 = p$ , then at least two of  $x, y$ , and  $z$  must be non-zero. Thus, the set  $\{(\pm x, \pm y, \pm z)\}$  has either 4 or 8 elements. So,  $m_p \equiv 0 \pmod{4}$ , and  $2m_p \equiv 0 \pmod{8}$ . Therefore, the conjectured order of  $\text{III}(E_p/\mathbb{Q})$  is odd iff  $n_p \equiv 4 \pmod{8}$ .

Similarly, if  $(x, y, z)$  is a solution to  $x^2 + 2y^2 + 8z^2 = p$ , then so are all of the elements of  $\{(\pm x, \pm y, \pm z)\}$ . Observe that  $\{(\pm x, \pm y, \pm z)\}$  has 8 elements if  $x$ ,  $y$ , and  $z$  are all non-zero; otherwise, it has 4 elements. Since  $p$  is odd, it is impossible for  $x$  to be 0. If  $(x, 0, z)$  is a solution, then  $x^2 + 8z^2 = p$  implies that  $x^2 + 2(2z)^2 = p$ , so  $(x, 2z, 0)$  is a solution. Similarly, if  $(x, y, 0)$  is a solution with  $y$  even, then  $x^2 + 2y^2 = p$  implies  $x^2 + 8(y/2)^2 = p$ , so  $(x, 0, y/2)$  is also a solution. Therefore,  $n_p \equiv 4 \pmod{8}$  iff there are an odd number of solutions of  $x^2 + 2y^2 = p$  with  $x, y > 0$  and  $y$  odd. Any such solution has  $x^2 + 2y^2 \equiv 3 \pmod{8}$  since  $y$  is odd, so if  $p \equiv 1 \pmod{8}$ , then the conjectured order of  $\text{III}(E_p/\mathbb{Q})$  is even.

Now, suppose  $p \equiv 3 \pmod{8}$ . Let  $\omega = \sqrt{-2}$ . Then,  $\mathbb{Z}[\omega]$  is the ring of integers of  $\mathbb{Q}(\sqrt{-2})$  and is a unique factorization domain. Since  $p \equiv 3 \pmod{8}$ ,  $p$  is not prime over  $\mathbb{Z}[\omega]$ , so there exists  $\pi \in \mathbb{Z}[\omega]$  such that  $\pi\bar{\pi} = p$ . Observe that  $[\mathbb{Z}[\omega] : \mathbb{Z}] = 2$ , so  $p$  has at most 2 prime factors, and  $(\pi)$  and  $(\bar{\pi})$  must both be prime. Since  $\pi \in \mathbb{Z}[\omega]$ ,  $\pi = x + y\omega$  for some  $x, y \in \mathbb{Z}$ . Then,  $x^2 + 2y^2 = p$ , and  $y$  must be odd since  $p \equiv 3 \pmod{8}$ . Since  $\mathbb{Z}[\omega]$  is a unique factorization domain, this is the only solution of  $x^2 + 2y^2 = p$ , up to units. Therefore, there is only one solution to  $x^2 + 2y^2 = p$  with  $x, y > 0$  and  $y$  odd. So,  $n_p \equiv 4 \pmod{8}$ .

Therefore, the conjectured order of  $\text{III}(E_p/\mathbb{Q})$  is odd iff  $p \equiv 3 \pmod{8}$ .  $\square$

In [8, Theorem 1], Razar used alternate methods to show that, if  $p \equiv 3 \pmod{8}$ , then

$$\frac{2L(E_p, 1)}{\Omega(E_p)}$$

is odd. Combined with BSD II, this provides a different proof of the fact that the conjectured order of  $\text{III}(E_p/\mathbb{Q})$  is odd when  $p \equiv 3 \pmod{8}$ .

In section 2.1, we found that 0.49195 of the twists  $E_p$  had Tate-Shafarevich groups of even order; Proposition 3.2 explains why this is true.

### 3.2 $y^2 = x^3 - 4dx^2 + 16d^3$

Now, consider the family of curves  $E_d : y^2 = x^3 - 4dx^2 + 16d^3$ . For this section, we will take  $d$  to be a square free natural number which is relatively prime to 44.

Recall from section 2.2 that we defined

$$\begin{aligned} n_d &= \#\{(x, y, z) \in \mathbb{Z}^3 : x^2 + 11y^2 + 11z^2 = d\} \\ m_d &= \#\{(x, y, z) \in \mathbb{Z}^3 : 3x^2 + 2xy + 4y^2 + 11z^2 = d\} \\ a_d &= \frac{n_d - m_d}{2} \end{aligned}$$

Then, equation (2.5) gives us a relationship between  $a_d$  and the conjectured order of  $\text{III}(E_{-d}/\mathbb{Q})$ .

**Proposition 3.3.** *If  $d \equiv 1 \pmod{4}$ , then  $y^2 = x^3 - 4dx^2 + 16d^3$  is a minimal equation for  $E_{-d}$ . If  $d \equiv 3 \pmod{4}$ , then*

$$y^2 + y = x^3 + dx^2 - \frac{1}{4}(d^3 + 1)$$

*is a minimal equation for  $E_{-d}$ .*

**Proof.** Observe that  $E_{-d}$  has the Weierstrass equation

$$y^2 = x^3 + 4dx^2 - 16d^3 \tag{3.7}$$

Recall that a minimal equation for  $E_{-d}$  is a Weierstrass equation for  $E_{-d}$  with coefficients in  $\mathbb{Z}$  for which  $|\Delta(E_{-d})|$  is minimal.

First, we will show that equation (3.7) is minimal if  $d \equiv 1 \pmod{4}$ . Assume that the equation is not minimal. Then, there is a change of variables which produces a minimal equation. Since this change of variables fixes the point  $[0, 1, 0]$  on the curve and preserves the Weierstrass form of the equation, it must have the form  $x = u^2x' + r$ ,  $y = u^3y' + u^2sx' + t$  for  $u, r, s, t \in \overline{\mathbb{Q}}$ ; under this change of variables, the new curve will have discriminant  $u^{-12}(-2^{12}11d^6)$ . By [12, Proposition VII.1.3], we may take  $u, r, s, t \in \mathbb{Z}$  with  $u > 0$ . So,  $u$  must be 2, and the change of variables  $x = 4x' + r$ ,  $y = 8y' + 4sx' + t$  gives a minimal equation for some  $r, s, t \in \mathbb{Z}$ . Under this transformation, we get a curve  $y'^2 + a_1x'y' + a_3y' = x'^3 + a_2x'^2 + a_4x' + a_6$  where

$$\begin{aligned} 2a_1 &= 2s \\ 4a_2 &= 4d + 3r - s^2 \\ 8a_3 &= 2t \\ 16a_4 &= 8rd + 3r^2 - 2st \\ 64a_6 &= -16d^3 + 4r^2d + r^3 - t^2 \end{aligned}$$

Then, since  $16a_4 = 8rd + 3r^2 - 2st$  and  $a_4 \in \mathbb{Z}$ , we must have  $8rd + 3r^2 - 2st \equiv 0 \pmod{16}$ . In particular,  $r$  must be even. Since  $4a_2 = 4d + 3r - s^2$ ,  $3r - s^2 \equiv 0 \pmod{4}$ , and it must be the case that  $r \equiv 0 \pmod{4}$  and  $s$  is even. Then,  $4r^2d + r^3 \equiv 0 \pmod{64}$ , so  $64a_6 = -16d^3 + 4r^2d + r^3 - t^2 \equiv -16d^3 - t^2 \pmod{64}$ . Since  $a_6 \in \mathbb{Z}$ ,  $-16d^3 - t^2 \equiv 0 \pmod{64}$ . Recall that  $d \equiv 1 \pmod{4}$ , so  $d^3 \equiv 1 \pmod{4}$ , and  $16d^3 \equiv 16 \pmod{64}$ . Therefore,  $t^2 \equiv -16 \pmod{64}$ . However, this is impossible, so equation (3.7) must be minimal.

Now, suppose  $d \equiv 3 \pmod{4}$ . Applying the change of variables  $x = 4x'$ ,  $y = 8y' + 4$  to equation (3.7), we get the curve

$$y'^2 + y' = x'^3 + dx'^2 - \frac{1}{4}(d^3 + 1)$$

which has integer coefficients since  $d \equiv 3 \pmod{4}$ . This equation has discriminant  $-11d^6$  so is minimal by [12, VII, Remark 1.1].  $\square$

**Corollary 3.4.** *If  $d \equiv 1 \pmod{4}$ , then the discriminant of  $E_{-d}$  is  $-2^{12}11d^6$ . If  $d \equiv 3 \pmod{4}$ , then the discriminant of  $E_{-d}$  is  $-11d^6$ .*

**Proof.** This follows immediately from Proposition 3.3.  $\square$

Recall that we used the following proposition in Section 2.2:

**Proposition 3.5.** *If  $d \equiv 1 \pmod{4}$ , then  $\Omega(E_{-d}) = \Omega(E_{-1})/\sqrt{d}$ ; if  $d \equiv 3 \pmod{4}$ , then  $\Omega(E_{-d}) = 2\Omega(E_{-1})/\sqrt{d}$ .*

**Proof.** It is easy to check that  $x^3 - 4dx^2 + 16d^3$  has exactly one real root. Let  $r$  be the real root of  $x^3 + 4x^2 - 16$ . Then,  $rd$  is the real root of  $x^3 + 4dx^2 - 16d^3$ . Let

$$\Omega'(E_{-d}) = \int_{rd}^{\infty} \frac{dx}{|2y|}$$

Then,

$$\begin{aligned} \Omega'(E_{-d}) &= \int_{rd}^{\infty} \frac{dx}{|2y|} \\ &= \int_{rd}^{\infty} \frac{dx}{\sqrt{x^3 + 4dx^2 - 16d^3}} \\ &= \frac{1}{\sqrt{d}} \int_r^{\infty} \frac{dx}{\sqrt{x^3 + 4x^2 - 16}} \\ &= \frac{\Omega'(E_{-1})}{\sqrt{d}} \end{aligned} \tag{3.8}$$

If  $d \equiv 1 \pmod{4}$ , then  $y^2 = x^3 + 4dx^2 - 16d^3$  is minimal by Proposition 3.3, so  $\Omega(E_{-d}) = \Omega'(E_{-d})$ . In particular,  $\Omega(E_{-1}) = \Omega'(E_{-1})$ . By equation 3.8,  $\Omega(E_{-d}) = \Omega(E_{-1})/\sqrt{d}$ .

If  $d \equiv 3 \pmod{4}$ , then we showed in the proof of 3.3 that the change of variables  $x = 4x'$ ,  $y = 8y' + 4$  applied to  $y^2 = x^3 + 4dx^2 - 16d^3$  gives a minimal equation for  $E_{-d}$ . Then,

$$\begin{aligned} \Omega(E_{-d}) &= \int_{E_{-d}} (\mathbb{R}) \frac{dx'}{|2y' + 1|} \\ &= \int_{rd}^{\infty} \frac{dx/4}{|y/4|} \\ &= \int_{rd}^{\infty} \frac{dx}{|y|} \\ &= 2\Omega'(E_{-d}) \\ &= \frac{2\Omega'(E_{-1})}{\sqrt{d}} \text{ by equation (3.8)} \end{aligned}$$

We already showed that  $\Omega(E_{-1}) = \Omega'(E_{-1})$ , so  $\Omega(E_{-d}) = 2\Omega(E_{-1})/\sqrt{d}$ .  $\square$

Since  $x^3 + 4dx^2 - 16d^3$  has no rational roots,  $\#E_{-d}(\mathbb{Q})_{\text{tors}}$  is odd. By equation (2.5), the conjectured order of  $\text{III}(E_{-d}/\mathbb{Q})$  is odd iff

$$\frac{a_d^2}{\prod_{p|\Delta(E_{-d})} c_p}$$

is odd. In particular, if  $a_d$  is odd, then the conjectured order of  $\text{III}(E_{-d}/\mathbb{Q})$  must be odd as well. We will now give a sufficient condition for  $a_d$  to be odd.

**Proposition 3.6.**  *$a_d$  is odd iff  $3x^2 + 2xy + 4y^2 = d$  has an odd number of solutions with  $x > 0$ .*

**Proof.** By the definition of  $a_d$ ,  $a_d$  is odd iff  $n_d - m_d \equiv 2 \pmod{4}$ . Observe that if  $(x, y, z)$  is a solution to  $x^2 + 11y^2 + 11z^2 = d$ , then  $(\pm x, \pm y, \pm z)$  are solutions as well. Since  $d$  is square-free, at least two of  $x$ ,  $y$ , and  $z$  must be non-zero. In particular,  $\{(\pm x, \pm y, \pm z)\}$  has either 4 or 8 elements. Thus,  $n_d \equiv 0 \pmod{4}$ , and  $a_d$  is odd iff  $m_d \equiv 2 \pmod{4}$ .

Similarly, if  $(x, y, z)$  is a solution to  $3x^2 + 2xy + 4y^2 + 11z^2 = d$ , then  $(x, y, \pm z)$  and  $(-x, -y, \pm z)$  are also solutions. The set  $\{(x, y, \pm z), (-x, -y, \pm z)\}$  has 2 distinct elements if  $z = 0$  and 4 distinct elements otherwise. So,  $m_d \equiv 2 \pmod{4}$  iff there are an odd number of pairs of solutions  $\{(x, y, 0), (-x, -y, 0)\}$ . Equivalently,  $m_d \equiv 2 \pmod{4}$  iff  $3x^2 + 2xy + 4y^2 = d$  has an odd number of solutions with  $x > 0$ .  $\square$

Fix a square-free  $d$  which is not divisible by 11. Let  $K = \mathbb{Q}(E_{-d}[2]) = \mathbb{Q}(E[2])$ .

We showed in Corollary 3.4 that  $\sqrt{\Delta(E_{-d})} = n\sqrt{-11}$  for some integer  $n$ , so  $\sqrt{-11} \in K$ . Therefore,  $\mathbb{Q}(\sqrt{-11}) \subseteq K$ . Let  $\omega = \frac{1+\sqrt{-11}}{2}$ . Then,  $\omega\bar{\omega} = 3$ , and  $3x^2 + 2xy + 4y^2 = (\omega x + 2y)(\bar{\omega}x + 2y)$ . Moreover,  $\mathbb{Z}[\omega]$  is the ring of algebraic integers of  $\mathbb{Q}(\sqrt{-11})$ , and  $\mathbb{Z}[\omega]$  is a principal ideal domain.

**Lemma 3.7.** *Let  $\mathfrak{p}$  be a prime in  $\mathbb{Q}(\sqrt{-11})$  which is unramified in  $K$ . Since  $\mathbb{Z}[\omega]$  is a principal ideal domain,  $\mathfrak{p}$  has a generator  $\pi$ . Then,  $\mathfrak{p}$  is prime in  $K$  iff  $\pi \notin 1 + 2\mathbb{Z}[\omega]$ . If  $\mathfrak{p}$  is not prime in  $K$ , then it splits into three primes over  $K$ .*

**Proof.** Let  $F = \mathbb{Q}(\sqrt{-11}) \subseteq K$ . Then,  $\mathcal{O}_F = \mathbb{Z}[\omega]$ . Recall that  $K$  is the splitting field of the polynomial  $x^3 + 4x^2 - 16$ , so  $K/\mathbb{Q}$  is a Galois extension. Then,  $K/F$  is also Galois. Observe that  $[K : F] = 3$ , so  $K/F$  is a cyclic extension; in particular,  $K/F$  is abelian. For a prime  $\mathfrak{p}$  of  $F$ , let  $N_{\mathfrak{p}}$  denote the number of elements of  $\mathcal{O}_F/\mathfrak{p}$ . There is a map which sends each prime  $\mathfrak{p}$  of  $F$  which is unramified in  $K$  to the unique  $\sigma \in \text{Gal}(K/F)$  that satisfies  $\sigma\alpha \equiv \alpha^{N_{\mathfrak{p}}} \pmod{\mathfrak{P}}$  for all  $\alpha \in \mathcal{O}_K$  where  $\mathfrak{P}$  is a prime above  $\mathfrak{p}$ ; the choice of  $\mathfrak{P}$  does not matter since  $K/F$  is abelian. This map can be extended to the subgroup  $I(\mathfrak{d})$  of fractional ideals prime to the discriminant  $\mathfrak{d}$  of  $K/F$  by multiplicativity. This new map is a homomorphism  $\phi : I(\mathfrak{d}) \rightarrow \text{Gal}(K/F)$ , called the Artin map (see [6, X.§1]).

We need a few more definitions; see [6, VI.§1] and [6, VII.§4] for more details.

A cycle of  $F$  is a formal product

$$\mathfrak{c} = \prod_{v \in M_F} v^{m(v)}$$

where  $m(v)$  are non-negative integers such that only finitely many  $m(v)$  are non-zero. Let

$$\mathfrak{c}_0 = \prod_{\mathfrak{p} \neq v_\infty} \mathfrak{p}^{m(\mathfrak{p})}.$$

Let  $I(\mathfrak{c})$  be the group of fractional ideals relatively prime to  $\mathfrak{c}_0$ . Let  $P_{\mathfrak{c}}$  be the subgroup of  $I(\mathfrak{c})$  consisting of principal ideals  $(\alpha)$  such that  $\alpha$  satisfies the following two conditions:

1. If  $\mathfrak{p}$  is a prime ideal with multiplicity  $m(\mathfrak{p}) > 0$  in  $\mathfrak{c}$ , then  $\alpha$  lies in the local ring  $(\mathcal{O}_F)_{\mathfrak{p}}$  and  $\alpha \equiv 1 \pmod{\mathfrak{m}_{\mathfrak{p}}^{m(\mathfrak{p})}}$  where  $\mathfrak{m}_{\mathfrak{p}}$  is the maximal ideal of  $(\mathcal{O}_F)_{\mathfrak{p}}$ .
2. If  $v$  is a real absolute value in  $M_F$  having multiplicity  $m(v) > 0$  in  $\mathfrak{c}$ , and  $\sigma_v$  is the corresponding embedding of  $F$  in  $\mathbb{R}$ , then  $\sigma_v \alpha > 0$ .

Let  $\mathfrak{N}(\mathfrak{c})$  denote the subgroup of  $I(\mathfrak{c})$  consisting of all norms  $N_F^K \mathfrak{A}$  where  $\mathfrak{A}$  is a fractional ideal of  $K$  prime to  $\mathfrak{c}$ .

Let  $\mathfrak{p}$  be a prime of  $F$  which is unramified in  $K$ . Since  $K/F$  is Galois and  $[K : F] = 3$ , either  $\mathfrak{p}$  is prime over  $K$ , or  $\mathfrak{p}$  splits completely into the product of three primes. It is shown in [6, I.§6] that a prime  $\mathfrak{p}$  splits completely iff  $\mathfrak{p} \in \ker \phi$ . Thus, it suffices to show that  $\ker \phi = P_2$ .

It is easy to check that 2 is the only prime in  $F$  which is ramified in  $K$ . By [6, X.§2, Theorem 2], there exists a cycle  $\mathfrak{c}$  of  $F$  divisible only by 2 such that the kernel of the Artin map in  $I(\mathfrak{c})$  is equal to  $P_{\mathfrak{c}} \mathfrak{N}(\mathfrak{c})$ . In particular,  $P_{\mathfrak{c}}$  is contained in the kernel of the Artin map. Since  $\mathfrak{c}$  is divisible only by 2,  $\mathfrak{c} = 2^k$  for some integer  $k$ . By [6, X.§1, Theorem 1],  $\phi : I(\mathfrak{c}) \rightarrow \text{Gal}(K/F)$  is surjective, so  $I(\mathfrak{c})/\ker \phi \cong \text{Gal}(K/F) \cong \mathbb{Z}/3\mathbb{Z}$ . Assume  $k = 0$ ; then  $P_{\mathfrak{c}}$  is the set of principal fractional ideals. We can check that  $F$  has class number 1, so  $P_{\mathfrak{c}} = I(\mathfrak{c})$ , a contradiction since then  $I(\mathfrak{c})/\ker \phi$  is trivial. So,  $k$  must be positive, and  $P_{\mathfrak{c}}$  is a subgroup of  $P_2$ .

Since  $P_{\mathfrak{c}}$  is contained in  $\ker \phi$ , the map  $\bar{\phi} : P_2/P_{\mathfrak{c}} \rightarrow \text{Gal}(K/F)$  defined by  $\bar{\phi}(\mathfrak{a} + P_{\mathfrak{c}}) = \phi(\mathfrak{a})$  is well-defined. Observe that  $P_2/P_{\mathfrak{c}}$  has order  $2^{k-1}$  while  $\text{Gal}(K/F)$  has order 3, so  $\bar{\phi}$  must be the trivial map. That is,  $P_2 \subseteq \ker \phi$ . Since  $|I(\mathfrak{c}) : P_2| = 3 = |I(\mathfrak{c}) : \ker \phi|$ ,  $P_2$  must be the kernel of  $\phi$ .  $\square$

**Corollary 3.8.** *Let  $p \neq 11$  be an odd prime. If  $p$  is not a quadratic residue mod 11, then  $p$  splits into three primes over  $K$ . If  $p$  is a quadratic residue mod 11, then  $p$  splits into either two or six primes over  $K$ .*

**Proof.** Let  $F = \mathbb{Q}(\sqrt{-11})$ . If  $p$  is not a quadratic residue mod 11, then  $p$  is prime over  $F$ . Since  $p$  is odd,  $p$  is unramified and  $p \in 1 + 2\mathbb{Z}[\omega]$ . By Lemma 3.7,  $p$  splits into three primes over  $K$ .

Now, suppose  $p$  is a quadratic residue mod 11. Then,  $p$  is not prime over  $F$ . Since  $p$  is unramified over  $F$  and  $[F : \mathbb{Q}] = 2$ ,  $p$  must split as the product of two primes over  $F$ , so  $p = (\pi)(\bar{\pi})$  for some prime  $\pi$ . Observe that  $\pi \in 1 + 2\mathbb{Z}[\omega]$  iff  $\bar{\pi} \in 1 + 2\mathbb{Z}[\omega]$ . By Lemma 3.7, either  $\pi$  and  $\bar{\pi}$  are both prime over  $K$ , or they both split into three primes over  $K$ . So,  $p$  splits into either two or six primes over  $K$ .  $\square$

**Lemma 3.9.** *Suppose  $p$  is an odd prime which is a square mod 11. Then,  $a_p$  is odd iff  $p$  splits into two primes over  $K$ , and  $a_p$  is even iff  $p$  splits into six primes over  $K$ .*

**Proof.** By Corollary 3.8,  $p$  splits into either two primes or six primes over  $K$ . Also,  $p$  splits into two primes over  $\mathbb{Q}(\sqrt{-11})$ . Since  $\mathbb{Z}[\omega]$  is a principal ideal domain, it is a unique factorization domain. Therefore,  $(\omega x + 2y)(\bar{\omega}x + 2y) = 3x^2 + 2xy + 4y^2 = p$  has either 0 or 1 solution with  $x > 0$ . Suppose first that  $a_p$  is odd. Then, there exist  $x, y \in \mathbb{Z}$  with  $x > 0$  such that  $3x^2 + 2xy + 4y^2 = (\omega x + 2y)(\bar{\omega}x + 2y) = p$ . Since  $p$  is an odd prime and  $2xy + 4y^2$  is even,  $x$  must be odd. Since  $p$  is square-free,  $y \neq 0$ . Let  $\pi = \omega x + 2y$ . Then,  $\bar{\pi} = \bar{\omega}x + 2y$ , so  $\pi\bar{\pi} = p$ . Since  $x$  is odd,  $\pi \in \omega + 2\mathbb{Z}[\omega]$  and  $\bar{\pi} \in \bar{\omega} + 2\mathbb{Z}[\omega]$ . Recall that  $p$  factors as the product of two primes in  $\mathbb{Z}[\omega]$ , so  $(\pi)$  and  $(\bar{\pi})$  must be prime. By Lemma 3.7,  $(\pi)$  and  $(\bar{\pi})$  are prime in  $K$ , so  $p$  splits into two primes over  $K$ .

Otherwise,  $a_p$  is even, so  $3x^2 + 2xy + 4y^2 = p$  has no solutions. Since  $p$  is a square mod 11,  $p$  is not prime over  $K$ , so  $p = \pi\bar{\pi}$  for some  $\pi \in \mathbb{Z}[\omega]$ . Again,  $(\pi)$  and  $(\bar{\pi})$  must be prime since  $p$  splits into two primes in  $\mathbb{Z}[\omega]$ . We can express  $\pi$  as  $a + b\omega$  for some  $a, b \in \mathbb{Z}$ . Since  $3x^2 + 2xy + 4y^2 = (\omega x + 2y)(\bar{\omega}x + 2y) = p$  has no solutions, it must be the case that  $a$  is odd. Observe that  $\omega + \bar{\omega} = 1$ , so  $p = \pi\bar{\pi} = (a + b\omega)(a + b\bar{\omega}) = [(a + b) - b\bar{\omega}][(a + b) - b\omega]$ . If  $b$  is odd, then  $a + b$  is even, so  $3x^2 + 2xy + 4y^2 = p$  has a solution, a contradiction. So, it must be the case that  $b$  is even. Therefore,  $a + b\omega \in 1 + 2\mathbb{Z}[\omega]$ , and  $\pi$  splits into 3 primes over  $K$  by Lemma 3.7. Similarly,  $\bar{\pi}$  splits into 3 primes over  $K$ , so  $p$  splits into 6 primes over  $K$ .  $\square$

**Proposition 3.10.** *Let  $d$  be a square-free natural number which is relatively prime to 44. Then,  $a_d$  is odd iff each prime divisor of  $d$  splits into two primes over  $K$ .*

**Proof.** By Corollary 3.8, any square-free natural number  $d$  which is relatively prime to 44 can be expressed as

$$\left( \prod_{i=1}^n p_i \right) \left( \prod_{i=1}^m q_i \right) \left( \prod_{i=1}^l r_i \right)$$

where each  $p_i$  is a rational prime which splits into two primes over  $K$ , each  $q_i$  is

a rational prime which splits into three primes over  $K$ , and each  $r_i$  is a rational prime which splits into six primes over  $K$ .

Suppose  $(x, y)$  is a solution to  $3x^2 + 2xy + 4y^2 = d$ . Since  $d$  is odd,  $x$  must be odd as well. Then,  $(\omega x + 2y)(\bar{\omega}x + 2y) = d$ , and  $\omega x + 2y \in \omega + 2\mathbb{Z}[\omega]$ . By Lemma 3.7, each  $p_i$  can be factored as  $\pi_i \bar{\pi}_i$  where  $\pi_i \in \omega + 2\mathbb{Z}[\omega]$  and  $(\pi_i), (\bar{\pi}_i)$  are prime. Each  $q_i$  is prime over  $\mathbb{Z}[\omega]$ , and each  $r_i$  can be factored over  $\mathbb{Z}[\omega]$  as  $\rho_i \bar{\rho}_i$  where  $\rho_i \in 1 + 2\mathbb{Z}[\omega]$  and  $(\rho_i), (\bar{\rho}_i)$  are prime. Each prime factor of  $\omega x + 2y$  must be one of the  $\pi_i, \bar{\pi}_i, q_i, \rho_i$ , or  $\bar{\rho}_i$ . So, there exist  $a_i, b_i, c_i, d_i, e_i$  such that

$$\omega x + 2y = \left( \prod \pi_i^{a_i} \right) \left( \prod \bar{\pi}_i^{b_i} \right) \left( \prod q_i^{c_i} \right) \left( \prod \rho_i^{d_i} \right) \left( \prod \bar{\rho}_i^{e_i} \right).$$

Then,

$$\begin{aligned} d &= (\omega x + 2y)(\bar{\omega}x + 2y) \\ &= \left( \prod p_i^{a_i+b_i} \right) \left( \prod q_i^{2c_i} \right) \left( \prod r_i^{d_i+e_i} \right). \end{aligned}$$

Since  $d$  is square-free,  $c_i$  must be 0 for each  $i$ . Also,  $a_i + b_i = d_i + e_i = 1$  for each  $i$ . So, there exist sets  $S \subseteq \{1, \dots, n\}$  and  $T \subseteq \{1, \dots, l\}$  such that

$$\omega x + 2y = \left( \prod_{i \in S} \pi_i \right) \left( \prod_{i \notin S} \bar{\pi}_i \right) \left( \prod_{i \in T} \rho_i \right) \left( \prod_{i \notin T} \bar{\rho}_i \right)$$

Conversely, it is easy to check that if this product is in  $\omega + 2\mathbb{Z}[\omega]$ , then it can be expressed as  $\omega x + 2y$ , and  $(\omega x + 2y)(\bar{\omega}x + 2y) = d$ .

By Proposition 3.6,  $a_d$  is odd iff  $3x^2 + 2xy + 4y^2 = d$  has an odd number of solutions with  $x > 0$ . Thus, to determine if  $a_d$  is odd, we need to count solutions to  $3x^2 + 2xy + 4y^2 = d$ . From what we have shown so far, it suffices to count the number of products

$$\left( \prod_{i \in S} \pi_i \right) \left( \prod_{i \notin S} \bar{\pi}_i \right) \left( \prod_{i \in T} \rho_i \right) \left( \prod_{i \notin T} \bar{\rho}_i \right)$$

which lie in  $\omega + 2\mathbb{Z}[\omega]$ . Observe that, for any  $T \subseteq \{1, \dots, l\}$ ,

$$\left( \prod_{i \in T} \rho_i \right) \left( \prod_{i \notin T} \bar{\rho}_i \right) \in 1 + 2\mathbb{Z}[\omega]$$

because  $\rho_i \in 1 + 2\mathbb{Z}[\omega]$ . Also, there are  $2^l$  choices of  $T$ . On the other hand,

$$\left( \prod_{i \in S} \pi_i \right) \left( \prod_{i \notin S} \bar{\pi}_i \right) \in \omega^{|S|} \bar{\omega}^{n-|S|} + 2\mathbb{Z}[\omega]$$

so

$$\left( \prod_{i \in S} \pi_i \right) \left( \prod_{i \notin S} \overline{\pi_i} \right) \in \omega + 2\mathbb{Z}[\omega]$$

iff  $(|S|, n - |S|) \equiv (0, 2), (1, 0), (2, 1) \pmod{3}$ . The number of  $S$  such that this occurs is

$$f(n) = \begin{cases} \binom{n}{0} + \binom{n}{3} + \cdots + \binom{n}{n-2}, & n \equiv 2 \pmod{3} \\ \binom{n}{1} + \binom{n}{4} + \cdots + \binom{n}{n-1}, & n \equiv 1 \pmod{3} \\ \binom{n}{2} + \binom{n}{5} + \cdots + \binom{n}{n-1}, & n \equiv 0 \pmod{3} \end{cases}$$

Then, since  $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$ ,  $f(n+1) = 2^n - f(n)$  for every  $n$ . In particular, since  $f(1)$  is odd,  $f(n)$  is odd for all  $n$ .

So, the number of solutions to  $3x^2 + 2xy + 4y^2 = d$  with  $x > 0$  is  $2^l f(n)$ . Then,  $a_d$  is odd iff  $l = 0$ ; equivalently,  $a_d$  is odd iff  $d$  is a product of primes, each of which splits into two primes over  $K$ .  $\square$

**Corollary 3.11.** *If each prime factor of  $d$  splits into two primes over  $K$ , then the conjectured order of  $\text{III}(E_{-d}/\mathbb{Q})$  is odd.*

**Proof.** If each prime factor of  $d$  splits into two primes over  $K$ , then  $a_d$  is odd by Proposition 3.10. Then, the corollary follows immediately from the fact that the conjectured order of  $\text{III}(E_{-d}/\mathbb{Q})$  is odd iff

$$\frac{a_d^2}{\prod_{p|\Delta(E_{-d})} c_p}$$

is odd.  $\square$

## 4 Descent

In the previous section, we used the Birch-Swinnerton Dyer Conjectures to find  $\#\text{III}(E_{-p}/\mathbb{Q})[2]$  in certain cases. In this section, we will use the method of 2-descent to prove these results without using the Birch-Swinnerton Dyer Conjectures.

### 4.1 $y^2 = x^3 - d^2x$

Let  $E_d : y^2 = x^3 - d^2x$ . We will only consider the case when  $d$  is an odd prime. We showed in section 3.1 that, if  $d \equiv 5, 7 \pmod{8}$ , then  $L(E_d, 1) = 0$ . Assuming the truth of BSD I, this implies that  $E_d$  has positive rank. Using the method of complete 2-descent described in [12], we will reprove Proposition 3.2 without using BSD II.

**Proposition 4.1.** *If  $p$  is an odd prime and  $E_p$  has rank 0, then*

$$\text{III}(E_p/\mathbb{Q})[2] \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & p \equiv 1 \pmod{8} \\ 0, & p \equiv 3 \pmod{8} \end{cases}.$$

Let  $S = \{2, p, \infty\}$ , the set of all places of  $\mathbb{Q}$  including all archimedean places, all places dividing 2, and all places at which  $E_p$  has bad reduction. Let  $\mathbb{Q}(S, 2) = \{b \in \mathbb{Q}^*/\mathbb{Q}^{*2} : \text{ord}_v(b) \equiv 0 \pmod{2} \text{ for all } v \notin S\}$ . Then,  $\{\pm 1, \pm 2, \pm p, \pm 2p\}$  is a set of representatives of  $\mathbb{Q}(S, 2)$ , and we will identify this with  $\mathbb{Q}(S, 2)$ . By [12, Example X.4.5.1], we may identify  $S_2(E/\mathbb{Q})$  with a subgroup of  $\mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ . For any pair  $(b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$ , let  $C$  be the curve in  $\mathbb{P}^3$  given by the equations

$$b_1 z_1^2 - b_2 z_2^2 = p z_0^2 \quad (4.9)$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = -p z_0^2 \quad (4.10)$$

Then,  $(b_1, b_2) \in S_2(E_p/\mathbb{Q})$  iff  $C(\mathbb{Q}_v) \neq \emptyset$  for every  $v \in S$ .

If  $b_1 < 0$  and  $b_2 > 0$ , then  $b_1 z_1^2 - b_2 z_2^2 < 0$ , so equation (4.9) has no solutions, and  $(b_1, b_2) \notin S_2(E_p/\mathbb{Q})$ . Similarly, if  $b_1 > 0$  and  $b_2 < 0$ , then  $b_1 z_1^2 - b_1 b_2 z_3^2 > 0$ , so equation (4.10) has no solutions, and  $(b_1, b_2) \notin S_2(E_p/\mathbb{Q})$ .

By [12, Proposition X.1.4], there is an injective homomorphism  $E_p(\mathbb{Q})/2E_p(\mathbb{Q}) \rightarrow \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$  defined by

$$P = (x, y) \mapsto \begin{cases} (x, x - p), & x \neq 0, p \\ (-1, -p), & x = 0 \\ (p, 2), & x = p \\ (1, 1), & P = O \end{cases}$$

and the image of this map gives points in  $S_2(E_p/\mathbb{Q})$ . In particular,  $O \mapsto (1, 1)$ ,  $(p, 0) \mapsto (p, 2)$ ,  $(-p, 0) \mapsto (-p, -2p)$ , and  $(0, 0) \mapsto (-1, -p)$ , so  $(1, 1)$ ,  $(p, 2)$ ,  $(-p, -2p)$ ,  $(-1, -p) \in S_2(E_p/\mathbb{Q})$ .

Now, consider the pair  $(b_1, b_2) = (p, 2p)$ . Then, the homogeneous space  $C$  is described by the equations  $p z_1^2 - 2p z_2^2 = p z_0^2$  and  $p z_1^2 - 2p^2 z_3^2 = -p z_0^2$ . These can be simplified to

$$z_1^2 - 2z_2^2 = z_0^2 \quad (4.11)$$

$$z_1^2 - 2p z_3^2 = -z_0^2 \quad (4.12)$$

If  $C(\mathbb{Q}_p) \neq \emptyset$ , then equation (4.12) has a solution, and  $z_1^2 \equiv -z_0^2 \pmod{p}$ . Therefore,  $-1$  is a square mod  $p$ , which implies that  $p \equiv 1 \pmod{8}$ . So, if  $p \equiv 3 \pmod{8}$ , then  $(p, 2p) \notin S_2(E_p/\mathbb{Q})$ .

Suppose that  $p \equiv 1 \pmod{8}$ . Then,  $-1$  is a square mod  $p$ , so there exists  $a$  such that  $a^2 \equiv -1 \pmod{8}$ . Then,  $z_0 = 1$ ,  $z_1 = a$ ,  $z_3 = 0$  is a solution to  $z_1^2 - 2p z_3^2 \equiv -z_0^2 \pmod{p}$ ; by Hensel's Lemma, this lifts to a solution  $(z_0, z_1, z_3) =$

$(1, A, 0) \in \mathbb{Q}_p^3$  of equation (4.12). Then, equation (4.11) becomes  $A^2 - 2z_2^2 = 1$ ; since  $A^2 \equiv -1 \pmod{p}$ , this simplifies to  $2z_2^2 \equiv -2 \pmod{p}$ , which has a solution  $z_2 \pmod{p}$  that lifts to a solution in  $\mathbb{Q}_p$ . Thus,  $C(\mathbb{Q}_p) \neq \emptyset$ .

Similarly, observe that we can find a solution  $(z_0, z_1, z_2, z_3) = (1, 1, 0, 1)$  to  $z_1^2 - 2z_2^2 \equiv z_0^2 \pmod{8}$  and  $z_1^2 - 2pz_3^2 \equiv -z_0^2 \pmod{8}$ . This lifts to a solution in  $\mathbb{Q}_2$ , so  $C(\mathbb{Q}_2) \neq \emptyset$ . Therefore,  $(p, 2p) \in S_2(E_p/\mathbb{Q})$  iff  $p \equiv 1 \pmod{8}$ .

Since  $S_2(E_p/\mathbb{Q})$  is a group and  $(1, 1), (p, 2), (-p, -2p), (-1, -p) \in S_2(E_p/\mathbb{Q})$ , we have that  $(1, p), (-1, -1), (-p, -2) \in S_2(E_p/\mathbb{Q})$  iff  $p \equiv 1 \pmod{8}$ . Similarly, we can check that  $(p, p) \in S_2(E/\mathbb{Q})$  iff  $p \equiv 1 \pmod{8}$ . This gives

$$S_2(E_p/\mathbb{Q}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & p \equiv 1 \pmod{8} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & p \equiv 3 \pmod{8} \end{cases} \quad (4.13)$$

Since  $E_p$  has rank 0,  $E_p(\mathbb{Q}) = E_p(\mathbb{Q})_{\text{tors}}$ . As we showed in section 3.1, the 2-part of  $E_p(\mathbb{Q})$  consists of the points of order 2 so is isomorphic to  $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . Then,  $E_p(\mathbb{Q})/2E_p(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$  as well. By [12, Theorem X.4.2], there is an exact sequence

$$0 \longrightarrow E_p(\mathbb{Q})/2E_p(\mathbb{Q}) \xrightarrow{\phi} S_2(E_p/\mathbb{Q}) \xrightarrow{\psi} \text{III}(E_p/\mathbb{Q})[2] \longrightarrow 0.$$

Then,  $\phi$  is injective, so  $\ker \psi = \text{im } \phi \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ . Also,  $\psi$  is surjective, so  $\text{III}(E_p/\mathbb{Q})[2]$  is isomorphic to  $S_2(E_p/\mathbb{Q})/\ker \psi$ . By equation (4.13),

$$\text{III}(E_p/\mathbb{Q})[2] \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, & p \equiv 1 \pmod{8} \\ 0, & p \equiv 3 \pmod{8} \end{cases}.$$

which completes the proof.  $\square$

In particular,  $\#\text{III}(E_p/\mathbb{Q})$  is odd iff  $p \equiv 3 \pmod{8}$ .

In [7, Theorem 2], Razar shows a similar result. He proves that if  $p$  is a prime such that either  $p \equiv 9 \pmod{16}$  and 2 is a quartic residue of  $p$ , or  $p \equiv 1 \pmod{16}$  and 2 is not a quartic residue of  $p$ , then the 2-component of  $\text{III}(E_p/\mathbb{Q})$  has order 4.

## 4.2 $y^2 = x^3 - 4dx^2 + 16d^3$

The method of complete 2-descent we used in the previous section will not work for the family  $y^2 = x^3 - 4dx^2 + 16d^3$  because  $x^3 - 4dx^2 + 16d^3$  does not have any rational roots. So, we will use the method described in [5]. Recall that  $K$  is the field obtained by adjoining the roots of  $x^3 - 4x^2 + 16$  to  $\mathbb{Q}$ ; we will only consider the case where  $d$  is an odd prime which splits into 2 primes over  $K$ . For convenience, we will use slightly different notation. Let  $p$  be an odd

prime which splits into 2 primes over  $K$ , and let  $f(x) = x^3 + 4px^2 - 16p^3$ . Let  $E : y^2 = f(x)$ ; this is the twist of our original curve by  $-p$ . Let  $A = \mathbb{Q}[x]/f(x)$ .

Let  $S = \{2, 11, p, \infty\}$ , the set of places of  $\mathbb{Q}$  which lie above 2 and the primes dividing the conductor of  $E$ . Let  $A(S, 2)$  be the set  $\{b \in A^*/A^{*2} : b > 0, \text{ord}_v(b) \equiv 0 \pmod{2} \text{ for all } v \notin S\}$ .

Using PARI, we can check that  $A$  has class number 1. Moreover, (2) factors over  $A$  as  $\mathfrak{p}_2^3$  for some prime ideal  $\mathfrak{p}_2$ , and (11) factors as  $\mathfrak{p}_{11}\mathfrak{p}_{11}^{*2}$  for some primes  $\mathfrak{p}_{11}, \mathfrak{p}_{11}^*$ .

Recall that  $p$  splits into 2 primes over  $K$ ; that is,  $p = \mathfrak{r}_1\mathfrak{r}_2$  for some primes  $\mathfrak{r}_1, \mathfrak{r}_2$  of  $K$ . If  $\mathfrak{p}$  is a prime of some subfield  $L$  of  $K$  which divides  $p$ , let  $f(\mathfrak{r}_i/\mathfrak{p})$  denote the degree of the residue class field extension  $\mathcal{O}_K/\mathfrak{r}_i$  over  $\mathcal{O}_L/\mathfrak{p}$  (we will take  $L$  to be either  $\mathbb{Q}$  or  $A$ ). Then, by [6, I.§7, Corollary 2],  $f(\mathfrak{r}_1/p) = f(\mathfrak{r}_2/p)$  and [6, I.§7, Proposition 21] shows that  $f(\mathfrak{r}_1/p) + f(\mathfrak{r}_2/p) = [K : \mathbb{Q}] = 6$ , so  $f(\mathfrak{r}_1/p) = f(\mathfrak{r}_2/p) = 3$ .

Since  $p$  splits into 2 primes over  $K$ ,  $p$  splits into at most 2 primes over  $A$ , so either  $p = \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}$  for primes  $\mathfrak{q}_i$  and natural numbers  $e_i$ , or  $p = \mathfrak{q}^e$  for some prime  $\mathfrak{q}$  and natural number  $e$ . Assume that  $p = \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}$ . By [6, I.§7, Proposition 20], since  $p = \mathfrak{r}_1\mathfrak{r}_2$ ,  $e_i|1$ , so  $e_i = 1$ . That is,  $p = \mathfrak{q}_1\mathfrak{q}_2$ . Since  $f(\mathfrak{r}_i/p) = 3$  for  $i = 1, 2$ ,  $f(\mathfrak{q}_i/p)$  divides 3 by [6, I.§7, Proposition 20]. Therefore,  $f(\mathfrak{q}_i/p)$  is either 1 or 3. However,  $f(\mathfrak{q}_1/p) + f(\mathfrak{q}_2/p) = [A : \mathbb{Q}] = 3$ , which is impossible since  $f(\mathfrak{q}_i/p)$  is either 1 or 3. So, it must be the case that  $p = \mathfrak{q}^e$  for some prime  $\mathfrak{q}$  and natural number  $e$ . Again,  $e|1$ , so  $e = 1$ , and  $p$  must be prime over  $A$ .

Since  $A$  has class number 1,  $\mathfrak{p}_2$  has a generator  $\pi_2$ , and we can choose  $\pi_2$  so that it is positive at the real embedding of  $A$  into  $\mathbb{R}$ . Similarly,  $\mathfrak{p}_{11}, \mathfrak{p}_{11}^*$ , and  $p$  have generators  $\pi_{11}, \pi_{11}^*$ , and  $\pi_p$  that are positive at the real embedding of  $A$  into  $\mathbb{R}$ . Using PARI, we find that  $u = \frac{x}{2p} + 1$  is a fundamental unit of  $A$ . Then,  $A(S, 2) = \langle \pm 1, u, \pi_2, \pi_{11}, \pi_{11}^*, \pi_p \rangle$ .

Consider the norm map  $N$  as a map from  $A(S, 2)$  to  $\mathbb{Q}^*/\mathbb{Q}^{*2}$ . Let  $U$  be the kernel of this map. Observe that  $N(\mathfrak{p}_2) = \mathfrak{p}_2^3 = (2)$ , so  $N(\pi_2)$  is a generator of (2). Since  $A$  has one real embedding and 2 conjugate complex embeddings,  $N(\pi_2)$  has the same sign as  $\pi_2$ . That is,  $N(\pi_2)$  is positive, so  $N(\pi_2) = 2$ . Similarly, the norm of  $\pi_{11}$  and  $\pi_{11}^*$  must be 11. The norm of  $\pi_p$  is  $p^3$ , and the norm of  $u$  is 1. Any  $\alpha \in A(S, 2)$  can be expressed as  $(-1)^a u^b \pi_2^c \pi_{11}^d \pi_{11}^{*e} \pi_p^f$ . Then,  $N(\alpha) = (-1)^a 2^c 11^{d+e} p^{3f}$ . By the definition of  $U$ ,  $\alpha \in U$  iff the norm of  $\alpha$  is a square, which occurs iff  $a, c, d + e, f$  are even. So,  $U = \langle u, \pi_{11}\pi_{11}^* \rangle$ .

By [5], there exist injective homomorphisms  $F : E(\mathbb{Q})/2E(\mathbb{Q}) \rightarrow U$  and  $F_\ell : E(\mathbb{Q}_\ell)/2E(\mathbb{Q}_\ell) \rightarrow A_\ell^*/A_\ell^{*2}$  such that  $F(s, t) = s - x$  if  $t \neq 0$  and  $F_\ell(s, t) = s - x$  if  $t \neq 0$ . Let  $\beta_\ell : U \rightarrow A_\ell^*/A_\ell^{*2}$  be the inclusion map. By [9, §3],

$$S_2(E/\mathbb{Q}) \cong \bigcap_{\ell \in S} \beta_\ell^{-1}(F_\ell(E(\mathbb{Q}_\ell)/2E(\mathbb{Q}_\ell))).$$

In particular,  $U$  has a subgroup isomorphic to  $S_2(E/\mathbb{Q})$ .

By [12, Proposition 6.3],  $E(\mathbb{Q}_\ell)$  contains a subgroup of finite index which is isomorphic to  $\mathbb{Z}_\ell$ . That is,  $E(\mathbb{Q}_\ell) \cong \mathbb{Z}_\ell \times E(\mathbb{Q}_\ell)_{\text{tors}}$ .

We will first consider the case  $\ell = 11$ .

**Proposition 4.2.**  $\beta_{11}^{-1}(F_{11}(E(\mathbb{Q}_{11})/2E(\mathbb{Q}_{11}))) \subseteq \langle u \rangle$ .

**Proof.** Observe that  $f(x) \equiv (x - 5p)(x - p)^2 \pmod{11}$ . By Hensel's Lemma, since  $f'(5p) \not\equiv 0 \pmod{11}$ ,  $(5p, 0)$  lifts to a point  $(e_1, 0)$  in  $E(\mathbb{Z}_{11})$  with  $e_1 \in 5p + 11\mathbb{Z}_{11}$ . Then, we can write  $f(x)$  as  $(x - e_1)f_0(x)$  for some  $f_0(x) \in \mathbb{Q}_{11}[x]$ . As we noted before,  $E(\mathbb{Q}_{11}) \cong \mathbb{Z}_{11} \times E(\mathbb{Q}_{11})_{\text{tors}}$ ; therefore,  $E(\mathbb{Q}_{11})/2E(\mathbb{Q}_{11}) \cong E(\mathbb{Q}_{11})_{\text{tors}}/2E(\mathbb{Q}_{11})_{\text{tors}}$ .

We can check that  $f(x) \equiv (x - 60p)(x^2 + 64px + 89p^2) \pmod{121}$ , and  $x^2 + 64px + 89p^2$  has no roots mod 121 because  $x^2 + 64x + 89$  has no roots mod 121. So,  $f(x)$  has only one root in  $\mathbb{Q}_{11}$ , and  $E(\mathbb{Q}_{11})$  has only one point of order 2. Then,  $E(\mathbb{Q}_{11})_{\text{tors}}/2E(\mathbb{Q}_{11})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}$ . Using the duplication formula, it is easy to check that there is a point  $(e, y)$  of order 4 in  $E(\mathbb{Q}_{11})$  with  $e \in 9p + 11\mathbb{Z}_{11}$ . Using the duplication formula again, it is easy to verify that there is no point  $(x_0, y_0)$  such that  $2(x_0, y_0) = (e, y)$ , so  $(e, y) \notin 2E(\mathbb{Q}_{11})$ . This implies that  $(e, y)$  is non-trivial in  $E(\mathbb{Q}_{11})/2E(\mathbb{Q}_{11})$ ; then, since  $E(\mathbb{Q}_{11})/2E(\mathbb{Q}_{11})$  is cyclic of order 2, it must be generated by  $(e, y)$ .

Recall that the map  $F_\ell : E(\mathbb{Q}_\ell)/2E(\mathbb{Q}_\ell) \rightarrow A_\ell^*/A_\ell^{*2}$  has  $F_\ell(s, t) = s - x$  when  $t \neq 0$ . In particular, since  $(e, y)$  is not a point of order 2,  $y \neq 0$ , and  $F_{11}(e, y) = e - x$ . Observe that  $A_{11} \cong \mathbb{Q}_{11}[x]/f(x) \cong \mathbb{Q}_{11}[x]/(x - e_1) \oplus \mathbb{Q}_{11}(x)/f_0(x)$ . We may identify  $\mathbb{Q}_{11}[x]/(x - e_1)$  with  $\mathbb{Q}_{11}$  and  $\mathbb{Q}_{11}(x)/f_0(x)$  with a quadratic extension  $L$  of  $\mathbb{Q}_{11}$ . So, we may identify points of  $A_{11}$  with ordered pairs in  $\mathbb{Q}_{11} \oplus L$ . We will focus on the projection of points of  $A_{11} \cong \mathbb{Q}_{11} \oplus L$  to  $\mathbb{Q}_{11}$ .

The isomorphism  $\mathbb{Q}_{11}[x]/(x - e_1) \cong \mathbb{Q}_{11}$  maps  $x$  to  $e_1$ , so  $e - x \mapsto e - e_1 \in 4p + 11\mathbb{Z}_{11}$ . Since  $p$  is a square mod 11,  $e - e_1 \in \mathbb{Q}_{11}^{*2}$ , and  $e - e_1 = 1$  in  $\mathbb{Q}_{11}^*/\mathbb{Q}_{11}^{*2}$ . So, the image of  $F_{11}(e, y)$  in  $\mathbb{Q}_{11}^*/\mathbb{Q}_{11}^{*2}$  is 1.

Recall that  $u = \frac{x}{2p} + 1$ . Then, the image of  $\beta_{11}(u)$  in  $\mathbb{Q}_{11}$  is  $\frac{e_1}{2p} + 1 \in 9 + 11\mathbb{Z}_{11}$ . So, the image of  $\beta_{11}(u)$  in  $\mathbb{Q}_{11}^*/\mathbb{Q}_{11}^{*2}$  is 1.

Since  $\pi_{11}\pi_{11}^{*2} = 11$  is a prime in  $\mathbb{Q}[x]/(x - e_1)$ , it must be the case that  $\pi_{11}$  is prime in  $\mathbb{Q}_{11}[x]/(x - e_1)$  while  $\pi_{11}^*$  is a unit. Therefore,  $\pi_{11}\pi_{11}^*$  is not a square, and the image of  $\beta_{11}(\pi_{11}\pi_{11}^*)$  in  $\mathbb{Q}_{11}$  is not a square. Then, the image of  $\beta_{11}(\pi_{11}\pi_{11}^*)$  in  $\mathbb{Q}_{11}^*/\mathbb{Q}_{11}^{*2}$  is not 1. In particular, the image of  $\beta_{11}(\pi_{11}\pi_{11}^*)$  in  $A_{11}^*/A_{11}^{*2} \cong \mathbb{Q}_{11}^*/\mathbb{Q}_{11}^{*2} \oplus L^*/L^{*2}$  is neither the identity element nor the image of  $(e, y)$  under  $F_{11}$ . Thus,  $\pi_{11}\pi_{11}^* \notin \beta_{11}^{-1}(F_{11}(E(\mathbb{Q}_{11})/2E(\mathbb{Q}_{11})))$ .

Since the image of  $\beta_{11}(u)$  in  $\mathbb{Q}_{11}^*/\mathbb{Q}_{11}^{*2}$  is 1 while the image of  $\beta_{11}(\pi_{11}\pi_{11}^*)$  is not 1, the image of  $\beta_{11}(u\pi_{11}\pi_{11}^*)$  in  $\mathbb{Q}_{11}^*/\mathbb{Q}_{11}^{*2}$  must not be 1. Therefore,  $u\pi_{11}\pi_{11}^* \notin \beta_{11}^{-1}(F_{11}(E(\mathbb{Q}_{11})/2E(\mathbb{Q}_{11})))$ .

So,  $\beta_{11}^{-1}(F_{11}(E(\mathbb{Q}_{11})/2E(\mathbb{Q}_{11}))) \subseteq \langle u \rangle$ . □

To show that  $S_2(E/\mathbb{Q})$  is trivial, it suffices to show that  $u \notin S_2(E/\mathbb{Q})$ . First, we need the following lemma:

**Lemma 4.3.** *Suppose  $a, b, c, d$  are odd integers with  $a + b + c + d \equiv 2 \pmod{4}$ . Then, the polynomial  $ax^6 + bx^4 + cx^2 + d$  does not factor as  $(a_3x^3 + a_2x^2 + a_1x + a_0)(b_3x^3 + b_2x^2 + b_1x + b_0) \pmod{8}$ .*

**Proof.** Assume  $ax^6 + bx^4 + cx^2 + d = (a_3x^3 + a_2x^2 + a_1x + a_0)(b_3x^3 + b_2x^2 + b_1x + b_0) \pmod{8}$ . Then, mod 8,

$$\begin{aligned} a &\equiv a_3b_3 \\ 0 &\equiv a_3b_2 + a_2b_3 \\ b &\equiv a_3b_1 + a_2b_2 + a_1b_3 \\ 0 &\equiv a_3b_0 + a_2b_1 + a_1b_2 + a_0b_3 \\ c &\equiv a_2b_0 + a_1b_1 + a_0b_2 \\ 0 &\equiv a_1b_0 + a_0b_1 \\ d &\equiv a_0b_0 \end{aligned}$$

In particular, since  $a_3b_3 \equiv a$ ,  $a_0b_0 \equiv d \pmod{8}$ , and both  $a$  and  $d$  are odd,  $a_0, b_0, a_3, b_3$  must all be odd. Then,  $a_3b_2 + a_2b_3 \equiv 0 \pmod{8}$  implies that  $a_2 \equiv b_2 \pmod{2}$ . Since  $b \equiv a_3b_1 + a_2b_2 + a_1b_3 \pmod{8}$  and  $b$  is odd,  $a_2b_2$  must be odd, so  $a_2$  and  $b_2$  are odd as well. Since  $a_2 + b_0 + a_1b_1 + a_0b_2 \equiv c \pmod{8}$  and  $c$  is odd,  $a_1$  and  $b_1$  must be odd as well.

Observe that  $a + b + c + d \equiv (a_0 + a_2)(b_0 + b_2) + (a_1 + a_3)(b_1 + b_3) \equiv 0 \pmod{4}$  since each  $a_i$  and  $b_i$  is odd. This is a contradiction since  $a + b + c + d \equiv 2 \pmod{4}$ , so  $ax^6 + bx^4 + cx^2 + d$  is not the product of two degree-3 polynomials mod 8. □

**Proposition 4.4.**  $u \notin \beta_2^{-1}(F_2(E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)))$ .

**Proof.** It is easy to check that  $x^3 + 4x^2 - 16$  has no solutions mod 32, so  $x^3 + 4px^2 - 16p^3$  has no solutions mod 32 either. Therefore,  $E(\mathbb{Q}_2)$  has no points of order 2, so  $E(\mathbb{Q}_2)_{\text{tors}}$  has odd order. Recall that  $E(\mathbb{Q}_2) \cong \mathbb{Z}_2 \times E(\mathbb{Q}_2)_{\text{tors}}$ , so  $E(\mathbb{Q}_2)/2E(\mathbb{Q}_2) \cong \mathbb{Z}/2\mathbb{Z}$ . To find a generator of  $E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)$ , it suffices to find a point  $P \in E(\mathbb{Q}_2)$  such that  $F_2(P) \notin A_2^{*2}$ . Observe that  $f(-3) = (-3)^3 + 4p(-3)^2 - 16p^3 \equiv -27 + 36p - 16p^3 \equiv 5 + 4p \equiv 1 \pmod{8}$  because  $p$  is odd. By Hensel's Lemma,  $(-3, 1)$  lifts to a point  $P = (-3, y)$  in  $E(\mathbb{Q}_2)$ . Then,  $F_2(P) = -3 - x$ .

Let  $e_1, e_2, e_3$  be the roots of  $x^3 + 4x^2 - 16$  over an algebraic closure of  $\mathbb{Q}_2$ . Then,  $f(x) = (x - pe_1)(x - pe_2)(x - pe_3)$ , and  $A_2 \cong \mathbb{Q}_2(e_1)$ . Let  $L = \mathbb{Q}_2(e_1)$ .

First, we will show that  $-3 - x \notin A_2^{*2}$ . Equivalently, we will show that  $-3 - e_1 \notin L^{*2}$ . Assume that  $-3 - e_1 \in L^{*2}$ . Then, there exists  $\theta \in L^*$  such that  $\theta^2 = -3 - e_1$ . Let  $g(t) = [t^2 - (-3 - e_1)][t^2 - (-3 - e_2)][t^3 - (-3 - e_2)] = t^6 + 5t^4 + 3t^2 + 7$ .

Then,  $g(\theta) = (e_1 - e_1)(e_1 - e_2)(e_1 - e_3) = 0$ . Since  $\theta \in L^*$  and  $[L : \mathbb{Q}_2] = 3$ , the minimal polynomial of  $\theta$  over  $\mathbb{Q}_2$  has degree at most 3. We can check using PARI that  $t^6 + 5t^4 + 3t^2 + 7$  is irreducible over  $\mathbb{Q}_2$ , so  $g$  is the minimal polynomial of  $\theta$ , a contradiction. So,  $-3 - x \notin A_2^{*2}$ . Therefore,  $F_2(P)$  is not the trivial element in  $A^*/A^{*2}$ , and  $P$  is not trivial in  $E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)$ .

Now, to show that  $u \notin \beta_2^{-1}(F_2(E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)))$ , we simply need to check that  $\beta_2(u) \neq 1, -3 - x$  in  $A_2^*/A_2^{*2}$ . First, we will show that  $\beta_2(u) \neq -3 - x$ . It suffices to show that  $(-3 - x)\beta_2(u) \notin A_2^{*2}$ . Assume  $(-3 - x)u \in A_2^{*2}$ . Since  $u = \frac{x}{2p} + 1$ ,

$$(-3 - x)\beta_2(u) = -\frac{1}{2p}[x^2 + (2p + 3)x + 6].$$

Then,

$$-\frac{1}{2p}[e_1^2 + (2p + 3)e_1 + 6] \in L^{*2},$$

so there exists  $\theta \in L^*$  such that

$$\theta^2 = -\frac{1}{2p}[e_1^2 + (2p + 3)e_1 + 6].$$

Let  $\alpha = 2p + 3$ . Observe that

$$\begin{aligned} 0 &= (e_1 - e_1)[e_1 + (\alpha + e_1)](e_1 - e_2)[e_1 + (\alpha + e_2)](e_1 - e_3)[e_1 + (\alpha + e_3)] \\ &= [e_1^2 + \alpha e_1 - e_1(\alpha + e_1)][e_1^2 + \alpha e_1 - e_2(\alpha + e_2)][e_1^2 + \alpha e_1 - e_3(\alpha + e_3)] \\ &= [-2\theta^2 - 6 - e_1(\alpha + e_1)][-2\theta^2 - 6 - e_2(\alpha + e_2)][-2\theta^2 - 6 - e_3(\alpha + e_3)] \\ &= -8[p^3\theta^6 + (11p^2 - 4p^3)\theta^4 + (35p - 48p^2)\theta^2 + (16p^3 + 40p^2 - 96p + 47)] \end{aligned}$$

Since  $\theta \in L^*$  and  $[L : \mathbb{Q}_2] = 3$ , the minimal polynomial of  $\theta$  over  $\mathbb{Q}_2$  has degree 1 or 3;  $\theta \notin \mathbb{Q}_2$ , so the minimal polynomial of  $\theta$  over  $\mathbb{Q}_2$  has degree 3. In particular,

$$p^3x^6 + (11p^2 - 4p^3)x^4 + (35p - 48p^2)x^2 + (16p^3 + 40p^2 - 96p + 47) \quad (4.14)$$

can be expressed as the product of two polynomials, each of degree 3, in  $\mathbb{Q}_2[x]$ . Since  $p$  is odd, the polynomial in (4.14) has odd coefficients, and the sum of the coefficients is congruent to 2 (mod 4), a contradiction to Lemma 4.3. So,  $\theta \notin L^*$ , and  $-3 - x \neq \beta_2(u)$  in  $A_2^*/A_2^{*2}$ .

Now, we will show that  $\beta_2(u) \neq 1$  in  $A_2^*/A_2^{*2}$ . Equivalently, we will show that  $\beta_2(u) \notin A_2^{*2}$ . Assume that  $\beta_2(u) \in A_2^{*2}$ . Then, there exists  $\theta \in L^*$  such that

$$\theta^2 = \frac{e_1}{2p} + 1.$$

Observe that

$$\begin{aligned} 0 &= (e_1 - e_1)(e_1 - e_2)(e_1 - e_3) \\ &= [2p(\theta^2 - 1) - e_1][2p(\theta^2 - 1) - e_2][2p(\theta^2 - 1) - e_3] \\ &= 8[p^3\theta^6 + (2p^2 - 3p^3)\theta^4 + (3p^3 - 4p^2)\theta^2 + (2p^2 - p^3 - 2)] \end{aligned}$$

Since  $\theta \in L^*$  and  $[L : \mathbb{Q}_2] = 3$ , the minimal polynomial of  $\theta$  over  $\mathbb{Q}_2$  has degree 1 or 3;  $\theta \notin \mathbb{Q}_2$ , so the minimal polynomial of  $\theta$  over  $\mathbb{Q}_2$  has degree 3. In particular,

$$p^3x^6 + (2p^2 - 3p^3)x^4 + (3p^3 - 4p^2)x^2 + (2p^2 - p^3 - 2) \quad (4.15)$$

can be expressed as the product of two polynomials, each of degree 3, in  $\mathbb{Q}_2[x]$ . Since  $p$  is odd, the polynomial in (4.15) has odd coefficients, and the sum of the coefficients is congruent to 2 (mod 4), a contradiction to Lemma 4.3. So,  $\theta \notin L^*$ , and  $\beta_2(u) \neq 1$  in  $A_2^*/A_2^{*2}$ .

Therefore,  $u \notin \beta_2^{-1}(F_2(E(\mathbb{Q}_2)/2E(\mathbb{Q}_2)))$ . □

The previous two propositions show that  $S_2(E/\mathbb{Q})$  is trivial. By [12, Theorem X.4.2], there is an exact sequence

$$0 \rightarrow E(\mathbb{Q})/2E(\mathbb{Q}) \rightarrow S_2(E/\mathbb{Q}) \rightarrow \text{III}(E/\mathbb{Q})[2] \rightarrow 0.$$

In particular, since  $S_2(E/\mathbb{Q})$  is trivial,  $\text{III}(E/\mathbb{Q})[2]$  must be trivial as well. So,  $\#\text{III}(E/\mathbb{Q})$  must be odd.

**Corollary 4.5.** *Let  $p$  be an odd prime which splits into two primes over  $K$ . Then, the conjectured order and the real order of  $\text{III}(E_{-p}/\mathbb{Q})[2]$  are equal.*

**Proof.** In this section, we showed that the actual order of  $\text{III}(E_{-p}/\mathbb{Q})[2]$  is 1. In Corollary 3.11, we showed that the conjectured order of  $\text{III}(E_{-p}/\mathbb{Q})[2]$  is also 1. □

## References

- [1] J. A. Antoniadis, M. Bungert, and G. Frey, *Properties of twists of elliptic curves*, J. Reine Angew. Math. **405** (1990), 1-28.
- [2] B. Birch, H. P. F. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. Reine Angew. Math. **218** (1965), 79-108.
- [3] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin, 1993.
- [4] C. Delaunay, *Heuristics on Tate-Shafarevitch Groups of Elliptic Curves defined over  $\mathbb{Q}$* .
- [5] Z. Djabri, E. F. Schaefer, and N. P. Smart, *Computing the  $p$ -Selmer Group of an Elliptic Curve*, Trans. Amer. Math. Soc. **352** (2000), no. 12, 5583–5597.
- [6] S. Lang, *Algebraic Number Theory*, Addison-Wesley, Reading, MA, 1970.

- [7] M. J. Razar, *A Relation Between the Two-Component of the the Tate-Safarevic Group and  $L(1)$  for Certain Elliptic Curves*, Amer. J. Math. **96** (1974), 127-144.
- [8] M. J. Razar, *The Non-Vanishing of  $L(1)$  for Certain Elliptic Curves with no First Descents*, Amer. J. Math. **96** (1974), 104-126.
- [9] E. F. Schaefer, *2-descent on the Jacobians of Hyperelliptic Curves*, J. Number Th. **51** (1995), 219-232.
- [10] G. Shimura, *On Modular Forms of Half Integral Weight*, Ann. of Math. **97** (1973), 440-481.
- [11] A. Silverberg, *Open Questions in Arithmetic Algebraic Geometry*, IAS / Park City Mathematics Series.
- [12] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics. **106**, Springer-Verlag, New York, 1986.
- [13] J. B. Tunnell, *A Classical Diophantine Problem and Modular Forms*, Invent. Math. **72** (1983), 323-334.