# 2-SELMER GROUPS, 2-CLASS GROUPS AND RATIONAL POINTS ON ELLIPTIC CURVES

CHAO LI

Abstract. Let $E : y^2 = F(x)$ be an elliptic curve over $\mathbb{Q}$ defined by a monic irreducible integral cubic polynomial $F(x)$ with negative square-free discriminant $-D$. We determine its 2-Selmer rank in terms of the 2-rank of the class group of the cubic field $L = \mathbb{Q}[x]/F(x)$.

When the 2-rank of the class group of $L$ is at most 1 and the root number of $E$ is $-1$, the Birch and Swinnerton-Dyer conjecture predicts that $E(\mathbb{Q})$ should have rank 1. We construct a canonical point in $E(\mathbb{Q})$ using a new Heegner point construction. We naturally conjecture it to be of infinite order. We verify this conjecture explicitly for the case $D = 11$, and propose an approach towards the general case based on a mod 2 congruence between elliptic curves and Artin representations.

## Contents



## 1. Introduction

1.1. **$p$-Selmer rank one conjecture.** Given an elliptic curve $E$ defined over $\mathbb{Q}$, the rational points $E(\mathbb{Q})$ form a finitely generated abelian group by the Mordell–Weil theorem. It is a central question in number theory to understand the rank of $E(\mathbb{Q})$, known as the *algebraic rank*

$$r_{\mathrm{alg}}(E/\mathbb{Q}) := \mathrm{rk}\, E(\mathbb{Q}).$$

Let $p$ be a prime number. Recall that we have the *p-descent* exact sequence (see [Sil09, X.4])

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \mathrm{Sel}_p(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[p] \to 0, \tag{1.1}$$

where $\mathrm{Sel}_p(E/\mathbb{Q})$ is the *p-Selmer group* and $Ш(E/\mathbb{Q})$ is the *Tate–Shafarevich group.* We define the *p-Selmer rank* of $E/\mathbb{Q}$ to be

$$s_p(E/\mathbb{Q}) := \dim_{\mathbb{F}_p} \mathrm{Sel}_p(E/\mathbb{Q}) - \dim_{\mathbb{F}_p} E(\mathbb{Q})[p].$$

---

2010 *Mathematics Subject Classification.* 11G05 (primary), 14G35, 11G40, 11F33 (secondary).
*Key words and phrases.* elliptic curves, Selmer groups, class groups, Heegner points.

It follows from the $p$-descent sequence (1.1) that

$$r_{\mathrm{alg}}(E/\mathbb{Q}) = s_p(E/\mathbb{Q}) - \dim_{\mathbb{F}_p} Ш(E/\mathbb{Q})[p].$$

Due to the Cassels–Tate pairing, the finiteness of the $p$-primary part $Ш(E/\mathbb{Q})[p^\infty]$ would imply that $Ш(E/\mathbb{Q})[p]$ has even $\mathbb{F}_p$-dimension, hence $s_p(E/\mathbb{Q})$ and $r_{\mathrm{alg}}(E/\mathbb{Q})$ have the same parity. In particular, the finiteness of $Ш(E/\mathbb{Q})[p^\infty]$ would imply the following conjecture, which we call the *p-Selmer rank one conjecture*.

**Conjecture 1.2.** *If $s_p(E/\mathbb{Q}) = 1$, then $r_{\mathrm{alg}}(E/\mathbb{Q}) = 1$.*

Conjecture 1.2, despite looking simple, was only recently proved for $p \geq 5$ under certain assumptions ([Zha14], [Ski14], [SZ14], [Wan14], [CW15], [Ven16]). These known cases of Conjecture 1.2 played a key role in the recent breakthrough of Bhargava–Skinner–Zhang ([BSZ14]) that a majority of elliptic curves over $\mathbb{Q}$ satisfy the rank part of the Birch and Swinnerton-Dyer conjecture.

On the other hand, very little about Conjecture 1.2 is known for $p = 2$, though the 2-Selmer group is the easiest to compute in practice and provides as of present the best tool for computing $E(\mathbb{Q})$. More recently there has also been growing interest in studying the 2-Selmer group and its variation in families (e.g., Klagsbrun–Mazur–Rubin [KMR13],[KMR14]), in view of its connection with Hilbert's tenth problem ([MR10]) and Goldfeld's conjecture ([KL16], [Smi17]).

The theme of this article is explore Conjecture 1.2 for a large class of elliptic curves. We now turn to our main results.

1.3. **2-Selmer groups and 2-class groups.** Let $F(x) \in \mathbb{Z}[x]$ be an irreducible monic cubic polynomial with negative and square-free discriminant $-D$. Let $E$ be given by the Weierstrass equation $y^2 = F(x)$. Our first main result is to determine the 2-Selmer rank $s_2(E/\mathbb{Q})$ in terms of the 2-part of the ideal class group of the cubic field $L = \mathbb{Q}(x)/F(x)$ and the global root number $\varepsilon(E/\mathbb{Q})$ of $E/\mathbb{Q}$.

**Theorem 1.4** (Theorem 2.18)**.** *Let $\mathrm{Cl}(L)$ be the ideal class group of the cubic field $L = \mathbb{Q}[x]/F(x)$. Let $k = \dim_{\mathbb{F}_2} \mathrm{Cl}(L)[2]$ be its 2-rank. Then*

$$s_2(E/\mathbb{Q}) = k \text{ or } k+1,$$

*depending on whether the root number $\varepsilon(E/\mathbb{Q}) = (-1)^k$ or $(-1)^{k+1}$.*

1.5. **Heegner points on elliptic curves of conductor $4D$.** Theorem 1.4 has the following immediate consequence (applied to $k = 0$ or 1, only the upper bound on $s_2(E/\mathbb{Q})$ is needed).

**Corollary 1.6.** *Assume $\varepsilon(E/\mathbb{Q}) = -1$. If the 2-rank of $\mathrm{Cl}(L)$ is at most 1, then $s_2(E/\mathbb{Q}) = 1$. In this case, Conjecture 1.2 implies that $r_{\mathrm{alg}}(E/\mathbb{Q}) = 1$.*

This consequence naturally raises two challenges:

(1) to construct a rational point $P \in E(\mathbb{Q})$ when $\varepsilon(E/\mathbb{Q}) = -1$,
(2) to verify the constructed point $P$ is of infinite order when the 2-rank of $\mathrm{Cl}(L)$ is at most 1.

In §3 we complete (1) under an additional assumption that $E$ has Kodaira type IV at 2. This assumption allows us to pin down the conductor of $E$ to be the minimal $N = 4D$, and interestingly also forces the root number $\varepsilon(E/\mathbb{Q}(i))$ to be $-1$. In this case $E$ admits a parametrization by a Shimura curve $X$ associated to the quaternion order of reduced discriminant $4D$,

$$\mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}ij, \quad i^2 = -1, j^2 = D, ij = -ji. \tag{1.2}$$

Our second main result is a construction of a canonical point $P \in E(\mathbb{Q}(i))$ (Theorem 3.23), using Heegner points on $X$ associated to the imaginary quadratic field $\mathbb{Q}(i)$ with the following desired property as in (1).

**Theorem 1.7** (Theorem 3.21)**.** *$P$ lies in $E(\mathbb{Q})$ if and only if $\varepsilon(E/\mathbb{Q}) = -1$.*

1.8. **A conjecture on the canonical point $P$.** In view of the Gross-Zagier formula ([GZ86], [YZZ13]), we naturally conjecture as in (2):

**Conjecture 1.9** (Conjecture 4.1)**.** *Assume $\varepsilon(E/\mathbb{Q}) = -1$. If the 2-rank of $\mathrm{Cl}(L)$ is at most 1, then $P \in E(\mathbb{Q})$ is of infinite order.*

Conjecture 1.9 seems quite difficult to us. The known general approach of showing that a Heegner point on $E$ is of infinite order is usually by showing the $L$-function $L(E, s)$ vanishes to order 1 at $s = 1$, either via explicit forms of the Gross–Zagier formula, or via its $p$-adic variants (e.g., the BDP formula [BDP13], [LZZ14]) and Iwasawa theory. However, the input of Conjecture 1.9 is purely algebraic — in terms of the 2-class group of cubic fields, and a more direct link with Heegner points or $L$-functions seems missing at the moment.

Nevertheless, we provide a piece of evidence of Conjecture 1.9 by verifying it for the case $D = 11$ in Example 4.2. We end this article by proposing a potential approach towards Conjecture 1.9, based on an unusual mod 2 congruence between elliptic curves and Artin representations (§5).

1.10. **Novelty of the methods and remarks on the proofs.**

1.10.1. *2-Selmer groups and 2-class groups.* The idea that there should be a connection between the 2-Selmer group and the 2-class group of the cubic field $L$ has been, of course, known for a long time. For example, the classical work of Brumer and Kramer [BK77, 7.1] gives a general upper bound on the 2-Selmer rank in terms of the 2-class group and other arithmetic invariants of $E$. See also Schaefer [Sch96] (and references therein) for the connection between the $p$-Selmer group and the $p$-class group of the $p$-torsion field for general $p$.

Thus the novelty of Theorem 1.4 lies in making this connection *explicit* and *sharp* for the large class of elliptic curves under consideration.

1.10.2. *Heegner points.* Since quadratic twisting $E : y^2 = F(x)$ by a quadratic field $K$ does not preserve the square-freeness of the discriminant of $F(x)$ unless $K = \mathbb{Q}(i)$, we are naturally led to construct Heegner points over $\mathbb{Q}(i)$. However, the elliptic curve $E$ necessarily has *additive reduction* at 2 and 2 is *ramified* in $\mathbb{Q}(i)$, which forbids the classical construction of Heegner points associated to Eichler orders. See recent works Kohen–Pacetti [KP15], Cai–Chen–Liu [CCL16] and Longo–Rotger–de Vera-Piquero [LRd16] addressing different aspects of this issue.

The order (1.2) we naturally consider is in fact *not* a classical Eichler order, and thus leads to a new construction of Heegner points. The associated Shimura curve $X$ is an example of more general Shimura curves of "level $p^2$" associated to a *non-maximal* order at a prime $p$ *ramified* in the quaternion algebra studied in [Li15, Chap 5], and also an example of Hijikata-Pizer-Shemanske curves more recently studied in [LRd16]. Though our new construction of Heegner points easily generalizes to general prime $p$, we stick to $p = 2$ for simplicity, in connection with the concrete problem at hand.

1.10.3. *A canonical rational point.* For classical modular curves $X_0(N)$ (or Shimura curves of Eichler level), there is essentially one modular parameterization $X_0(N) \to E$, which is given by the associated newform $f_E$ of level $N$. More precisely, the group of homomorphisms $\mathrm{Hom}_{\mathbb{Q}}(J_0(N), E)$ defined over $\mathbb{Q}$ has rank 1. Another new feature of our work is that this 1-dimensionality no longer holds for the Shimura curve $X$. In fact, we show that $\mathrm{Hom}_{\mathbb{Q}}(J_X, E)$ has exactly rank 2 (Proposition 3.13 (1)), so there is *no* canonical choice of a modular parametrization $J_X \to E$.

Nevertheless, we are able to construct a *canonical* point in $E(\mathbb{Q}(i))$ by utilizing the entire rank 2 space of homomorphisms. The observation is that the Shimura curve $X$ admits extra automorphisms by the symmetric group $S_3$ and we are able to determine the $S_3$-action on $\mathrm{Hom}_{\mathbb{Q}}(J_X, E)$ (Proposition 3.13 (3)). To do so, we use the key fact that there is a *unique* admissible representation of $\mathrm{PGL}_2(\mathbb{Q}_2)$ has conductor 2 (§3.10 (5)), which allows us to make the Jacquet–Langlands correspondence completely explicit. Notice that this uniqueness is quite special and fails for admissible representations of conductor 2 of $\mathrm{PGL}_2(\mathbb{Q}_p)$ when $p > 2$.

1.10.4. *The case $D = 11$.* The computation of Heegner points on Shimura curves is more difficult than its counterpart on modular curves. When $D = 11$, to compute the Heegner points on $X$ we utilize the results of Elkies for Heegner points on a classical Shimura curve $Y$ (of Eichler level), and a degree 3 map $X \to Y$. The same method also allows us to verify Conjecture 1.9 for some other small values of $D$. Unfortunately, when $D$ is large ($X$ has large genus), this computation becomes infeasible.

1.11. **Acknowledgments.** I am deeply grateful to Benedict Gross for his constant encouragement and advice throughout this project. I would also like to thank Noam Elkies for helpful conversation on Shimura curves computations and Barry Mazur and Yifeng Liu for useful comments on an earlier draft of this article. The examples in this article are computed using Sage ([S$^+$13]).

## 2. 2-Selmer groups and 2-class groups

Let $E/\mathbb{Q}$ be an elliptic curve. We impose the following assumption in this §2.

**Assumption 2.1.** Suppose $E$ has equation $y^2 = F(x)$, where $F(x) = x^3 + a_2x^2 + a_4x + a_6$ is an integral polynomial which

(1) is irreducible, and
(2) has negative and square-free discriminant $-D$.

2.2. **Properties of the cubic field $L$.** Let $L = \mathbb{Q}[x]/F(x)$. Then $L$ has the following elementary properties:

(1) Since $F(x)$ is irreducible and has negative discriminant, we know that $F(x)$ has Galois group $S_3$. The field $L = \mathbb{Q}[x]/F(x)$ is a complex cubic field, i.e., $L_\infty := L \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R} \times \mathbb{C}$.
(2) Since $\operatorname{disc} F(x) = -D$ is square-free, we know that $D \equiv 3 \pmod 4$, $L$ has discriminant $d_L = \operatorname{disc} F(x) = -D$, and $L$ has ring of integers $A = \mathbb{Z}[x]/F(x)$.

(3) Since $L$ has a unique real embedding, we know that the unit group $A^\times$ has rank one by Dirichlet's unit theorem. Let $u_L$ be a fundamental unit. Then $A^\times = u_L^{\mathbb{Z}} \times \{\pm 1\}$. After possibly replacing $u_L$ by $-u_L$, we may assume $u_L > 0$. After possibly replacing $u_L$ by $u_L^{-1}$, we may further assume $u_L > 1$.

2.3. **Properties of the elliptic curve $E$.** The elliptic curve $E : y^2 = F(x)$ has the following elementary properties:

(1) Since $F(x)$ is irreducible, we have $E(\mathbb{Q})[2] = 0$.
(2) The 2-torsion field $\mathbb{Q}(E[2])$, as the Galois closure of $L$, is an $S_3$-extension over $\mathbb{Q}$.
(3) $E$ has discriminant $\Delta = -2^4 D$. Since no 12th power divides $\Delta$, the equation $y^2 = F(x)$ is minimal. It follows that $E$ has bad reduction precisely at $p \mid 2D$.
(4) For $p \mid D$, since $D$ is square-free, by comparing the power of $p$ appearing on both sides of

$$c_4^3 - c_6^2 = -2^{10} \cdot 3^3 \cdot D,$$

we see that $p \nmid c_4$ (even for $p = 3$). Hence $E$ has multiplicative reduction of type $I_1$ at $p \mid D$. In particular, the component group of the Néron model of $E/\mathbb{Q}_p$ is trivial.
(5) We compute that $c_4 = 16(a_2^2 - 3a_4)$, so $2 \mid c_4$ and $E$ has additive reduction at 2.
(6) Therefore the conductor of $E$ is of the form $N = 2^{2+\delta} D$ for some $\delta \geq 0$. The order of $N$ at 2 is determined by the Ogg–Saito formula ([Sil94, 11.1])

$$\mathrm{ord}_2(N) = \mathrm{ord}_2(\Delta) + 1 - m = 5 - m, \tag{2.1}$$

where $m$ is the size of the component group of the Néron model of $E/\mathbb{Q}_2$.

Our main goal in this §2 is to relate the 2-Selmer group of $E/\mathbb{Q}$ and the 2-part of the ideal class group of the cubic field $L$, under Assumption 2.1.

2.4. **2-Selmer groups.** Recall that for an elliptic curve $E/\mathbb{Q}$, we have the global and local Kummer exact sequences, fitting into the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(\mathbb{Q})/2E(\mathbb{Q}) & \xrightarrow{\delta} & H^1(\mathbb{Q}, E[2]) & \longrightarrow & H^1(\mathbb{Q}, E)[2] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow {\scriptstyle \prod_v \mathrm{res}_v} & & \downarrow & & \\ 0 & \longrightarrow & \prod_v E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) & \xrightarrow{\prod_v \delta_v} & \prod_v H^1(\mathbb{Q}_v, E[2]) & \longrightarrow & \prod_v H^1(\mathbb{Q}_v, E)[2] & \longrightarrow & 0. \end{array}$$

Here the vertical maps are given by the product of restriction maps over all places $v$ of $\mathbb{Q}$.

**Definition 2.5.** The *2-Selmer group*

$$\mathrm{Sel}_2(E/\mathbb{Q}) \subseteq H^1(\mathbb{Q}, E[2])$$

consists of cohomology classes whose restriction at $v$ lies in the image of the local Kummer map $\delta_v$ for every $v$:

$$\mathrm{Sel}_2(E/\mathbb{Q}) = \{c \in H^1(\mathbb{Q}, E[2]) : \mathrm{res}_v(c) \in \mathrm{im}(\delta_v)\}.$$

Colloquially, the 2-Selmer group is cut out by the *local conditions*

$$\mathrm{im}(\delta_v) \subseteq H^1(\mathbb{Q}_v, E[2])$$

coming from local points for all $v$. By definition, we have an injection

$$E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \mathrm{Sel}_2(E/\mathbb{Q}).$$

The 2-Selmer group, due to its local nature, is easier to understand and the 2-Selmer rank $s_2(E/\mathbb{Q})$ provides an upper bound for the rank of $E(\mathbb{Q})$.

2.6. **Kummer maps.** Our goal is this subsection to give an explicit description of the global and local Kummer maps in terms of the cubic field $L$.

**Lemma 2.7.** *We have an exact sequence of finite group schemes over* $\mathbb{Q}$,

$$1 \to E[2] \to \mathrm{Res}_{L/\mathbb{Q}}\,\mu_2 \xrightarrow{\mathbb{N}} \mu_2 \to 1,$$

*where* $\mathbb{N}$ *is induced by the norm map from* $L$ *to* $\mathbb{Q}$. *We have an isomorphism*

$$H^1(\mathbb{Q}, E[2]) \cong (L^\times/(L^\times)^2)_{\mathbb{N}=\square}. \tag{2.2}$$

*Here* $(L^\times/(L^\times)^2)_{\mathbb{N}=\square}$ *consists of all classes in* $L^\times/(L^\times)^2$ *with square norms to* $\mathbb{Q}^\times$.

*Proof.* It suffices to check that we have an exact sequence of $G_\mathbb{Q}$-modules on the level of $\overline{\mathbb{Q}}$-points. Suppose $F(x)$ has the three roots $x_1, x_2, x_3 \in \overline{\mathbb{Q}}$. Then the $\overline{\mathbb{Q}}$-points of $E[2]$ consist of $P_i = (x_i, 0)$, $(i = 1, 2, 3)$ and $\infty$. The Galois group $G_\mathbb{Q}$ acts trivially on $\infty$ and permutes the three points $P_i$ via its $\mathrm{Gal}(\mathbb{Q}(E[2])/\mathbb{Q}) \cong S_3$-action on $x_i$. Also, the group of $\overline{\mathbb{Q}}$-points of $\mathrm{Res}_{L/\mathbb{Q}}\,\mu_2$ is isomorphic to $\mu_2 \times \mu_2 \times \mu_2$, where the three factors are indexed by the three roots $x_i$ and the Galois action permutes the three factors in the same way. The norm map simply multiplies the three factors and respects the $G_\mathbb{Q}$-action. One sees that the map

$$\infty \mapsto (1, 1, 1), \quad P_1 \mapsto (1, -1, -1), \quad P_2 \mapsto (-1, 1, -1), \quad P_3 \mapsto (-1, -1, 1)$$

gives an injective homomorphism of $G_\mathbb{Q}$-modules $E[2] \to \mathrm{Res}_{L/\mathbb{Q}}\,\mu_2$. Moreover, its image is exactly the kernel of the norm map. This finishes the proof of the first part.

Taking the long exact sequence in Galois cohomology, we obtain

$$H^0(\mathbb{Q}, \mathrm{Res}_{L/\mathbb{Q}}\,\mu_2) \xrightarrow{\mathbb{N}} H^0(\mathbb{Q}, \mu_2) \to H^1(\mathbb{Q}, E[2]) \to H^1(\mathbb{Q}, \mathrm{Res}_{L/\mathbb{Q}}\,\mu_2) \xrightarrow{\mathbb{N}} H^1(\mathbb{Q}, \mu_2).$$

Since $H^0(\mathbb{Q}, \mathrm{Res}_{L/\mathbb{Q}}\,\mu_2) = \mu_2(L) = \{\pm 1\}$, $H^0(\mathbb{Q}, \mu_2) = \mu_2(\mathbb{Q}) = \{\pm 1\}$ and $L/\mathbb{Q}$ has odd degree, we know that the first map is surjective. By Kummer theory, we know that

$$H^1(\mathbb{Q}, \mathrm{Res}_{L/\mathbb{Q}}\,\mu_2) \cong L^\times/(L^\times)^2, \quad H^1(\mathbb{Q}, \mu_2) \cong \mathbb{Q}^\times/(\mathbb{Q}^\times)^2.$$

Therefore

$$H^1(\mathbb{Q}, E[2]) = \ker(\mathbb{N} : L^\times/(L^\times)^2 \to \mathbb{Q}^\times/(\mathbb{Q}^\times)^2) = (L^\times/(L^\times)^2)_{\mathbb{N}=\square}.$$

This finishes the proof of the second part. □

**Proposition 2.8.** *Under the isomorphism (2.2), the global Kummer map* $\delta$ *can be described as*

$$\delta : E(\mathbb{Q})/2E(\mathbb{Q}) \to (L^\times/(L^\times)^2)_{\mathbb{N}=\square}, \quad P \mapsto x(P) - \beta,$$

*where* $x(P)$ *is the* $x$*-coordinate of* $P$ *and* $\beta$ *is the image of* $x$ *in* $L = \mathbb{Q}[x]/F(x)$.

*Proof.* Let $e_2 : E[2] \times E[2] \to \mu_2$ be the Weil pairing. Then we see that the homomorphism $E[2] \to \mathrm{Res}_{L/\mathbb{Q}}\,\mu_2$ in Lemma 2.7 is also given by

$$P \mapsto (e_2(P, P_1), e_2(P, P_2), e_2(P, P_3)).$$

The rational function $f_i = x - x_i$ has the divisor $(f_i) = 2P_i - 2\infty$ $(i = 1, 2, 3)$ and there exists some rational function $g_i$ (over $\overline{\mathbb{Q}}$) such that $f_i \circ [2] = g_i^2$ (see [Sil09, III.8]). The Weil pairing

$e_2$ is then given by

$$e_2(P,P_i) = \frac{g_i(X+P)}{g_i(X)},$$

where $X \in E(\overline{\mathbb{Q}})$ is any point such that $g(X+P)$ and $g(X)$ are both defined and nonzero. For $P \in E(\mathbb{Q})$, we choose $Q \in E(\overline{\mathbb{Q}})$ such that $[2]Q = P$. Then $\delta(P)$ corresponds to the cocycle $\{\sigma \mapsto Q^\sigma - Q\} \in H^1(\mathbb{Q}, E[2])$. Taking $P = Q^\sigma - Q$ and $X = Q$, we know that

$$e_2(Q^\sigma - Q, P_i) = \frac{g_i(Q)^\sigma}{g_i(Q)}. \tag{2.3}$$

By the identification $H^1(\mathbb{Q}, \mathrm{Res}_{L/\mathbb{Q}}\,\mu_2) \cong (L^\times/(L^\times)^2)_{\mathbb{N}=\square}$ coming from Kummer theory, Equation (2.3) implies that

$$\delta(P) \equiv g_i(Q)^2 \mod (L^\times)^2$$

under the embedding $L \hookrightarrow \overline{\mathbb{Q}}$ associated to $x_i$. But by the construction of $g_i$, we have $g_i(Q)^2 = f_i(P) = x(P) - x_i$. Hence

$$\delta(P) \equiv x(P) - x_i \mod (L^\times)^2$$

under the embedding $L \hookrightarrow \overline{\mathbb{Q}}$ associated to $x_i$, which finishes the proof. □

Base changing to $\mathbb{Q}_v$ in Lemma 2.7 and Proposition 2.8 , we obtain the analogous explicit description of the local Kummer maps $\delta_v$.

**Proposition 2.9.** *The local Kummer maps for $E$ are given by*

$$\delta_v : E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) \to H^1(\mathbb{Q}_v, E[2]) \cong (L_v^\times/(L_v^\times)^2)_{\mathbb{N}=\square}, \quad P \mapsto x(P) - \beta,$$

*where $\beta$ is the image of $x$ in $L_v = \mathbb{Q}_v[x]/F(x)$.*

*Remark* 2.10. Even though $E(\mathbb{Q})[2] = 0$, it is possible that $E(\mathbb{Q}_v)[2] \neq 0$. For a nonzero point $P \in E(\mathbb{Q}_v)[2]$, the expression $x(P) - \beta$ does not lie in $L_v^\times$ and it should be interpreted using the group structure: write $P = P_1 - P_2$ as the difference of two points $P_1, P_2 \in E(\mathbb{Q}_v)$ which are not 2-torsion, then $\delta_v(P) = (x(P_1) - \beta)/(x(P_2) - \beta)$.

2.11. **Local conditions.** In this subsection, we explain how Assumption 2.1 allows us to determine explicitly the local condition $\mathrm{im}(\delta_v)$ for each place $v$.

**Lemma 2.12.** *Let $p$ be a prime. Then the valuation of $\delta_p(P)$ is even for any $P \in E(\mathbb{Q}_p)$, namely,*

$$\delta_p(P) \in (A_p^\times/(A_p^\times)^2)_{\mathbb{N}=\square},$$

*where $A = \mathbb{Z}[x]/F(x)$ is the ring of integers of $L$ and $A_p = A \otimes \mathbb{Z}_p$.*

*Proof.* Let $P \in E(\mathbb{Q}_p)$ and write $x = x(P)$ for short.

First consider the case $p \nmid D$. So $p$ is unramified in $L$. There are three cases:

(1) $L_p \cong \mathbb{Q}_{p^3}$ is the unramified cubic extension of $\mathbb{Q}_p$. From $y^2 = F(x)$, we know that $2\,\mathrm{ord}_p(y) = 3\,\mathrm{ord}_p(x-\beta)$, hence $\mathrm{ord}_p(x-\beta)$ is even.
(2) $L_p \cong \mathbb{Q}_{p^2} \times \mathbb{Q}_p$, where $\mathbb{Q}_{p^2}$ is the unramified quadratic extension of $\mathbb{Q}_p$. Write $\beta = (\gamma, c)$, then $\gamma \not\equiv c \pmod p$, $\mathrm{ord}_p(\gamma) = 0$ and $\mathrm{ord}_p(c) \geq 0$. From $y^2 = F(x)$, we know that $2\,\mathrm{ord}_p(y) = \mathrm{ord}_p(x-\gamma) + \mathrm{ord}_p(x-c)$. There are two cases:
   - If $\mathrm{ord}_p(x) < 0$, then $\mathrm{ord}_p(x-\gamma) = \mathrm{ord}_p(x-c) = \mathrm{ord}_p(x)$. Therefore $2\,\mathrm{ord}_p(y) = 3\,\mathrm{ord}_p(x)$, hence $\mathrm{ord}_p(x-\gamma) = \mathrm{ord}_p(x-c) = \mathrm{ord}_p(x)$ are all even.
   - If $\mathrm{ord}_p(x) \geq 0$, then $\mathrm{ord}_p(x-\gamma) = 0$. So $\mathrm{ord}_p(x-c) = 2\,\mathrm{ord}_p(y)$ is even.

(3) $L_p \cong \mathbb{Q}_p \times \mathbb{Q}_p \times \mathbb{Q}_p$. Write $\beta = (c_1, c_2, c_3)$. Then $c_i \not\equiv c_j \pmod p$ whenever $i \neq j$. Similarly, there are two cases:
   - If $\mathrm{ord}_p(x) < 0$, then $\mathrm{ord}_p(x - c_i) = \mathrm{ord}_p(x)$. Therefore $2\,\mathrm{ord}_p(y) = 3\,\mathrm{ord}_p(x)$, hence $\mathrm{ord}_p(x - c_i) = \mathrm{ord}_p(x)$ are all even.
   - If $\mathrm{ord}_p(x) \geq 0$, then $\mathrm{ord}_p(x - c_i) \geq 0$. Since $c_i \not\equiv c_j \pmod p$, at least two of the $\mathrm{ord}_p(x - c_i)$'s are zeros. Thus $2\,\mathrm{ord}_p(y) = \mathrm{ord}_p(x - c_1) + \mathrm{ord}_p(x - c_2) + \mathrm{ord}_p(x - c_3)$ implies the third one must have even valuation as well.

Now consider the case $p \mid D$. So $p$ is ramified in $L$. Since $D$ is square-free, we know that $L_p \cong K_p \times \mathbb{Q}_p$, where $K_p$ is a ramified quadratic extension of $\mathbb{Q}_p$. Denote by $\mathfrak{p}$ the prime for $K_p$ and write $\beta = (\gamma, c)$. Then $\gamma \not\equiv c \pmod p$, $\mathrm{ord}_p(\gamma) > 0$ and $\mathrm{ord}_p(c) \geq 0$. From $y^2 = F(x)$, we know that $2\,\mathrm{ord}_p(y) = \mathrm{ord}_{\mathfrak{p}}(x - \gamma) + \mathrm{ord}_p(x - c)$. We argue similarly:

- If $\mathrm{ord}_p(x) < 0$, then $\mathrm{ord}_{\mathfrak{p}}(x - \gamma) = 2\,\mathrm{ord}_p(x)$ and $\mathrm{ord}_p(x - c) = \mathrm{ord}_p(x)$. Hence $\mathrm{ord}_p(x)$ is even, therefore both $\mathrm{ord}_{\mathfrak{p}}(x - \gamma)$ and $\mathrm{ord}_p(x - c)$ are even.
- If $\mathrm{ord}_p(x) \geq 0$, then $\mathrm{ord}_{\mathfrak{p}}(x - \gamma) \geq 0$ and $\mathrm{ord}_p(x - c) \geq 0$. Since $\gamma \not\equiv c \pmod p$, at least one of $\mathrm{ord}_{\mathfrak{p}}(x - \gamma)$ and $\mathrm{ord}_p(x - c)$ is zero. Hence both of them are even. □

*Remark* 2.13. When $p \neq 2$, Lemma 2.12 can be proved by a more "pure thought" argument: since the component group of Néron model of $E/\mathbb{Q}_p$ is trivial (2.3 (4)), the local condition at $p$ corresponds to the unramified cohomology $H^1_{\mathrm{ur}}(\mathbb{Q}_p, E[2])$ ([GP12, Lemma 6]), which consists of the units $(A_p^\times/(A_p^\times)^2)_{\mathbb{N}=\square}$ under the isomorphism (2.2). Here we preferred the above direct computational proof using the explicit description of $\delta_p$ in Proposition 2.9, which depends on less machinery and also treats the case $p = 2$.

**Proposition 2.14.** *We have*

*(1) For $v = \infty$, both $E(\mathbb{R})/2E(\mathbb{R})$ and $(L_\infty^\times/(L_\infty^\times)^2)_{\mathbb{N}=\square}$ are trivial. In particular, the local condition* $\mathrm{im}(\delta_\infty)$ *is trivial.*

*(2) For $v = p > 2$, the local condition* $\mathrm{im}(\delta_p) = (A_p^\times/(A_p^\times)^2)_{\mathbb{N}=\square}$.

*(3) For $v = p = 2$, the local condition* $\mathrm{im}(\delta_2)$ *has index 2 in* $(A_2^\times/(A_2^\times)^2)_{\mathbb{N}=\square}$ *and contains all units* $\equiv 1 \pmod 4$.

*Proof.* For $v = \infty$, since $L_\infty \cong \mathbb{R} \times \mathbb{C}$, we know that

$$(L_\infty^\times/(L_\infty^\times)^2)_{\mathbb{N}=\square} = (\mathbb{R}^\times/(\mathbb{R}^\times)^2)_{\mathbb{N}=\square} = \{1\}.$$

For $v = p$, we know from Lemma 2.12 that $\mathrm{im}(\delta_p) \subseteq (A_p^\times/(A_p^\times)^2)_{\mathbb{N}=\square}$. Since the norm map is surjective on the units, we know that

$$\#(A_p^\times/(A_p^\times)^2)_{\mathbb{N}=\square} = \frac{\#A_p^\times/(A_p^\times)^2}{\#\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2}.$$

Notice that $\#\mathbb{Z}_p^\times/(\mathbb{Z}_p^\times)^2$ is $2^2$ or 2 depending on whether $p = 2$ or not. If $L_p$ is a product of $k$ fields ($k = 1, 2, 3$), then $\#A_p^\times/(A_p^\times)^2$ is $2^{k+3}$ or $2^k$ depending on whether $p = 2$ or not. It follows that

$$\#(A_p^\times/(A_p^\times)^2)_{\mathbb{N}=\square} = \begin{cases} 2^{k-1}, & p \neq 2, \\ 2^{k+1}, & p = 2. \end{cases}$$

Since $E(\mathbb{Q}_p)$ has a finite index subgroup isomorphic to $\mathbb{Z}_p$, we know that

$$\#E(\mathbb{Q}_p)/2E(\mathbb{Q}_p) = \begin{cases} \#E(\mathbb{Q}_p)[2], & p \neq 2, \\ 2 \cdot \#E(\mathbb{Q}_p)[2], & p = 2. \end{cases}$$

All claims except the last one then follow because $\#E(\mathbb{Q}_p)[2]$ is the same as 1 plus the number of $\mathbb{Q}_p$-rational solutions of $F(x)=0$ , which is $2^{k-1}$ in all cases. To see the last claim that $\mathrm{im}(\delta_2)$ contains all the units $\equiv 1 \pmod 4$, let us consider a point $P \in \hat{E}(2\mathbb{Z}_2)$, where $\hat{E}$ is the formal group of $E$ over $\mathbb{Q}_2$ given by the minimal equation. For a general elliptic curve $E$ with minimal equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

the general formula ([Sil94, IV.1]) reads

$$x(P) = z^{-2} - a_1z^{-1} - a_2 - a_3z + O(z^2),$$

where $z = -x/y$ is the parameter for the formal group. In our case $a_1 = 0$, therefore

(2.4)

$$\delta_2(P) = x(P) - \beta = z^{-2} - a_2 - \beta + O(z) \equiv 1-(a_2+\beta)z^2 + O(z^3) \equiv 1-(a_2+\beta)z^2 \mod (L_2^\times)^2,$$

where the last equality is because $z \in 2\mathbb{Z}_2$ and the units $\equiv 1 \pmod 8$ are squares. Since $F(x)$ mod 2 cannot be a product of three distinct linear factors in $\mathbb{F}_2[x]$, we know that 2 does not split in $L$. Now one can then check directly that $\mathrm{im}(\delta_2)$ contains the units $\equiv 1 \pmod 4$ with square norm in the remaining two cases:

- If $L_2 = \mathbb{Q}_8$, then all units $\equiv 1 \pmod 4$ with square norms are actually squares. So the claim that $\mathrm{im}(\sigma_2)$ contains all such units is trivial.
- If $L_2 = \mathbb{Q}_4 \times \mathbb{Q}_2$, then any class $(\alpha, a) \equiv 1 \pmod 4$ with square norm is represented by $(\alpha, \mathbb{N}\alpha)$ with $\alpha \equiv 1 \pmod 4$. There is a unique nontrivial class of units $\alpha \equiv 1 \pmod 4$ modulo squares, represented by $1 + 4\gamma$ if we write $\beta = (\gamma, c)$. It follows from (2.4) that $\mathrm{im}(\delta_2)$ contains this class. □

2.15. **2-class groups of cubic fields.** We now combine all the local conditions to give both upper and lower bounds for the 2-Selmer group.

**Lemma 2.16.** *Let*

$$M_1 = \{\alpha \in L^\times/(L^\times)^2 : L(\sqrt{\alpha})/L \textit{ is unramified}\},$$

*and*

$$M_2 = \{\alpha \in L^\times/(L^\times)^2 : \alpha > 0, (\alpha) = I^2, I \subseteq L \textit{ a fractional ideal}\}$$

*be subgroups of* $(L^\times/(L^\times)^2)_{\mathbb{N}=\square}$. *Then under the isomorphism (2.2), we have*

$$M_1 \subseteq \mathrm{Sel}_2(E/\mathbb{Q}) \subseteq M_2.$$

*Proof.* Elements of $M_2$ clearly have square norms since $\mathbb{N}\alpha = \mathbb{N}(I)^2$. If $\alpha \in \mathrm{Sel}_2(E/\mathbb{Q})$, then by Proposition 2.14, $\alpha > 0$ and $\alpha$ has even valuation at all finite places. The latter implies that there exists a fractional ideal $I$ such that $(\alpha) = I^2$. Thus $\alpha \in M_2$.

Let $\alpha \in L^\times/(L^\times)^2$. For $p$ odd, $L_p(\sqrt{\alpha})/L_p$ is unramified if and only if $\alpha$ has even valuation. For $p = 2$, $L_2(\sqrt{\alpha})/L_2$ is unramified if and only if $\alpha$ has even valuation and is represented by a unit $\equiv 1 \pmod 4$. From this description we see that $M_1 \subseteq M_2$ and elements $M_1$ have square norm. It also follows from this description and Proposition 2.14 that $M_1 \subseteq \mathrm{Sel}_2(E/\mathbb{Q})$. □

Class field theory supplies information about the two groups $M_1$ and $M_2$.

**Lemma 2.17.** *Let* $\mathrm{Cl}(L)$ *be the ideal class group of the cubic field* $L = \mathbb{Q}[x]/F(x)$. *Let* $k = \dim_{\mathbb{F}_2} \mathrm{Cl}(L)[2]$. *Then* $M_1$ *(resp.* $M_2$*) is an elementary 2-group of size* $2^k$ *(resp.* $2^{k+1}$*).*

*Proof.* Kummer theory tells us that

$$M_1 \cong \mathrm{Hom}(\mathrm{Gal}(M/L), \mu_2),$$

where $M$ is obtained by adjoining the square roots of all $\alpha \in M_1$ to $L$, which is the maximal unramified extension of $L$ of exponent 2. By class field theory, we have

$$\mathrm{Gal}(M/L) \cong \mathrm{Cl}(L)[2].$$

Since $\#(\mathrm{Cl}(L)/2\,\mathrm{Cl}(L)) = \#\,\mathrm{Cl}(L)[2]$, $M_1$ is an elementary 2-group of size $2^k$.

Suppose $\alpha \in M_2$ such that $(\alpha) = I^2$. Then the assignment $\alpha \mapsto I$ gives a well defined map

$$M_2 \to \mathrm{Cl}(L)[2].$$

This map is clearly surjective and its kernel is given by the positive units

$$\{\alpha \in A^\times/(A^\times)^2 : \alpha > 0\} = u_L^{\mathbb{Z}}/u_L^{2\mathbb{Z}} \cong \mathbb{Z}/2\mathbb{Z}.$$

Since $\#\,\mathrm{Cl}(L)[2] = 2^k$, we know that $M_2$ is an elementary 2-group of size $2^{k+1}$. □

Now we are ready to prove the main theorem of this §2.

**Theorem 2.18.** *Let* $\mathrm{Cl}(L)$ *be the ideal class group of the cubic field* $L = \mathbb{Q}[x]/F(x)$*. Let* $k = \dim_{\mathbb{F}_2} \mathrm{Cl}(L)/2\,\mathrm{Cl}(L)$*. Then*

$$s_2(E/\mathbb{Q}) = k \text{ or } k+1,$$

*depending on whether the root number* $\varepsilon(E/\mathbb{Q}) = (-1)^k$ *or* $(-1)^{k+1}$*.*

*Proof.* It follows from Lemma 2.16 and 2.17 that $s_2(E/\mathbb{Q}) = k$ or $k+1$. By [Mon96, Theorem 1.5], the parity of $s_2(E/\mathbb{Q})$ is determined by the root number $\varepsilon(E/\mathbb{Q})$, that is,

$$(-1)^{s_2(E/\mathbb{Q})} = \varepsilon(E/\mathbb{Q}).$$

The desired result then follows. □

2.19. **Examples.** We end this section with several explicit examples illustrating Theorem 2.18.

**Example 2.20.** Consider the elliptic curve (in Cremona's labeling)

$$E = 1132a1 : y^2 = F(x) = x^3 + x^2 - 5x + 4.$$

The polynomial $F(x)$ is irreducible and has discriminant $-D = -283$ and thus Assumption 2.1 holds. The elliptic curve $E$ has discriminant $\Delta = -2^4 \cdot 283$, conductor $N = 2^2 \cdot 283$. The cubic field $L = \mathbb{Q}[x]/F(x)$ has discriminant $d_L = -283$ and class number 2. We remark that $L$ has the *smallest* discriminant among all class number 2 cubic fields. Theorem 2.18 predicts that $s_2(E/\mathbb{Q}) = 1$ or 2 according to the root number. In fact, $\varepsilon(E/\mathbb{Q}) = +1$, $r_{\mathrm{alg}}(E/\mathbb{Q}) = s_2(E/\mathbb{Q}) = 2$ and the two points $(-1, 3)$ and $(1, -1)$ generate $E(\mathbb{Q})$.

**Example 2.21.** Consider the elliptic curve

$$E = 26284a1 : y^2 = F(x) = x^3 + x^2 - 9x + 16.$$

The polynomial $F(x)$ is irreducible and has discriminant $-D = -6571$ and thus Assumption 2.1 holds. The elliptic curve $E$ has discriminant $\Delta = -2^4 \cdot 6571$, conductor $N = 2^2 \cdot 6571$. The cubic field $L = \mathbb{Q}[x]/F(x)$ has discriminant $d_L = -6571$ and class group $\mathrm{Cl}(L) \cong (\mathbb{Z}/2\mathbb{Z})^2$. We remark that $L$ has the *smallest* discriminant among all cubic fields with class group $(\mathbb{Z}/2\mathbb{Z})^2$.

Theorem 2.18 predicts that $s_2(E/\mathbb{Q}) = 2$ or $3$ according to the root number. In fact, $\varepsilon(E/\mathbb{Q}) = -1$, $r_{\mathrm{alg}}(E/\mathbb{Q}) = s_2(E/\mathbb{Q}) = 3$ and the three points $(-4, 2)$, $(-3, 5)$, $(-1, 5)$ generate $E(\mathbb{Q})$.

**Example 2.22.** Consider the elliptic curve

$$E : y^2 = F(x) = x^3 - 49x + 169.$$

The polynomial $F(x)$ is irreducible and has discriminant $-D = -37 \cdot 8123$ and thus Assumption 2.1 holds. The elliptic curve $E$ has discriminant $\Delta = -2^4 \cdot 37 \cdot 8123$, conductor $N = 1202204 = 2^2 \cdot 37 \cdot 8123$. The cubic field $L = \mathbb{Q}[x]/F(x)$ has discriminant $d_L = -37 \cdot 8123$ and class group $\mathrm{Cl}(L) \cong (\mathbb{Z}/2\mathbb{Z})^3$. We remark that $L$ has the *smallest* discriminant among all cubic fields with class group $(\mathbb{Z}/2\mathbb{Z})^3$. Theorem 2.18 predicts that $s_2(E/\mathbb{Q}) = 3$ or $4$ according to the root number. In fact, $\varepsilon(E/\mathbb{Q}) = +1$, $r_{\mathrm{alg}}(E/\mathbb{Q}) = s_2(E/\mathbb{Q}) = 4$ and the four points $(-8, 7)$, $(-7, 13)$, $(-5, 17)$, $(-3, 17)$ generate $E(\mathbb{Q})$.

## 3. Heegner points on elliptic curves of conductor $4D$

Throughout this §3, we will impose the following assumption.

**Assumption 3.1.** Suppose $E$ has equation $y^2 = F(x)$, where $F(x) = x^3 + a_2x^2 + a_4x + a_6$ is an integral polynomial which

(1) is irreducible, and
(2) has negative and square-free discriminant $-D$.

We further assume that

(3) $E/\mathbb{Q}_2$ has Kodaira type IV.

*Remark* 3.2. The additional assumption (3) that $E/\mathbb{Q}_2$ has Kodaira type IV means that the special fiber of the minimal regular model of $E/\mathbb{Q}_2$ consists of three $\mathbb{P}^1$'s intersecting at a triple point. It implies that $m = 3$ in Equation (2.1). Hence $\mathrm{ord}_2(N) = 2$ and $E$ has the minimal possible conductor $N = 4D$. It also implies that the $j$-invariant of $E$ has positive 2-adic valuation ([Sil94, Table 4.1]). In particular, $E$ has potentially good reduction at 2.

**Example 3.3.** If we assume

$$\begin{cases} a_6 \equiv 1 & \pmod 4, \\ a_4^2 \equiv 4a_2 & \pmod 8, \end{cases}$$

then it follows from Tate's algorithm [Sil94, IV.9] that $E$ has Kodaira type IV over $\mathbb{Q}_2$. In fact, making a change of variable $y' = y + 1$, $x' = x$, we obtain the following equation

$$y'^2 + 2y' = x'^3 + a_2x'^2 + a_4x' + (a_6 - 1),$$

satisfying $2 \mid a_3', a_4', a_6'$. We compute that

$$b_2' = 4a_2, \quad b_4' = 2a_4, \quad b_6' = 4a_6, \quad b_8' = 4a_2a_6 - a_4^2, \quad c_4' = 16(a_2^2 - 3a_4).$$

So

$$2 \mid c_4', \quad 2^2 \mid a_6', \quad 2^3 \mid b_8', \quad 2^3 \nmid b_6',$$

and Tate's algorithm outputs the Kodaira type IV. Moreover, the component group of the Néron model over $\mathbb{Q}_2$ is either $\mathbb{Z}/3\mathbb{Z}$ or $\mu_3$. It is $\mathbb{Z}/3\mathbb{Z}$ if and only if $x^2 + x - (a_6 - 1)/4 \equiv 0 \pmod 2$ has a solution, if and only if $a_6 \equiv 1 \pmod 8$.

3.4. **Root numbers.** As we will see, the additional assumption (3) also pins down the root number of $E$ over the quadratic field $\mathbb{Q}(i)$ to be $-1$ (Proposition 3.7).

**Lemma 3.5.** *The field $\mathbb{Q}_2(E[3])$ generated by 3-torsion points of $E$ is the tamely ramified $S_3$-extension $\mathbb{Q}_2(\zeta_3, \sqrt[3]{\Delta})$.*

*Proof.* The assumption of Kodaira type IV at 2 allows us to compute $\mathbb{Q}_2(E[3])$ as follows. Since the component group of the Néron model of $E/\mathbb{Q}_2$ is either $\mathbb{Z}/3\mathbb{Z}$ or $\mu_3$, we know that $E$ has a subgroup $\mathbb{Z}/3\mathbb{Z}$ over the unramified quadratic extension $M = \mathbb{Q}_2(\zeta_3)$. Let $G = \mathrm{Gal}(M(E[3])/M) \subseteq \mathrm{GL}_2(\mathbb{F}_3)$. Then by the Weil pairing, the inertia subgroup $I \subseteq G$ acts as a subgroup of $\{(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix})\} \subseteq \mathrm{GL}_2(\mathbb{F}_3)$, hence $I$ is either trivial or of order 3. But $\mathbb{Q}_2(E[3])$ always contains $\sqrt[3]{\Delta}$ (see [Ser72, p. 305]), so $\mathbb{Q}_2(E[3])/\mathbb{Q}_2$ is ramified and $I$ is of order 3. Notice that $\mathbb{Q}_2(\zeta_3, \sqrt[3]{\Delta})$, as the Galois closure of $\mathbb{Q}_2(\sqrt[3]{\Delta})$, has Galois group $S_3$, so we know that $G$ cannot be cyclic of order 3 or 6. Since $I$ is normal in $G$ and $G/I$ is cyclic, it follows that $G \cong S_3$ by inspection on possible subgroups of $\mathrm{GL}_2(\mathbb{F}_3)$. Therefore $\mathbb{Q}_2(E[3]) = \mathbb{Q}_2(\zeta_3, \sqrt[3]{\Delta})$. □

*Remark* 3.6. It also follows from this lemma directly that $\mathrm{ord}_2(N) = 2$, which reproves the Ogg–Saito formula in this case.

**Proposition 3.7.** *The root number $\varepsilon(E/\mathbb{Q}(i))$ of $E/\mathbb{Q}(i)$ is $-1$.*

*Proof.* Recall that the root number is the product of local root numbers over all places $v$

$$\varepsilon(E/\mathbb{Q}(i)) = \prod_v \varepsilon_v(E/\mathbb{Q}(i)).$$

We compute all the local root numbers (cf. [Dok13, 3.4]) as follows.

(1) The local root number of an elliptic curve is always $-1$ at an infinite place.
(2) For $\mathfrak{p} \nmid 2D$, the elliptic curve $E$ has good reduction at $\mathfrak{p}$ and thus $\varepsilon_\mathfrak{p}(E/\mathbb{Q}(i)) = +1$.
(3) For $\mathfrak{p} \mid D$, the elliptic curve $E$ has multiplicative reduction at $\mathfrak{p}$.
   - When $\mathfrak{p}$ lies above $p \equiv 3 \bmod 4$, $\mathbb{Q}(i)_\mathfrak{p}$ is the unramified quadratic extension of $\mathbb{Q}_p$ and thus $E$ has split multiplicative reduction at $\mathfrak{p}$. Therefore $\varepsilon_\mathfrak{p}(E/\mathbb{Q}(i)) = -1$. Because $D \equiv 3 \pmod 4$ is square-free, there are an odd number of primes $\mathfrak{p} \mid D$ lying above $p \equiv 3 \pmod 4$. Hence the product over all $\mathfrak{p}$ above $p \equiv 3 \pmod 4$ is $-1$.
   - When $\mathfrak{p}$ lies above $p \equiv 1 \pmod 4$, $E$ may have split or nonsplit multiplicative reduction at $\mathfrak{p}$. But since $p = \mathfrak{p}\mathfrak{p}'$ splits as two primes in $\mathbb{Q}(i)$ and $\varepsilon_\mathfrak{p}(E/\mathbb{Q}(i)) = \varepsilon_{\mathfrak{p}'}(E/\mathbb{Q}(i))$, we know that the product over all $\mathfrak{p}$ above $p \equiv 1 \pmod 4$ is $+1$.
(4) When $\mathfrak{p} \mid 2$, we know the 3-torsion points $E[3]$ generate a $S_3$-extension over the wildly ramified quadratic extension $\mathbb{Q}(i)_\mathfrak{p} = \mathbb{Q}_2(i)$ by Lemma 3.5. The local root number is $-1$ in this case by [DD08, Remark 5].

Combining all the local results gives the desired root number $\varepsilon(E/\mathbb{Q}(i)) = -1$. □

Now let

$$E^* : y^2 = F^*(x) = x^3 - a_2x^2 + a_4x - a_6$$

be the quadratic twist of $E$ by $\mathbb{Q}(i)$. By Proposition 3.7, we have

$$\varepsilon(E/\mathbb{Q}) \cdot \varepsilon(E^*/\mathbb{Q}) = \varepsilon(E/\mathbb{Q}(i)) = -1.$$

It follows that the functional equations for $L(E/\mathbb{Q}, s)$ and $L(E^*/\mathbb{Q}, s)$ have different signs $\varepsilon(E/\mathbb{Q})$ and $\varepsilon(E^*/\mathbb{Q})$. We denote by $E^\pm = E$ or $E^*$ so that $\varepsilon(E^\pm/\mathbb{Q}) = \pm 1$.

Notice that $E^*$ also satisfies Assumption 2.1. Moreover, the cubic field defined by $\mathbb{Q}[x]/F^*(x)$ is isomorphic to $L = \mathbb{Q}[x]/F(x)$. When the 2-rank of $\mathrm{Cl}(L)$ is at most 1, the 2-Selmer rank $s_2(E^-/\mathbb{Q}) = 1$ by Theorem 2.18. The 2-Selmer rank one conjecture (Conjecture 1.2) then predicts that

**Conjecture 3.8.** *If the 2-rank of* $\mathrm{Cl}(L)$ *is at most 1, then* $r_{\mathrm{alg}}(E^-/\mathbb{Q}) = 1$.

We pursue a canonical construction of a point (conjecturally) of infinite order using Shimura curves in the sequel.

*Remark* 3.9. Our construction below works well for any elliptic curve $E/\mathbb{Q}$ with conductor $N = 4D$ and $\varepsilon(E/\mathbb{Q}(i)) = -1$. We assume (3) of Assumption 3.1 only for concreteness.

3.10. **Explicit Jacquet–Langlands correspondence.** By the modularity theorem, there is an automorphic representation $\pi = \bigotimes_v \pi_v$ of $\mathrm{GL}_2(\mathbb{A})$ associated to the elliptic curve $E$, where $\mathbb{A}$ is the ring of adeles of $\mathbb{Q}$. It can be characterized as follows:

(1) $\pi$ has trivial central character.
(2) $\pi_\infty$ is a holomorphic discrete series with Harish-Chandra parameter $\frac{1}{2}$ (corresponding to weight 2 modular forms).
(3) For $p \nmid 2D$, $\pi_p$ is unramified. Its Satake parameter has characteristic polynomial $X^2 - a_pX + p$, where $a_p = p + 1 - \#E(\mathbb{F}_p)$.
(4) For $p \mid D$, $\pi_p$ is the Steinberg representation or the unramified quadratic twist of the Steinberg representation, depending on whether $\varepsilon_p(E/\mathbb{Q}) = -1$ or $\varepsilon_p(E/\mathbb{Q}) = +1$.
(5) For $p = 2$, $\pi_2$ has conductor 2 (since $\mathrm{ord}_2(N) = 2$). It cannot be a tamely ramified principal series, since there are no tamely ramified characters of $\mathbb{Q}_2^\times$! Therefore $\pi_2$ is a depth zero supercuspidal representation, which is compactly induced from $\mathrm{PGL}_2(\mathbb{Z}_2)$ using the unique discrete series representation of $\mathrm{PGL}_2(\mathbb{F}_2) \cong S_3$, the sign character $S_3 \to \{\pm 1\}$.

Let $B = (-1, D)_{\mathbb{Q}}$ be the rational quaternion algebra

$$\mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}ij, \quad i^2 = -1, j^2 = D, ij = -ji.$$

Then $B$ is split at $\infty$ and is ramified at primes in

$$\Sigma = \{2\} \cup \{p \mid D : p \equiv 3 \pmod 4\}.$$

Notice that $\Sigma$ has even cardinality since $D \equiv 3 \pmod 4$. Let

$$R = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}ij \subseteq B. \tag{3.1}$$

Then $R$ is an order of reduced discriminant $4D$. We now give a description of the local orders $R_p = R \otimes \mathbb{Z}_p$ and the normalizers of $R_p^\times$.

**Proposition 3.11.** *Let* $W_p = N_{B_p^\times}(R_p^\times)/R_p^\times \mathbb{Q}_p^\times$, *where* $N_G(H)$ *denotes the normalizer of* $H$ *in* $G$. *Then*

$$W_p \cong \begin{cases} \mathbb{Z}/2\mathbb{Z}, & p \mid D, \\ S_3, & p = 2, \\ \{1\}, & \textit{otherwise}. \end{cases}$$

*Proof.* We have the following cases:

- For $p \nmid 2D$, $B_p$ is isomorphic to the matrix algebra $M_2(\mathbb{Q}_p)$ and $R_p$ is a maximal order $M_2(\mathbb{Z}_p)$ (up to conjugation). Hence $N_{B_p^\times}(R_p^\times) = \mathrm{GL}_2(\mathbb{Z}_p) \cdot \mathbb{Q}_p^\times = R_p^\times \cdot \mathbb{Q}_p^\times$ and $W_p$ is trivial.

- For $p \mid 2D$, $p \notin \Sigma$, $B_p$ is isomorphic to $M_2(\mathbb{Q}_p)$ and $R_p$ is an order of reduced discriminant $p\mathbb{Z}_p$, which is $\begin{pmatrix} \mathbb{Z}_p & \mathbb{Z}_p \\ p\mathbb{Z}_p & \mathbb{Z}_p \end{pmatrix}$ (up to conjugation). Therefore $R_p^\times$ is the standard Iwahori subgroup of $\mathrm{GL}_2(\mathbb{Q}_p)$ and $N_{B_p^\times}(R_p^\times)/R_p^\times\mathbb{Q}_p^\times \cong \mathbb{Z}/2\mathbb{Z}$ generated by the element $\left(\begin{smallmatrix} 0 & 1 \\ p & 0 \end{smallmatrix}\right)$.
- For odd $p \in \Sigma$, $B_p$ is a quaternion algebra over $\mathbb{Q}_p$ and $R_p$ is the maximal order of $B_p$. Hence $N_{B_p^\times}(R_p^\times)/R_p^\times\mathbb{Q}_p^\times \cong \mathbb{Z}/2\mathbb{Z}$ is generated by a uniformizer of $B_p$.
- For $p = 2$, since $R_2$ has reduced discriminant $4\mathbb{Z}_2$, it is the unique index 2 suborder of the maximal order $\mathcal{O}_2$ of $B_2$,
$$R_2 = \{x \in \mathcal{O}_2 : (x \bmod \mathfrak{m}_2) \in \mathbb{F}_2 \subseteq \mathbb{F}_4 = \mathcal{O}_2/\mathfrak{m}_2\},$$
where $\mathfrak{m}_2$ is the maximal ideal of $\mathcal{O}_2$. Then $N_{B_2^\times}(R_2^\times)/R_2^\times\mathbb{Q}_2^\times \cong B_2^\times/R_2^\times\mathbb{Q}_2^\times \cong S_3$, which is generated by the order 2 class of a uniformizer and the cyclic quotient $\mathcal{O}_2^\times/R_2^\times \cong \mathbb{F}_4^\times/\mathbb{F}_2^\times \cong \mathbb{Z}/3\mathbb{Z}$. □

*Remark* 3.12. Since $R_p$ is a local Eichler order of reduced discriminant $p$ for any $p \neq 2$ (for background on Eichler orders, see [AB04, 1.2]) and Eichler orders are determined by its localizations ([AB04, 1.51]), we know that there is a unique Eichler order $S$ such that
$$S_p = R_p \text{ for } p \neq 2, \quad S_2 = \mathcal{O}_2.$$
Then $S$ is the unique Eichler order of reduced discriminant $2D$ containing $R$ and $R \subseteq S$ is the unique index 2 suborder, given by
$$R = \{x \in S : (x \bmod \mathfrak{m}_2) \in \mathbb{F}_2 \subseteq \mathbb{F}_4 = \mathcal{O}_2/\mathfrak{m}_2\}.$$

The Jacquet–Langlands correspondence associates to $\pi$ an automorphic representation
$$\sigma = \sigma_f \otimes \sigma_\infty = \bigotimes_v \sigma_v$$
of $B^\times(\mathbb{A})$ of the same conductor $4D$. We can characterize it as follows:

(1) $\sigma$ has trivial central character.
(2) $\sigma_\infty \cong \pi_\infty$ is a holomorphic discrete series with Harish-Chandra parameter $\frac{1}{2}$ (corresponding to weight 2 modular forms).
(3) For $p \nmid 2D$, we have $B_p^\times \cong \mathrm{GL}_2(\mathbb{Q}_p)$ and $\sigma_p \cong \pi_p$ is unramified. Its Satake parameter has characteristic polynomial $X^2 - a_pX + p$, where $a_p = p + 1 - \#E(\mathbb{F}_p)$.
(4) For $p \mid 2D$, $p \notin \Sigma$, we also have $B_v^\times \cong \mathrm{GL}_2(\mathbb{Q}_v)$ and $\sigma_v \cong \pi_v$. Since $\sigma_p$ has conductor 1 and $R_p^\times$ is the standard Iwahori subgroup of $\mathrm{GL}_2(\mathbb{Q}_p)$, the fixed space $\sigma_p^{R_p^\times}$ is 1-dimensional. The group $W_p$ acts on $\delta_p^{R_p^\times}$ via the sign or the trivial character depending on whether $\pi_p$ is the Steinberg representation or the unramified quadratic twist of the Steinberg representation.
(5) For odd $p \in \Sigma$, since $\sigma_p$ has conductor 1, the fixed space $\sigma_p^{R_p^\times}$ is a 1-dimensional representation of $W_p$. It is either the trivial or the sign character depending on whether $\pi_p$ is the Steinberg representation or the unramified quadratic twist of the Steinberg representation.
(6) For $p = 2$, since $\sigma_2$ has conductor 2 ($\mathrm{ord}_2(N) = 2$), we have $\sigma_2^{R_2^\times} \neq 0$. Since $\pi_2$ is supercuspidal, we know that $\sigma_2$ is the unique 2-dimensional irreducible representation of $B_2^\times/R_2^\times\mathbb{Q}_2^\times \cong S_3$.

Let $\hat{R}^\times = (R \otimes \hat{\mathbb{Z}})^\times$. The following proposition follows immediately from the previous local description of $\sigma$.

**Proposition 3.13.**
*(1) The space of invariants* $\sigma_f^{\hat{R}^\times}$ *is 2-dimensional.*
*(2) For* $p \mid D$*,* $W_p \cong \mathbb{Z}/2\mathbb{Z} = \langle w_p \rangle$ *acts on* $\sigma_f^{\hat{R}^\times}$ *via 2 copies of the character*

$$w_p \mapsto \left(\frac{-1}{p}\right)\varepsilon_p(E/\mathbb{Q}).$$

*(3) For* $p = 2$*,* $W_2 \cong S_3$ *acts on* $\sigma_f^{\hat{R}^\times}$ *via the unique 2-dimensional representation of* $S_3$*.*

3.14. **Shimura curves and Heegner points.** Let $\mathcal{H}^\pm = \mathbb{C} - \mathbb{R}$ be the union of the upper and lower half plane. Associated to the order $R$ we have a Shimura curve

$$X = R^\times \backslash \mathcal{H}^\pm,$$

where $R^\times$ acts on $\mathcal{H}^\pm$ via an embedding $R^\times \hookrightarrow (B \otimes \mathbb{R})^\times \cong \mathrm{GL}_2(\mathbb{R})$. Let $T/\mathbb{Q}$ be the maximal torus in $B^\times$ induced by the natural embedding $\mathbb{Z}[i] \hookrightarrow R$ (so $T$ is split by $\mathbb{Q}(i)$). Let $M$ be the $\mathrm{GL}_2(\mathbb{R})$-conjugates of the natural homomorphism $h_0 : T(\mathbb{R}) = \mathbb{C}^\times \hookrightarrow \mathrm{GL}_2(\mathbb{R})$, then $M \cong \mathcal{H}^\pm$ and $h_0$ is naturally identified with $i \in \mathcal{H}^+$. The Shimura curve $X$ has the adelic description

$$X \cong B^\times(\mathbb{Q}) \backslash M \times B^\times(\mathbb{A}_f)/\hat{R}^\times. \tag{3.2}$$

It is a well-known fact due to Shimura [Shi67] that the points of $X$ classify abelian surfaces together with endomorphisms by $R$ and this moduli interpretation provides the Shimura curve $X$ with a canonical smooth projective model over $\mathbb{Q}$.

*Remark* 3.15. Shimura curves associated to Eichler orders are well studied before. Let $Y$ be the Shimura curve associated to the Eichler order $S$ (Remark 3.12). Then the natural covering map $X \to Y$ has degree $[S_2^\times : R_2^\times] = [\mathbb{F}_4^\times : \mathbb{F}_2^\times] = 3$.

**Definition 3.16.** Let $K/\mathbb{Q}$ be an imaginary quadratic field with an embedding $\tau : \mathcal{O}_K \hookrightarrow R$. Then the induced homomorphism $h : (K \otimes \mathbb{R})^\times = \mathbb{C}^\times \hookrightarrow (B \otimes \mathbb{R})^\times \cong \mathrm{GL}_2(\mathbb{R})$ corresponds to a point $y_K$ on $X$, known as a *Heegner point*. Notice that $y_K$ depends on the choice of the embedding $\tau$. In terms of the moduli interpretation, $y_K$ corresponds to an abelian surface which is isomorphic to a product of two elliptic curves with complex multiplication by $\mathcal{O}_K$. By the theory of complex multiplication, $y_K$ is defined over the Hilbert class field of $K$.

We specialize to the case $K = \mathbb{Q}(i)$ and the natural embedding

$$\tau : \mathcal{O}_K = \mathbb{Z}[i] \hookrightarrow R = \mathbb{Z} + \mathbb{Z}i + \mathbb{Z}j + \mathbb{Z}ij.$$

The associated Heegner point $y_K$ is represented by the point $[h_0, 1]$ under the double quotient (3.2) and it is $K$-rational since $K$ has class number one.

The finite group $W = \prod_{p \mid 4D} W_p$ acts on $X$ as automorphisms defined over $\mathbb{Q}$. The generator $w_p$ of $W_p$ for $p \mid D$ are known as the *Atkin–Lehner involution*.

**Proposition 3.17.** *Let* $w = \prod_{p \mid D} w_p \in W$*. Then* $w(y_K) = \overline{y_K}$*, the complex conjugate of* $y_K$*.*

*Proof.* In view of the moduli interpretation, the point $\overline{y_K}$ corresponds to the complex conjugate embedding $\bar{\tau} : \mathbb{Z}[i] \hookrightarrow R$ of $\tau$. Since $jij^{-1} = -i$, we know that conjugating $\tau$ by $j \in B^\times$ gives $\bar{\tau}$ and thus $jy_K = \overline{y_K}$. On the other hand, the reduced norm of $j^2$ is $-D$, so we see that

$$jR_p^\times \mathbb{Q}_p^\times / R_p^\times \mathbb{Q}_p^\times = \begin{cases} w_p, & p \mid D, \\ 1, & p \nmid D. \end{cases}$$

It follows that $jy_K = j[h_0, 1] = [h_0, w] = w(y_K)$. We conclude that $w(y_K) = \overline{y_K}$. □

**Proposition 3.18.** *Each point in the set* $W(y_K) = \{\sigma(y_K), \sigma \in W\}$ *has a stabilizer of order 2 (contained in* $W_2$*) under the action of* $W$*. In particular,* $W(y_K)$ *has size* $3 \cdot 2^{\#\{p|D\}}$ *and* $W_2(y_K)$ *has size* 3.

*Proof.* The stabilizer of $y_K = [h_0, 1]$ under the action of $B^\times$ is $T(\mathbb{Q}) = \mathbb{Q}(i)^\times \subseteq B^\times$. Since $\mathbb{Q}(i)$ is unramified at $p \neq 2$, it follows that for $p \neq 2$, $\mathbb{Q}_p(i)^\times R_p^\times / R_p^\times \mathbb{Q}_p^\times = \{1\}$ and thus $W_p$ acts on $W(y_K)$ freely. For $p = 2$, $\mathbb{Q}(i)$ is ramified at 2 and $\mathbb{Q}_2(i)^\times R_2^\times / R_2^\times \mathbb{Q}_2^\times \cong \mathbb{Z}/2\mathbb{Z}$ is generated by the class of a uniformizer of $\mathbb{Q}_2(i)$. So $W_2$ acts on $y_K$ with a stabilizer of order 2. □

3.19. **Uniformization by Shimura curves.** Let $J_X = \mathrm{Jac}(X)$ be the Jacobian of $X$ and $H = \mathrm{Hom}_{\mathbb{Q}}(J_X, E)$ be the group of homomorphisms (defined over $\mathbb{Q}$) from $J_X$ to $E$, then $W$ acts on $J_X$ and $H$. Notice that $H$ is a free abelian group and by [YZZ13, §3.2.3], we have

$$H \otimes \mathbb{C} \cong \sigma_f^{\hat{R}^\times},$$

as $W_2 \cong S_3$-representations. We know from Proposition 3.13 that $\sigma_f^{\hat{R}^\times}$ is the irreducible 2-dimensional representation of $S_3$, thus $H$ is a free abelian group of rank 2. In particular, the elliptic curve $E$ is uniformized by the Shimura curve $X$, in *two independent ways* which cannot be distinguished from each other.

3.20. **Heegner points on elliptic curves.** Let $D^0$ be the free abelian group of degree 0 divisors supported on the $K$-rational points $W(y_K)$. The following theorem shows that the image of these divisors under the projection maps $J_X \to E$ lies in the desired subgroup $E^-(\mathbb{Q})$ of $E(\mathbb{Q}(i))$.

**Theorem 3.21.** *Let* $d \in D^0$ *and* $\phi \in H$*. Then* $\phi(d) \in E^-(\mathbb{Q}) \subseteq E(\mathbb{Q}(i))$.

*Proof.* For any $d \in D^0$, it follows from Proposition 3.17 that $wd = \overline{d}$. Therefore

$$\overline{\phi(d)} = \phi(\overline{d}) = \phi(\sigma d) = \phi^\sigma(d) = w(\phi)(d).$$

By Proposition 3.13, this is equal to

$$\prod_{p|D} \left(\frac{-1}{p}\right) \varepsilon_p(E/\mathbb{Q}) \cdot \phi(d).$$

But $\varepsilon_2(E/\mathbb{Q}) = -1$ and $\prod_{p|D} \left(\frac{-1}{p}\right) = -1$ since $D \equiv 3 \pmod 4$, we obtain that

$$\overline{\phi(d)} = -\varepsilon(E/\mathbb{Q}) \cdot \phi(d).$$

Hence $\overline{\phi(d)} = \phi(d)$ if and only if $\varepsilon(E/\mathbb{Q}) = -1$. In other words, the image lies in $E^-(\mathbb{Q})$. □

The pairing between two free abelian groups

$$\langle \ , \ \rangle : H \times D^0 \to E(\mathbb{Q}(i)), \quad \langle \phi, d \rangle = \phi(d)$$

is bilinear and satisfies $\langle \phi^\sigma, d \rangle = \langle \phi, \sigma d \rangle$ for any $\sigma \in W$. Hence it induces a map

$$H \otimes_{\mathbb{Z}[W]} D^0 \to E(\mathbb{Q}(i)),$$

whose image lies in $E^-(\mathbb{Q})$ by Theorem 3.21.

3.22. **A canonical rational point.** We now use the extra automorphisms in $W_2$ to produce a canonical (up to sign) rational point $P$ in $E^-(\mathbb{Q})$. Let $D_2^0 \subseteq D^0$ be the subgroup of divisors supported on the set of three points $W_2(y_K)$.

**Theorem 3.23.** *$H \otimes_{\mathbb{Z}[W_2]} D_2^0$ is a free abelian group of rank one.*

*Proof.* There are two possibilities for the integral $S_3$-representation $H$: it is either the $A_2$-lattice

$$A_2 = \{a_1e_1 + a_2e_2 + a_3a_3 : \sum a_i = 0\} \subseteq \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3$$

or its dual

$$A_2^\vee = \mathrm{Hom}(A_2, \mathbb{Z}) = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3/\mathbb{Z}(e_1 + e_2 + e_3),$$

where $S_3$ permutes the basis vectors $\{e_1, e_2, e_3\}$ in the natural way. On the other hand, by Proposition 3.18, $W_2(y_K)$ consists of three points. Hence as a $W_2 \cong S_3$-representation, $D_2^0$ is isomorphic to the $A_2$-lattice.

If $H = A_2^\vee$, then the natural pairing between $A_2$ and $A_2^\vee$ induces an isomorphism

$$H \otimes_{\mathbb{Z}[W_2]} D_2^0 \cong A_2 \otimes_{\mathbb{Z}[S_3]} A_2^\vee \cong \mathbb{Z}.$$

It remains to check that the case $H = A_2$, i.e., it remains to show that

$$A_2 \otimes_{\mathbb{Z}[S_3]} A_2 \cong \mathbb{Z}.$$

Since $A_2$ is freely generated by the two vectors $u = e_1 - e_2$ and $v = e_2 - e_3$, it suffices to check that $u \otimes u$, $v \otimes v$, $u \otimes v$ and $v \otimes u$ in $A_2 \otimes_{\mathbb{Z}[S_3]} A_2$ generate a free abelian group of rank one. In fact, we have

$$u \otimes u = (e_1 - e_2) \otimes (e_1 - e_3 + e_3 - e_2) = \sigma_{12}(e_1 - e_2) \otimes \sigma_{12}(e_1 - e_3) - u \otimes v = -2u \otimes v,$$

$$v \otimes v = (e_2 - e_3) \otimes (e_2 - e_3) = \sigma_{13}(e_2 - e_3) \otimes \sigma_{13}(e_2 - e_3) = u \otimes u,$$

and

$$u \otimes v = (e_1 - e_2) \otimes (e_2 - e_3) = \sigma_{13}(e_1 - e_2) \otimes \sigma_{13}(e_2 - e_3) = v \otimes u,$$

where $\sigma_{ij} \in S_3$ denotes the transposition switching $e_i$ and $e_j$. It follows that

$$v \otimes v = u \otimes u = -2u \otimes v, \quad v \otimes u = u \otimes v,$$

and thus $A_2 \otimes_{\mathbb{Z}[S_3]} A_2$ is freely generated on one element $u \otimes v$. □

Finally, we define our desired canonical rational point $P \in E^-(\mathbb{Q})$ to be the image of the generator (up to sign) of $H \otimes_{\mathbb{Z}[W_2]} D_2^0$.

## 4. A conjecture on the canonical point $P$

In view of Conjecture 3.8, we propose the following conjecture.

**Conjecture 4.1.** *If the 2-rank of* $\mathrm{Cl}(L)$ *is at most 1, then* $P \in E^-(\mathbb{Q})$ *has infinite order.*

We now verify this conjecture for an explicit example.

**Example 4.2.** Consider the case $D = 11$. The Shimura curve $X$ associated to the quaternion order of discriminant 44 has genus 2. The Shimura curve $Y$ associated to the maximal order of discriminant 22 has genus 0. The degree 3 map $X \to Y$ (Remark 3.15) is ramified at the 4 elliptic points of order 3 on $Y$. Elkies in 2007 computed the elliptic points of $Y$ (see [Elk08] for his method). We can then deduce that $X$ has equation

$$-y^2 = x^6 - 7x^4 + 59x^2 + 11$$

and the three elliptic points in $W_2(y_K)$ are $\infty$, $(1,8i)$ and $(-1,8i)$ . The Jacobian $J_X$ is $(2,2)$-isogenous to $E\times\tilde{E}$, where

$$E=44a1: y^2=x^3+7x^2+59x-11,\quad \tilde{E}=44a2: y^2=x^3-59x^2-77x-121,$$

and the map $J_X\to E\times\tilde{E}$ is induced from the two maps

$$X\to E,\quad (x,y)\mapsto(-x^2,y),\qquad X\to\tilde{E},\quad (x,y)\mapsto\left(-\frac{11}{x^2},\frac{11y}{x^3}\right).$$

The two elliptic curves $E,\tilde{E}$ are 3-isogenous to each other and we see that $\mathrm{Hom}_{\mathbb{Q}}(J_X,E)$ is indeed of rank 2. The cubic field $L$ has discriminant $-44$ and class number $h_L=1$. The root number $\varepsilon(E/\mathbb{Q})=+1$. The quadratic twist of $E$ by $\mathbb{Q}(i)$ has equation

$$E^-=176c1: y^2=x^3-7x^2+59x+11.$$

As predicted by Conjecture 3.8, we have $r_{\mathrm{alg}}(E^-/\mathbb{Q})=1$. As predicted by Conjecture 4.1, the canonical point $P=(1,8)\in E^-(\mathbb{Q})$ we constructed is indeed a point of infinite order, generating a subgroup of index 2 in $E^-(\mathbb{Q})$.

## 5. A mod 2 congruence between elliptic curves and Artin representations

5.1. **A mod 2 congruence.** The mod 2 Galois representation $\bar{\rho}=\bar{\rho}_{E,2}: G_{\mathbb{Q}}\to\mathrm{GL}_2(\mathbb{F}_2)\cong S_3$ can also be viewed as a 2-dimensional irreducible Artin representation $\sigma$ via an embedding $S_3\hookrightarrow\mathrm{GL}_2(\mathbb{C})$. This Artin representation $\sigma$ has dihedral image and thus is induced from the imaginary quadratic field $K=\mathbb{Q}(\sqrt{-D})$. Then $\sigma$ is associated to a *weight one* newform with nebentypus the quadratic character $\varepsilon_K$, which is a Hecke theta series associated to $K$. On the other hand, there is a *weight two* newform $f$ with trivial nebentypus associated to the elliptic curve $E$ by the modularity theorem. By construction we have a congruence $f\equiv h \pmod 2$.

**Example 5.2** (cf. [Ser77, 7.3])**.** Consider the elliptic curve

$$E=92a1: y^2=F(x)=x^3+x^2+2x+1.$$

The polynomial $F(x)$ is irreducible and has square-free and negative discriminant $-D=-23$ and thus Assumption 2.1 holds. The elliptic curve $E$ has discriminant $\Delta=-2^4\cdot 23$, conductor $N=2^2\cdot 23$. The cubic field

$$L=\mathbb{Q}[x]/(x^3+x^2+2x+1)$$

has discriminant $d_L=-23$, hence the Artin representation $\sigma$ has conductor $N(\sigma)=23$. The class number of $L$ is 1 and we have $s_2(E/\mathbb{Q})=0$ as predicted by Theorem 2.18.

The the relevant Hecke character can be viewed as an order 3 character on the ideal class group $\mathrm{Cl}(K)$. We remark that $K$ is the cubic field of *smallest* (in the sense of the absolute value) discriminant with class number 3. The three ideal classes in $\mathrm{Cl}(K)$ are represented by the three integral binary quadratic forms of discriminant $d_K=-23$,

$$x^2+xy+6y^2,\quad 2x^2\pm xy+3y^2,$$

of order 1 and 3 respectively. We find that $h(z)$ is the following simple linear combination of theta series associated to these quadratic forms:

$$\begin{aligned} h(z) &= \frac{1}{2}\left(\sum_{m,n\in\mathbb{Z}} q^{m^2+mn+6n^2} - \sum_{m,n\in\mathbb{Z}} q^{2m^2+mn+3n^2}\right) \\ &= q - q^2 - q^3 + q^6 + q^8 - q^{13} - q^{16} + q^{23} - q^{24} + q^{25} \\ &\quad + q^{26} + q^{27} - q^{29} - q^{31} + q^{39} - q^{41} - q^{46} - q^{47} + q^{48} + q^{49} - q^{50} \cdots \end{aligned}$$

We remark that $\sigma$ is the irreducible 2-dimensional Artin representation of *smallest* conductor ([Ser77, 8.1]). Moreover, $h(z)$ can be written as the classical eta product:

$$h(z) = \eta(z)\eta(23z) = q\prod_{n\geq 1}(1-q^n)(1-q^{23n}),$$

where

$$\eta(z) = q^{1/24}\prod_{n\geq 1}(1-q^n) = \sum_{n\geq 1}\left(\frac{12}{n}\right)q^{\frac{n^2}{24}}$$

is Dedekind's eta function.

The first few Hecke eigenvalues of the newforms $f(z) \in S_2(92)$ and $h(z) \in S_1(23, \varepsilon_{-23})$ are listed in Table 1. We see that $a_p \equiv b_p \pmod 2$ for $p \neq 2$.

| $p$ | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 | 47 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a_p(f)$ | 0 | 1 | 0 | 2 | 0 | $-1$ | $-6$ | 2 | $-1$ | $-3$ | 5 | 8 | 3 | 8 | 9 |
| $b_p(h)$ | $-1$ | $-1$ | 0 | 0 | 0 | $-1$ | 0 | 0 | 1 | $-1$ | $-1$ | 0 | $-1$ | 0 | $-1$ |

TABLE 1. $E = 92a1$

**Example 5.3.** Notice the above mod 2 congruence does not require the conductor of $E$ to be of the form $N = 4D$. Consider the elliptic curve

$$E = X_0(11) = 11a1 : y^2 + y = x^3 - x^2 - 10x - 20,$$

which has the *smallest* conductor 11 among all elliptic curves over $\mathbb{Q}$. It has discriminant $\Delta = -11$. The cubic field

$$L \cong \mathbb{Q}[x]/(x^3 - x^2 + x + 1)$$

has discriminant $d_L = -2^2\cdot 11$. Hence the Artin representation $\sigma$ has conductor $N(\sigma) = 2^2\cdot 11$.

The ring class group of the quadratic order of discriminant $-44$ in $K = \mathbb{Q}(\sqrt{-11})$ has order 3, represented by the three binary quadratic form of discriminant $-44$,

$$2x^2 + 11y^2, \quad 3x^2 \pm 2xy + 4y^2$$

of order 1 and 3 respectively. We find that $h(z)$ is the following simple linear combination of theta series associated to these quadratic forms:

$$\begin{aligned} h(z) &= \frac{1}{2}\left(\sum_{m,n\in\mathbb{Z}} q^{2m^2+11n^2} - \sum_{m,n\in\mathbb{Z}} q^{3m^2+2mn+4n^2}\right) \\ &= q - q^3 - q^5 + q^{11} + q^{15} - q^{23} + q^{27} - q^{31} - q^{33} - q^{37} + 2q^{47} + q^{49} + \cdots \end{aligned}$$

Moreover, $h(z)$ is the classical eta product

$$h(z) = \eta(2z)\eta(22z) = q \prod_{n\geq 1}(1-q^{2n})(1-q^{22n}).$$

The newform $f(z) \in S_2(11)$ is also a classical eta product

$$\begin{aligned} f(z) = \eta^2(z)\eta^2(11z) &= q \prod_{n\geq 1}(1-q^n)^2(1-q^{11n})^2 \\ &= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} \\ &\quad + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + 2q^{20} + 2q^{21} - 2q^{22} \\ &\quad - q^{23} - 4q^{25} - 8q^{26} + 5q^{27} - 4q^{28} + 2q^{30} + 7q^{31} + 8q^{32} - q^{33} \\ &\quad + 4q^{34} - 2q^{35} - 4q^{36} + 3q^{37} - 4q^{39} - 8q^{41} - 4q^{42} - 6q^{43} + 2q^{44} \\ &\quad - 2q^{45} + 2q^{46} + 8q^{47} + 4q^{48} - 3q^{49} + 8q^{50} \cdots \end{aligned}$$

The first few Hecke eigenvalues of the newforms $f(z) \in S_2(11)$ and $h(z) \in S_1(44, \varepsilon_{-44})$ are listed in Table 2. We see that $a_p \equiv b_p \pmod 2$ for all $p$ (which one can also see directly from the eta products above):

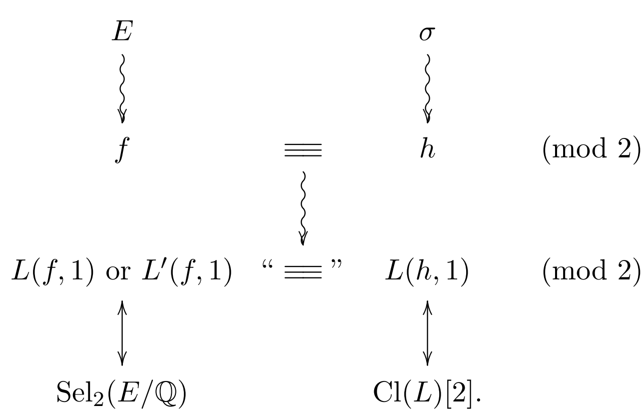
| $p$ | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 | 31 | 37 | 41 | 43 | 47 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $a_p(f)$ | $-2$ | $-1$ | 1 | $-2$ | 1 | 4 | $-2$ | 0 | $-1$ | 0 | 7 | 3 | $-8$ | $-6$ | 8 |
| $b_p(h)$ | 0 | $-1$ | $-1$ | 0 | 1 | 0 | 0 | 0 | $-1$ | 0 | $-1$ | $-1$ | 0 | 0 | 2 |

TABLE 2. $E = 11a1$

5.4. **An interpretation of Theorem 1.4.** Under the BSD conjecture, Theorem 1.4 can be interpreted as a mod 2 congruence between (suitably defined algebraic parts of) the special values of $L$-functions of these two modular forms $f$ and $h$ (of different weights!):

- the 2-part of $L(f,1)$ or $L'(f,1)$ (depending on the sign) is related to $s_2(E/\mathbb{Q})$ by the BSD formula;
- the 2-part of $L(h,1)$ is related to the 2-part of the ideal class group $\mathrm{Cl}(L)$ by the class number formula, since $L(h,s) = \zeta_L(s)/\zeta(s)$ is the quotient of the Dekind zeta function of $L$ by the Riemann zeta function.

We depict this as follows.



We find this mod 2 congruence rather unusual: $L(E,s)$ is of symplectic type with the sign of the functional equation $\pm 1$ whereas the Artin $L$-function $L(\sigma,s)$ is of orthogonal type with the sign of the functional equation always $+1$. Congruences of this type is unique to $p=2$. As B. Mazur pointed out to us, this may suggest something much more general with intersections mod 2 of 2-adic eigenvarieties of different (symplectic versus orthogonal) reductive groups. Also, the point $s=1$ is the central critical point for $L(E,s)$ but there is *no* critical point for $L(\sigma,s)$ in the sense of Deligne, which makes even the formulation of the congruences more subtle.

We hope to formulate this type of mod 2 congruence between $L$-values more precisely in the future, which may shed light on Conjecture 1.9 by producing a direct mod 2 congruence between Heegner points on $E$ and the class group of $L$.

## References


[AB04] M. Alsina and P. Bayer, *Quaternion orders, quadratic forms, and Shimura curves*, volume 22 of *CRM Monograph Series*, American Mathematical Society, Providence, RI, 2004.

[BDP13] M. Bertolini, H. Darmon and K. Prasanna, *Generalized Heegner cycles and $p$-adic Rankin $L$-series*, Duke Math. J. **162**(6), 1033–1148 (2013), With an appendix by Brian Conrad.

[BK77] A. Brumer and K. Kramer, *The rank of elliptic curves*, Duke Math. J. **44**(4), 715–743 (1977).

[BSZ14] M. Bhargava, C. Skinner and W. Zhang, *A majority of elliptic curves over $\mathbb{Q}$ satisfy the Birch and Swinnerton-Dyer conjecture*, ArXiv e-prints (July 2014), 1407.1826.

[CCL16] L. Cai, Y. Chen and Y. Liu, *Heegner Points on Modular Curves*, ArXiv e-prints (January 2016), 1601.04415.

[CW15] F. Castella and X. Wan, *Iwasawa Main Conjecture for Heegner Points: Supersingular Case*, ArXiv e-prints (June 2015), 1506.02538.

[DD08] T. Dokchitser and V. Dokchitser, *Root numbers of elliptic curves in residue characteristic 2*, Bull. Lond. Math. Soc. **40**(3), 516–524 (2008).

[Dok13] T. Dokchitser, Notes on the Parity Conjecture, in *Elliptic Curves, Hilbert Modular Forms and Galois Deformations*, pages 201–249, Springer, 2013.

[Elk08] N. D. Elkies, Shimura curve computations via $K3$ surfaces of Néron-Severi rank at least 19, in *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 196–211, Springer, Berlin, 2008.

[GP12] B. H. Gross and J. A. Parson, On the local divisibility of Heegner points, in *Number theory, analysis and geometry*, pages 215–241, Springer, New York, 2012.

[GZ86] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of $L$-series*, Invent. Math. **84**(2), 225–320 (1986).

[KL16] D. Kriz and C. Li, *Congruences between Heegner points and quadratic twists of elliptic curves*, ArXiv e-prints (June 2016), 1606.03172.

[KMR13] Z. Klagsbrun, B. Mazur and K. Rubin, *Disparity in Selmer ranks of quadratic twists of elliptic curves*, Ann. of Math. (2) **178**(1), 287–320 (2013).

[KMR14] Z. Klagsbrun, B. Mazur and K. Rubin, *A Markov model for Selmer ranks in families of twists*, Compos. Math. **150**(7), 1077–1106 (2014).

[KP15] D. Kohen and A. Pacetti, *On Heegner Points for primes of additive reduction ramifying in the base field*, ArXiv e-prints (May 2015), 1505.08059.

[Li15] C. Li, *2-Selmer groups and Heegner points on elliptic curves*, ProQuest LLC, Ann Arbor, MI, 2015, Thesis (Ph.D.)–Harvard University.

[LRd16] M. Longo, V. Rotger and C. de Vera-Piquero, *Heegner points on Hijikata-Pizer-Shemanske curves*, ArXiv e-prints (March 2016), 1603.03554.

[LZZ14] Y. Liu, S.-W. Zhang and W. Zhang, *On $p$-adic Waldspurger formula*, Preprint (2014), `http://www.math.northwestern.edu/~liuyf/logarithm.pdf`.

[Mon96] P. Monsky, *Generalizing the Birch-Stephens theorem. I. Modular curves*, Math. Z. **221**(3), 415–420 (1996).

[MR10] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181**(3), 541–575 (2010).

[S+13] W. Stein et al., *Sage Mathematics Software (Version 5.11)*, The Sage Development Team, 2013, `http://www.sagemath.org`.

[Sch96] E. F. Schaefer, *Class groups and Selmer groups*, J. Number Theory **56**(1), 79–114 (1996).

[Ser72] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15**(4), 259–331 (1972).

[Ser77] J.-P. Serre, Modular forms of weight one and Galois representations, in *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 193–268, Academic Press, London, 1977.

[Shi67] G. Shimura, *Construction of class fields and zeta functions of algebraic curves*, Ann. of Math. (2) **85**, 58–159 (1967).

[Sil94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1994.

[Sil09] J. H. Silverman, *The Arithmetic of Elliptic Curves (Graduate Texts in Mathematics)*, Springer, 2nd edition, 5 2009.

[Ski14] C. Skinner, *A converse to a theorem of Gross, Zagier, and Kolyvagin*, ArXiv e-prints (May 2014), 1405.7294.

[Smi17] A. Smith, *$2^\infty$-Selmer groups, $2^\infty$-class groups, and Goldfeld's conjecture*, ArXiv e-prints (February 2017), 1702.02325.

[SZ14] C. Skinner and W. Zhang, *Indivisibility of Heegner points in the multiplicative case*, ArXiv e-prints (July 2014), 1407.1099.

[Ven16] R. Venerucci, *On the p-converse of the Kolyvagin-Gross-Zagier theorem*, Comment. Math. Helv. **91**(3), 397–444 (2016).

[Wan14] X. Wan, *Heegner Point Kolyvagin System and Iwasawa Main Conjecture*, ArXiv e-prints (August 2014), 1408.4043.

[YZZ13] X. Yuan, S.-W. Zhang and W. Zhang, *The Gross-Zagier formula on Shimura curves*, volume 184 of *Annals of Mathematics Studies*, Princeton University Press, Princeton, NJ, 2013.

[Zha14] W. Zhang, *Selmer groups and the indivisibility of Heegner points*, Camb. J. Math. **2**(2), 191 – 253 (2014).

*E-mail address*: `chaoli@math.columbia.edu`

Department of Mathematics, Columbia University, 2990 Broadway, New York, NY 10027