QUADRATIC TWISTS OF GENUS ONE CURVES AND DIOPHANTINE QUINTUPLES

MATIJA KAZALICKI

Abstract. Motivated by the theory of Diophantine $m$-tuples, we study rational points on quadratic twists $H^d : dy^2 = (x^2 + 6x - 18)(-x^2 + 2x + 2)$, where $|d|$ is a prime. If we denote by $S(X) = \{ d \in \mathbb{Z} : H^d(\mathbb{Q}) \neq \emptyset, |d| \text{ is a prime and } |d| < X \}$, then, by assuming some standard conjectures about the ranks of elliptic curves in the family of quadratic twists, we prove that as $X \to \infty$

$$\frac{43}{256} + o(1) \leq \frac{\#S(X)}{2\pi(X)} \leq \frac{46}{256} + o(1).$$

1. Introduction

For an integer $d$, a set of $m$ distinct nonzero rational numbers with the property that the product of any two of its distinct elements plus $d$ is a square is called a rational Diophantine $m$-tuple with the property $D(d)$ or $D(d)$-m-tuple. The $D(1)$-m-tuples (with rational elements) are called simply rational Diophantine $m$-tuples and have been studied since ancient times, starting with Diophantus, Fermat, and Euler.

It is not known how large can a rational Diophantine tuple be. Dujella, Kazalicki, Mikić, and Szikszai [DKMS17] proved that there are infinitely many rational Diophantine sextuples, while no example of a rational Diophantine septuple is known. Also, no example of rational $D(d)$-sextuple is known if $d$ is not a perfect square. For more information on Diophantine $m$-tuples see the survey article [Duj16].

We are interested in the following question.

Question. Does there exist a rational $D(d)$-quintuple for every $d \in \mathbb{Z}$?

Dujella and Fuchs [DF12] proved that there are infinitely many squarefree integers $d$'s for which there are infinitely many rational $D(d)$-quintuples, and Dražić [Dra22] (improving the similar result from [DF12]) proved, assuming the Parity conjecture for the quadratic twists of several explicitly given elliptic curves, that for at least 99.5% of squarefree integers $d$ there are infinitely many rational $D(d)$-quintuples.

Following an idea from [DF12], we start with a $D(\frac{16}{9} x^2(x^2 - x - 3)(x^2 + 2x - 12))$-quintuple in $\mathbb{Z}[x]$

$$\left\{ \frac{1}{3}(x^2 + 6x - 18)(-x^2 + 2x + 2), \frac{1}{3}x^2(x + 5)(-x + 3), (x - 2)(5x + 6), \frac{1}{3}(x^2 + 4x - 6)(-x^2 + 4x + 6), 4x^2 \right\}$$

found by Dujella [Duj99] (and used to prove that there are infinitely many $D(-1)$-quintuples in [Duj02]). Note that for rational $u \neq 0$, if $\{a, b, c, d, e\}$ is $D(qu^2)$-quintuple, then $\{\frac{b}{u}, \frac{c}{u}, \frac{d}{u}, \frac{e}{u}\}$ is $D(q)$-quintuple. In particular, for squarefree integer $d$, if

$$dy^2 = (x^2 - x - 3)(x^2 + 2x - 12)$$

for some $x, y \in \mathbb{Q}$ then by dividing the elements of quintuple above with $\frac{4}{9}xy$ we obtain $D(d)$-quintuple. Thus, if the equation above has infinitely many solution, we may conclude that there are infinitely many $D(d)$-quintuples.

2010 Mathematics Subject Classification. 14H52, 11G05.

Key words and phrases. elliptic curves, quadratic twists, Selmer groups.
Consider the genus one quartic \[ H : \quad y^2 = (x^2 - x - 3)(x^2 + 2x - 12). \]
For a squarefree integer \( d \), we denote by \( H^d : dy^2 = f(x) \) the quadratic twist of \( H \) with respect to \( \mathbb{Q}(\sqrt{d}) \). Quartic \( H \), as a (singular) genus one curve with a rational point at infinity, is birationally equivalent to the elliptic curve \( E / \mathbb{Q} \)
\[ E : y^2 = (x - 9)(x - 8)(x + 18). \]
Likewise, we denote by \( E^d \) the quadratic twist of \( E \) by \( \mathbb{Q}(\sqrt{d}) \). Thus \( H^d(\mathbb{Q}) \neq \emptyset \) implies that \( H^d \) is birationally equivalent to \( E^d \). Since, by Proposition 3.4, \( H^d(\mathbb{Q}) \neq \emptyset \) implies that \( H^d(\mathbb{Q}) \) is infinite and consequently that there are infinitely many \( D(d) \)-quintuples, we are led to the study of squarefree integers \( d \) for which \( H^d(\mathbb{Q}) \neq \emptyset \).

In this paper we will focus on twists by \( \mathbb{Q}(\sqrt{d}) \) where \( |d| \) is a prime. Let
\[ S = \{ d \in \mathbb{Z} : H^d(\mathbb{Q}) \neq \emptyset \text{ and } |d| \text{ is a prime} \}. \]

**Question.** What is asymptotically the size of set \( S(X) = \{ d \in S : |d| < X \} \) as \( X \to \infty \)?

Surprisingly, and in contrast with the analogous problem for the quadratic twists of elliptic curves, not much is known about this question.

Çiperian and Ozman gave a criterion for the set of rational points of the quadratic twist of quartic to be non-empty in terms of the image of the global trace map \( tr_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}} \) on an elliptic curve (see Section 2 of [cO15]), but in general, no estimates for the size of set \( S(X) \) are known.

For a squarefree \( d \), the quartic \( H^d \), as a \( 2 \)-covering of \( E^d \), represents an element of \( Sel^2(E^d) \), the \( 2 \)-Selmer group of \( E^d \), provided that \( H^d \) is everywhere locally solvable (i.e. \( H^d(\mathbb{Q}_v) \neq \emptyset \) for all places \( v \) – we write ELS for short). For the interpretation of Selmer group elements as 2-coverings of \( E \) see Section 1.2 of [Sto12].

If \( |d| = p \) is a prime, then Proposition 2.4 implies that \( H^d \) is ELS if and only if \( \left( \frac{p}{d} \right) = 1 \) or \( p = 13 \). Thus, for such \( d \), \( H^d(\mathbb{Q}) = \emptyset \) if and only if \( H^d \) represents a nontrivial element in \( III(E^d)[2] \) (where \( III(E^d) \) denotes the Tate-Shafarevich group of \( E^d \)), or more precisely, if and only if the image of \( H^d \) under the map \( \iota : Sel^2(E^d) \to III(E^d)[2] \) from the exact sequence
\[
0 \to E^d(\mathbb{Q})/2E^d(\mathbb{Q}) \to Sel^2(E^d) \to III(E^d)[2] \to 0
\]
is nonzero. In this case, we say that \( H^d \) represents the element of order two in \( III(E^d) \).

Our main tool for studying the image of \( H^d \) in \( III(E^d)[2] \) is the Cassels-Tate pairing on \( III(E^d) \) with values in \( \mathbb{Q}/\mathbb{Z} \), or more precisely, its extension to a pairing on 2-Selmer group by
\[
\langle \cdot , \cdot \rangle_{CT} : Sel^2(E^d) \times Sel^2(E^d) \to \mathbb{Z}/2\mathbb{Z} = \{0, 1\}.
\]
This pairing is bilinear, alternating, and non-degenerate on \( III(E^d)[2]/2III(E^d)[4] \), or equivalently, on \( Sel^2(E^d)/2Sel^4(E^d) \) (see Section 1). In particular, \( dim_{\mathbb{F}_2} III(E^d)[2]/2III(E^d)[4] \) is even, thus equal to 0 or 2 if \( |d| \) is a prime (see Proposition 3.1). Thus, if we find a class \( L \in Sel^2(E^d) \) such that \( \langle H^d, L \rangle_{CT} = 1 \), we can conclude that \( \iota(H^d) \neq 0 \), and, hence, that \( H^d \) represents the element of order two in \( III(E^d) \). If \( III(E^d)[2] \) is nontrivial and \( III(E^d)[2] = 2III(E^d)[4] \) (see Proposition 3.9), then we can not obtain any information about \( H^d \) using this method.

For estimating the asymptotic behaviour of \( \# S(X) \) as \( X \to \infty \) we will assume the following “standard” conjectures.

**Conjecture 1.** 100% of quadratic twists \( E^d \) where \( |d| \) is a prime have rank 0 or 1.

Note that this conjecture is now a theorem under the BSD conjecture if we let \( d \) range over all squarefree integers (see Smith [Smi22a,Smi22b]).
Conjecture 2 (The parity conjecture). For all $d \in \mathbb{Z}$ where $|d|$ is prime,

$$(-1)^{\text{rank}(E^d)} = w(E^d),$$

where $w(E^d)$ is the root number of the elliptic curve $E^d$.

It follows from Proposition 3.3 that the contribution of $d$’s ($|d|$ is a prime) for which the root number $w(E^d)$ is equal to 1 to the $\#S(X)$ is negligible since by Conjecture 1 100% of the curves $E^d$ will have rank 0 or 1 and by Conjecture 2 that rank is even, hence zero.

On the other hand, in the case $w(E^d) = -1$, if $\dim_{\mathbb{F}_2} \text{Sel}^{(2)}(E^d) = 3$ (see Proposition 3.3 for the description of $\text{Sel}^{(2)}(E^d)$) then by Conjecture 2 $\text{rank}(E^d) = 1$ so $\text{III}(E^d)[2]$ is trivial (note that $E^d$ has full rational two torsion, hence $\dim_{\mathbb{F}_2} \text{III}(E^d)[2] = \dim_{\mathbb{F}_2} \text{Sel}^{(2)}(E^d) - \text{rank}(E^d) - 2 = 0$).

Hence the only interesting case (in which we expect $\text{III}(E^d)[2]$ generically to be nontrivial) is when $\dim_{\mathbb{F}_2} \text{Sel}^{(2)}(E^d) = 5$ or equivalently (see Proposition 3.1) when $d \in T = T^+ \cup T^-$ where

$$T^+ = \{d > 0 : |d| \text{ is prime}, \left(\frac{d}{13}\right) = 1, \left(\frac{d}{3}\right) = 1, d \equiv 1 \pmod{8} \},$$

$$T^- = \{d < 0 : |d| \text{ is prime}, \left(\frac{d}{13}\right) = 1, \left(\frac{d}{2}\right) \cdot \left(\frac{d}{3}\right) = -1, d \equiv 5, 7 \pmod{8} \}.$$

Define

$$H_1 : y^2 = 4x^4 - 56x^2 + 169 \in \text{Sel}^{(2)}(E),$$

$$H_2 : y^2 = 18x^4 - 24x^3 - 32x^2 + 40x + 34 \in \text{Sel}^{(2)}(E),$$

$$F_1 : y^2 = 11x^4 + 12x^3 + 56x^2 + 24x + 68 \in \text{Sel}^{(2)}(E^{-1}),$$

$$F_2 : y^2 = x^4 + 56x^2 + 676 \in \text{Sel}^{(2)}(E^{-1}).$$

We show in Proposition 3.1 that if $d \in T$, $\text{Sel}^{(2)}(E^d)$ is generated by the image of the two torsion $E^d[2]$ under the Kummer map, $H^d$, and by the quadratic twists of those classes in (1.2) which land in $\text{Sel}^{(2)}(E^d)$. Hence for such $d$’s $\dim_{\mathbb{F}_2} \text{Sel}^{(2)}(E^d) = 5$. Proposition 2.3 describes when these twists of quartics in (1.2) are ELS. Note that this simple explicit description of $\text{Sel}^{(2)}(E^d)$ (see Proposition 3.1) is the main reason why we considered only quadratic twists by $d$ where $|d|$ is prime. In general for squarefree $d$, $\dim_{\mathbb{F}_2} \text{Sel}^{(2)}(E^d)$ is unbounded.

Assuming the parity conjecture for $E^d$, where $d \in T$, we can deduce that $\dim_{\mathbb{F}_2} \text{III}(E^d)[2] = 0$ or 2. Assume further that $\text{III}(E^d)[2] \neq 2\text{III}(E^d)[4]$. The non-degeneracy of the Cassels-Tate pairing implies that for $d$ such that $\iota(H^d) \neq 0$ there exists class $L \in \text{Sel}^{(2)}(E^d)$ (also with $\iota(L) \neq 0$) for which $\langle H^d, L \rangle_{CT} = 1$. The following theorem then follows easily from Section 4 Proposition 3.1 and the previous discussion.

**Theorem 1.1.** Let $d \in T$ such that $\text{III}(E^d)[2] \neq 2\text{III}(E^d)[4]$. Assuming the parity conjecture for $E^d$, the following is true.

a) If $d < 0$ and $d \equiv 1 \pmod{4}$ then $\langle H^d, F_1^{-d} \rangle_{CT} = 1$. In particular, $\iota(H^d) \neq 0 \in \text{III}(E^d)[2]$.  

b) If $d < 0$ and $d \equiv 3 \pmod{4}$ then $\iota(H^d) \neq 0$ if and only if $\langle H^d, F_2^{-d} \rangle_{CT} = 1$.  
c) If $d > 0$ then $\iota(H^d) \neq 0$ if and only if $\langle H^d, H_1^d \rangle_{CT} = 1$ or $\langle H^d, H_2^d \rangle_{CT} = 1$.

It remains to explain how to compute the Cassels-Tate pairing of the quadratic twists of quartics. To each pair $(A, B)$ of quartics from Table 1 (see (1.2)), by the work of Smith (see Theorem 3.2. in [Sm16]), we can associate the governing field $L_{A,B}$ such that the value of pairing $\langle A^d, B^d \rangle_{CT}$ is determined by $(A, B)_{CT}$ and the splitting behaviour of $d$ in $L_{A,B}$. For example, for $d \in T$, it follows that $\langle H^d, H_2^d \rangle_{CT} = 0$ if and only if $d$ splits completely in
$L = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{13})(\sqrt{4 + 2\sqrt{13}})$. For complete description of governing fields see Table 1 and Section 4. Section 4 and Proposition 3.9 imply the following corollary of Theorem 1.1.

| $(A^d, B^d)_{CT}$ | $K_{A,B}$ | $\alpha_{A,B}$ |
|------------------|-------------|----------------|
| $(H^d, H^d_1)_{CT}$ | $\mathbb{Q}(\sqrt{3}, \sqrt{13})$ | $4 + \sqrt{13}$ |
| $(H^d, H^d_2)_{CT}$ | $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{13})$ | $4 + 2\sqrt{13}$ |
| $(H^{-d}, F^{-d}_1)_{CT}$ | $\mathbb{Q}(\sqrt{-2}, \sqrt{13})$ | $-1$ |
| $(H^{-d}, F^{-d}_2)_{CT}$ | $\mathbb{Q}(\sqrt{13}, \sqrt{-1}, \sqrt{-3})$ | $3(1 + \sqrt{13})(3 + \sqrt{13})$ |
| $(H^{-d}, F^{-d}_3)_{CT}$ | $\mathbb{Q}(\sqrt{3}, \sqrt{-1}, \sqrt{2})$ | $8(1 + \sqrt{3})(4 + 2\sqrt{3})$ |
| $(H^{-d}, F^{-d}_4)_{CT}$ | $\mathbb{Q}(\sqrt{3}, \sqrt{-1}, \sqrt{2})$ | $8(1 + \sqrt{3})(4 + 2\sqrt{3})$ |

Table 1. For $d = p > 0$ which splits completely in $K_{A,B}$ (and in the case $(H^d, H^d_1)_{CT}$ we in addition require $p \equiv 1 \pmod{4}$), we have $(A^d, B^d)_{CT} = 0$ if and only if $d$ splits completely in field $L_{A,B} = K_{A,B}(\sqrt{\alpha_{A,B}})$.

Corollary 1.2. Let $d \in T$. Assuming the parity conjecture for $E^d$, if $d$ does not split completely in $L_{H_1, H_2} = L_{F_1, F_2}$ and

a) $d = -p < 0$ with $p \equiv 1 \pmod{4}$ and $p$ splits completely in $L_{H^{-1}, F_2}$, or

b) $d = p > 0$ and $p$ splits completely in $L_{H, H_1}$ and $L_{H, H_2}$,

then $H^d(\mathbb{Q}) \neq \emptyset$. Hence, for such $d$ there exists infinitely many $D(d)$-quintuples.

Remark 1.3. As we already noted, if for $d = \pm p$ we have that $(\frac{d}{13}) = 1$ and $(\frac{d}{2}) \cdot (\frac{d}{5}) \cdot (\frac{d}{13}) = 1$ (hence $w(E^d) = -1$ by Proposition 3.4), but if $d \not\equiv T$ (hence $\dim_{\mathbb{F}_2}\text{Sel}^{(2)}(E^d) = 3$), then by Conjecture 1.1 $\text{III}(E^d)$ [2] is trivial, and $H^d(\mathbb{Q}) \neq \emptyset$, so there exists infinitely many $D(d)$-quintuples.

Example 1.4. The set of $d \in T, |d| < 3000$, for which Corollary 1.2 implies that $H^d(\mathbb{Q}) \neq \emptyset$ is equal to

$$\{-2857, -2833, -1993, -601, -337, -313, 1993, 2833, 2857\}.$$ 

For $d = -313$, we find a point $(-2107/1202, 389073/1444804) \in H^{-313}(\mathbb{Q})$ which produces a $D(-313)$-quintuple

$$\{81062614477261, 15660515591, 9009021853, 28246175292437, 2532614 \}.$$ 

Remark 1.5. Results about infinite number of $D(d)$-quintuples obtained as above from $d \in T$ where $d < 0$ are new, they are not covered in [Dra22].

Using Chebotarev’s density theorem to determine the factorization of primes in governing fields, we obtain the following bounds for $S(X)$.

Corollary 1.6. Assuming Conjecture 1.1, we have that as $X \to \infty$

$$C_1 + o(1) \leq \frac{\#S(X)}{2\pi(X)} \leq C_2 + o(1),$$

where $C_1 = \frac{\sqrt{\pi}}{\pi} = \frac{43}{290}$ and $C_2 = \frac{46}{290}$. 

Remark 1.7. We can rephrase the result above by saying that the classes $H^d \in \text{Sel}^{(2)}(E^d)$, for $d \in T$, are “equidistributed” in the quotient $\text{Sel}^{(2)}(E^d)/\kappa(E^d[2]) - \{0\}$ with respect to the image of rational points $E^d(\mathbb{Q})$ (rank is generically 1) under the Kummer map $\kappa : E^d(\mathbb{Q})/2E^d(\mathbb{Q}) \to \text{Sel}^{(2)}(E^d)$, since we have that the probability for $H^d \in \kappa(E^d(\mathbb{Q}))/\kappa(E^d[2]) \subset \text{Sel}^{(2)}(E^d)/\kappa(E^d[2])$ is $1/7$. Recall that by Proposition 3.4 $H^d$ is never an element of $\kappa(E^d[2])$ (thus $1/7$ and not $1/8$ is the “right” answer).
By Proposition 2.3 and Conjecture 1 the density of $d$’s ($|d|$ is a prime) for which $\III(E^d)[2]$ is nontrivial and $\III(E^d)[2] = 2\III(E^d)[4]$ is $\frac{3}{2\pi^2}$, so with this method we can not bridge the gap between $C_1$ and $C_2$.

2. Local properties

**Proposition 2.1.** For a square-free $d \in \mathbb{Z}$, the quartic $H^d$ is everywhere locally solvable if and only if for all primes $p | d$ we have $\left( \frac{d}{p} \right) = 1$ or $p = 13$.

*Proof.* Assume that $H^d$ is ELS. It follows that for every prime $p | d$, $p \neq 13$, the equation $(x^2 - x - 3)(x^2 + 2x - 12) = 0$ has a solution in $\mathbb{F}_p$, which implies that $\left( \frac{p}{13} \right) = 1$ since the discriminant of quadratic factors is 13 and $4 \cdot 13$ respectively.

Conversely assume that for all primes $p | d$ we have $\left( \frac{d}{p} \right) = 0$ or 1. Obviously, $H^d(\mathbb{R}) \neq \emptyset$. If $p | d$, then by assumption there is a solution $(x^2 - x - 3)(x^2 + 2x - 12) = 0$ in $\mathbb{F}_p$ which lifts by Hensel lemma to $H^d(\mathbb{Q}_p)$. If $p \nmid 2 \cdot 3 \cdot 13d$, then $H^d$ has a good mod $p$ reduction since 2, 3 and 13 are only primes dividing discriminant of $(x^2 - x - 3)(x^2 + 2x - 12)$. It follows that $H^d/\mathbb{F}_p$ is a genus one curve, hence $H^d(\mathbb{F}_p) \neq \emptyset$, thus by Hensel’s lemma $H^d(\mathbb{Q}_p) \neq \emptyset$. It remains to consider cases $p = 2, 3, 13$ and $p \nmid d$. Here reductions mod 2, 3 and 13 of $H^d$ are geometrically irreducible genus zero curve, so it follows that $H^d(\mathbb{F}_p) \neq \emptyset$, and consequently $H^d(\mathbb{Q}_p) \neq \emptyset$ for $p = 2, 3, 13$. \hfill \square

**Remark 2.2.** Novak [Nov22] showed (assuming GRH) that asymptotically the number of square-free $d$’s, $0 < d < x$, for which $H^d$ is ELS is equal to

$$\frac{2\sqrt{273}}{13} \pi^{-3/2} \prod_p \left( 1 + \frac{1}{p} \right)^{\left( \frac{p}{13} \right)/2} \frac{x}{\sqrt{\log x}}.$$

Similarly, the following proposition describes local solvability of quartics from (1.2).

**Proposition 2.3.** Let $p$ be a prime and $d = \pm p$.

a) $H^d_1$ is everywhere locally solvable if and only if $d \equiv 1 \pmod{12}$ or $d = -3$.

b) $H^d_2$ is everywhere locally solvable if and only if $d > 0$ and $d \equiv 1 \pmod{8}$.

c) $F^d_1$ is everywhere locally solvable if and only if $d > 0$ and $d \equiv 1, 3 \pmod{8}$.

d) $F^d_2$ is everywhere locally solvable if and only if $d > 0$ and $d \equiv 1 \pmod{12}$.

The following proposition computes the root number of $E^d$.

**Proposition 2.4.** For $d = \pm p$ where $p \neq 2, 3, 13$ is a prime, the root number $w(E^d)$ is equal to $-1$ if and only if

$$\left( \frac{p}{2} \right) \cdot \left( \frac{p}{3} \right) \cdot \left( \frac{p}{13} \right) = 1.$$

Here $\left( \frac{p}{d} \right)$ is the Kronecker symbol for odd $d$ defined by

$$\left( \frac{d}{2} \right) = \begin{cases} 1, & \text{if } |d| \equiv 1, 7 \pmod{8} \\ -1, & \text{if } |d| \equiv 3, 5 \pmod{8}. \end{cases}$$

*Proof.* Theorem 1.1. in [Des20] implies that

$$w(E^d) = -w_2(E^d)w_3(E^d)w_{13}(E^d)\left( \frac{-1}{p} \right),$$

where $w_p(E^d)$ is a local root number at $p$ of $E^d$. Since $E^d$ has multiplicative reduction at 13, Proposition 2 in [Roh92] implies that $w_{13}(E^d) = -\left( \frac{b}{13} \right)$ where $b = 64108800d^3$, thus $w_{13} = -\left( \frac{b}{13} \right)$ (since $w_{13}(E^d) = -1$ if and only if the reduction is split multiplicative). Likewise, for $p \neq 3,
Proposition 3.1. For prime $p \neq 2, 3, 13$, let $d = \pm p$ be such that $\left(\frac{d}{13}\right) = 1$ and $w(d) = -1$.

a) If $d \in T$ (i.e. $d \equiv 1 \pmod{8}$ if $d > 0$ or $d \equiv 5, 7 \pmod{8}$ if $d < 0$), then $\dim_{\mathbb{F}_2} \text{Sel}^{(2)}(E^d) = 5$. More precisely, if $d > 0$, then $\text{Sel}^{(2)}(E^d)$ is generated by torsion classes, $H^d$, $H^d_1$ and $H^d_2$. If $d < 0$, then $\text{Sel}^{(2)}(E^d)$ is generated by torsion classes, $H^d$, $F^{-1}_1$, and $F^{-d}_2$ if $d \equiv 7 \pmod{8}$ or $H^d_1$ if $d \equiv 5 \pmod{8}$.

b) If $d \notin T$, then we have that $\dim_{\mathbb{F}_2} \text{Sel}^{(2)}(E^d) = 3$.

Since $E$ has full 2-torsion over $\mathbb{Q}$, each class in $H^1(\mathbb{Q}, E[2])$ can be identified with an element of $(\mathbb{Q}^2/\mathbb{Q}^2)^3$ in the following way. Denote by $P_1 = (8,0)$, $P_2 = (-18,0)$ and $P_3 = (9,0)$ nontrivial elements in $E[2]$, by $e_2 : E[2] \times E[2] \to \mu_2$ the Weil pairing (hence $e_2(P_i, P_j) = -1$ if and only if $i \neq j$), and by $\omega : E[2] \to \text{Hom}(E[2], \mu_2^*)$, $T \mapsto (P_i \mapsto e_2(T, P_i))$ the group homomorphism induced by $e_2$. For each class $F \in H^1(\mathbb{Q}, E[2])$, we denote by $\omega_*(F)$ the pushforward of $\omega$ from $H^1(\mathbb{Q}, E[2])$ to $H^1(\mathbb{Q}, \mu_2^3) \cong (\mathbb{Q}^2/\mathbb{Q}^2)^3$ where the last isomorphism is given by the Kummer map sending $\alpha \in \mathbb{Q}^2/\mathbb{Q}^2$ to $\xi \in H^1(\mathbb{Q}, \mu_2)$ such that $\xi(\sigma) = \frac{x^2}{\sqrt{\sigma}}$ for every $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. One has that $\omega_*(F) = (a_1, a_2, a_3)$ is equivalent to $F(\sigma) = \chi_{a_1}(\sigma)P_1 + \chi_{a_2}(\sigma)P_2$, for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and $a_1, a_2, a_3 \in \mathbb{Q}^2$, where, for $a \in \mathbb{Q}$. Here, we denote by $\chi_a$ the nontrivial character of $\mathbb{Q}(\sqrt{a})$ with values in $\mathbb{Z}/2\mathbb{Z}$ (if $\mathbb{Q}(\sqrt{a}) = \mathbb{Q}$ then $\chi_a$ is trivial). It follows that $F$ is defined over $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2})$.

We start with the following standard lemma.

Lemma 3.2. For elliptic curve $\tilde{E} : y^2 = (x - a_1)(x - a_2)(x - a_3)$, where $a_1, a_2, a_3 \in \mathbb{Q}$, let $F$ be a quartic $y^2 = g(x)$, $g(x) \in \mathbb{Z}[x]$, isomorphic (over $\overline{\mathbb{Q}}$) to $\tilde{E}$, which represents an element in $H^1(\mathbb{Q}, \tilde{E}[2])$ (the quartic is not necessarily everywhere solvable, i.e. the element of the 2-Selmer group). For $d \in \mathbb{Z}$ let $E^d$ be the quadratic twist of $F$, thus representing the element in $H^1(\mathbb{Q}, E^d[2])$. After identifying $H^1(\mathbb{Q}, \tilde{E}[2]) \cong H^1(\mathbb{Q}, E^d[2])$, we have

$$\omega_*(F) = \omega_*(F^d).$$

Proof. The claim follows directly from the interpretation of the map $\omega_*$ in terms of two-descent theory. If $\omega_*(F) = (q_1, q_2, q_3)$, then $F$ is isomorphic (over $\mathbb{Q}$) to the curve

$$q_1 y^2 = x - a_1, \quad q_2 y^2 = x - a_2, \quad q_3 y^2 = x - a_3,$$

while its twist over $\mathbb{Q}(\sqrt{d})$ is given by

$$q_1 y^2 = x - da_1, \quad q_2 y^2 = x - da_2, \quad q_3 y^2 = x - da_3,$$

where the isomorphism $F \to F^d$ maps $(x, y_1, y_2, y_3) \mapsto (dx, \sqrt{dy_1}, \sqrt{dy_2}, \sqrt{dy_3})$. Since $E^d$ is isomorphic to $y^2 = (x - da_1)(x - da_2)(x - da_3)$, we recognize from the above that $\omega_*(F^d) = (q_1, q_2, q_3)$ (we identified $(a_i, 0)$ with $(da_i, 0)$), and the claim follows. □

3. Structure of $\text{Sel}^{(2)}(E^d)$

In this section we describe the structure of $\text{Sel}^{(2)}(E^d)$ in the case when $|d|$ is prime. We prove the following proposition.
For the proof of Proposition 3.1, we need to introduce three more quartics.

\[ H_3 : y^2 = 25x^4 + 48x^3 - 114x^2 - 144x + 225 \in Sel(E^3), \]
\[ F_3 : y^2 = -71x^4 - 336x^3 - 538x^2 - 336x - 71 \in Sel^2(E^{-1}), \]
\[ F_4 : y^2 = -5x^4 + 76x^3 - 168x^2 - 296x - 92 \in Sel^2(E^{-3}). \]

Recall that quadratic twist \( E^d \) has the Weierstrass model \( E^d : y^2 = (x - 8d)(x - 9d)(x + 18d). \)

Next, we prove linear independence of classes needed for the proof of Proposition 3.1.

**Lemma 3.3.** For \( d \in \mathbb{Z}, \) \( [d] \) prime, and \( [d] \neq \{2, 3, 13\}, \) denote by \( Q_1 = (8d, 0) \) and \( Q_2 = (-18d, 0) \) elements in \( E^d[2] \) which correspond to \( P_1 \) and \( P_2 \) under the natural isomorphism \( E[2] \cong E^d[2], \) and by \( \kappa : E^d(Q)/2E^d(Q) \to Sel^2(E^d) \subset H^1(Q, E^d[2]) \) the Kummer map. We have that

\[ \omega_\ast(H^d) = (13, 13, 1), \omega_\ast(\kappa(Q_1)) = (26d, -26d, -d), \omega_\ast(\kappa(Q_2)) = (78, -26d, -3d), \]
\[ \omega_\ast(H_1^d) = (3, 1, 3), \omega_\ast(H_2^d) = (2, -2, -1), \omega_\ast(H_3^d) = (6, -6, 1), \]
\[ \omega_\ast(F_1^d) = (-2, -2, 1), \omega_\ast(F_2^d) = (-3, -1, 3), \omega_\ast(F_3^d) = (6, 2, 3), \omega_\ast(F_4^d) = (6, 6, 1). \]

Moreover,

a) if \( d > 0, \) the classes \( \omega_\ast(F), \) for \( F \in \{\kappa(Q_1), \kappa(Q_2), H^d, H_1^d, H_2^d, H_3^d, F_3^d\} \) are (multiplicatively) independent in \( (\mathbb{Q}^\times/\mathbb{Q}^\times)^3 \) and locally solvable at infinity.

b) if \( d < 0, \) the classes \( \omega_\ast(F), \) for \( F \in \{\kappa(Q_1), \kappa(Q_2), H^d, H_1^d, F_1^d, F_3^d, F_4^d\} \) are (multiplicatively) independent in \( (\mathbb{Q}^\times/\mathbb{Q}^\times)^3 \), and locally solvable at infinity.

**Proof.** Using Magma [BCP97], we can easily compute the values of \( \omega_\ast(F^d) \) for quartics \( F \) from 1.2 as they don't depend on \( d \) by Lemma 3.2.

We can also compute classes of torsion points explicitly. For example, for \( Q_1 = (8d, 0) \in E^d(Q), \) one can check that \( 2R_1 = Q_1, \) where \( R_1 = (\frac{1}{2}d^2 - \frac{9d}{2}, \frac{1}{4}d^3 - \frac{29d}{2}), \) with \( r^4 - 50br^2 + 35d^2 = 0. \)

Here \( Q(r) = Q(\sqrt{-d}, \sqrt{-26}), \) and by inspection one obtains that \( R_1 - R_1 = \chi_{26d}(\sigma)Q_1 + \chi_{-26}(\sigma)Q_2, \) thus \( \omega_\ast(\kappa(Q_1)) = (26d, -26d, -d). \) Similarly, one computes \( \omega_\ast(\kappa(Q_2)). \)

The existence of real points on quartic (which determine local solvability at infinity) can be checked for each quartic separately.

If \( d > 0, \) it is not hard to see that the classes will be independent unless \( d \) is divisible only by 2, 3 and 13. In particular, for squarefree \( d, \) we compute that this happens for \( \{1, 2, 3, 6, 13, 26, 39, 78\}, \) thus the claim in a) follows. The claim in b) is proved in a similar way.

We have the following proposition as a consequence of the previous lemma.

**Proposition 3.4.** If \( d \in \mathbb{Z} \) is square free integer such that \( H^d(Q) \neq \emptyset, \) then \( H^d(Q) \) is infinite.

**Proof.** Assume that for some \( d \in \mathbb{Z}, \) \( H^d(Q) \neq \emptyset \) and \( H^d(Q) \) is finite. It follows that the rank of Mordell-Weil group of \( E^d(Q) \) is zero, hence \( H^d \) as an element of 2-Selmer group \( Sel^2(E^d) \) is in the image of the two torsion \( E^d[2] \) under the map \( E^d(Q)/2E^d(Q) \to Sel^2(E^d) \) from 1.1. More precisely, there is a point of order 4, \( Q \in E^d[4], \) such that \( H^d \) corresponds to the cocycle \( \sigma \mapsto Q^\sigma - Q. \) It follows from Lemma 3.3 that the image of this cocycle is of order 2 which implies that \( Q \) is defined over quadratic field. There are only finitely many \( d's \) that have a point of order 4 defined over quadratic field. Note that if \( x_0 \) is an \( x \)-coordinate of point of order 4 on \( E \) (it is defined over quadratic field), then \( d \cdot x_0 \) is an \( x \)-coordinate of point of order 4 on \( E^d. \) Moreover, if \( E_d : y^2 = f_d(x) = (x - 8d)(x - 9d)(x + 18d), \) then \( f_d(dx_0) = d^5 \cdot f_1(x_0) \) is a square in \( Q(x_0) \) if and only if \( d \cdot f_1(x_0) \) is a square. One can check that this is the case if and only if \( d = \{-26, -3, -1, 1, 3, 26\}. \) The proposition follows after verifying the claim for these special cases.

\qed
To obtain an upper bound for the size of 2-Selmer group, we will use the method and terminology from the paper of Mazur and Rubin [MR10][Section 3] (see also [Kra81,BD10]).

**Definition 3.5.** Suppose $\tilde{E}$ is an elliptic curve over $\mathbb{Q}$. For every place $v$ of $\mathbb{Q}$, let $H_f(Q_v, \tilde{E}[2])$ denote the image of the Kummer map

$$\tilde{E}(Q_v)/2\tilde{E}(Q_v) \to H^1(Q_v, \tilde{E}[2]).$$

The 2-Selmer group $\text{Sel}^{(2)}(\tilde{E})$ is the $\mathbb{F}_2$-vector space defined by the exactness of the sequence

$$0 \to \text{Sel}^{(2)}(\tilde{E}) \to H^1(Q, \tilde{E}[2]) \to \bigoplus_v H^1(Q_v, \tilde{E}[2])/H^1_f(Q_v, \tilde{E}[2]).$$

We say that 2-Selmer group $\text{Sel}^{(2)}(\tilde{E})$ is cut out by the local conditions $H_f(Q_v, \tilde{E}[2]).$

The following lemma describes the size of local conditions.

**Lemma 3.6.** Let $v$ be a finite rational place and $d$ an odd squarefree integer. We have

$$\dim_{\mathbb{F}_2} H^1_f(Q_v, E^d[2]) = \begin{cases} 2 & \text{if } v \neq 2 \\ 3 & \text{if } v = 2. \end{cases}$$

**Proof.** By Lemma 2.2 in [MR10], if $v \nmid 2\infty$, then $\dim_{\mathbb{F}_2} H^1_f(Q_v, E^d[2]) = \dim_{\mathbb{F}_2} E^d(Q_v)[2] = 2$.

Following [Sil01 Chapter 4.], denote by $\mathcal{F}$ the formal group associated to the elliptic curve $E^d/Q_2$, and by $\mathcal{F}(2\mathbb{Z}_2)$ the group associated to that formal group. Theorem 6.4. b) in [Sil01] implies that $\mathcal{F}(4\mathbb{Z}_2)$ is isomorphic (via formal logarithm map) to the additive group $\mathbb{G}_a(4\mathbb{Z}_2)$ which implies that $\mathcal{F}(4\mathbb{Z}_2)/2\mathcal{F}(4\mathbb{Z}_2) \cong \mathbb{Z}/2\mathbb{Z}$. On the other hand, since $\mathcal{F}(x,y) = x + y - a_1xy - a_2x^2y + xy^2 + \cdots$, where $a_1$ and $a_2$ are the usual Weierstrass coefficients of $E^d$, it follows that $[2](x) = 2x + O(x^3)$ (as $a_1 = 0$), thus $2\mathcal{F}(2\mathbb{Z}_2) = \mathcal{F}(4\mathbb{Z}_2)$. In particular, $\mathcal{F}(2\mathbb{Z}_2)/2\mathcal{F}(2\mathbb{Z}_2) \cong \mathbb{Z}/2\mathbb{Z}$.

If we denote by $E^d(Q_2)$ the subgroup of points in $E^d(Q_2)$ which reduce to the point at infinity modulo two, then it is well known that $E^d(Q_2) \cong \mathcal{F}(2\mathbb{Z}_2)$. Moreover, $E^d_0(Q_2)/E^d_0(Q_2)$, where $E^d_0(Q_2)$ is the subgroup of points of nonsingular reduction, is generated by two torsion point with odd $x$ coordinate. Finally, $E^d(Q_2)/E^d_0(Q_2)$ is generated by the point of order two with even $x$ coordinate (Tamagawa number of $E^d$ is two), and we have that $E^d(Q_2)/2E^d(Q_2) \cong (\mathbb{Z}/2\mathbb{Z})^3$, so the claim follows. \hfill $\square$

There is a natural identification of Galois modules $E[2] \cong E^d[2]$ - which is crucial for our argument. We identify point $(a,0) \in E(\mathbb{Q})$ with $(8a,0) \in E^d(\mathbb{Q})$ for $a \in \{8,9,-18\}$. It allows us to view $\text{Sel}^{(2)}(E^d)$ as a subspace of the $H^1(Q, E[2])$, but defined by the different sets of local conditions $H^1_f(Q_v, E^d[2]) \subset H^1(Q_v, E[2]).$

**Definition 3.7.** If $\tilde{T}$ is a finite set of places of $\mathbb{Q}$, define relaxed 2-Selmer group $S^T$ by the exactness of

$$0 \to S^{\tilde{T}} \to H^1(Q, E[2]) \to \bigoplus_{v \not\in \tilde{T}} H^1(Q_v, E[2])/H^1_f(Q_v, E[2]),$$

where the second arrow is induced by the sum of localization maps $H^1(Q, E[2]) \to H^1(Q_v, E[2]).$

By definition $\text{Sel}^{(2)}(E) \subset S^{\tilde{T}}$ for any $\tilde{T}$. We will choose $\tilde{T}$ such that $\text{Sel}^{(2)}(E^\dagger) \subset S^{\tilde{T}}$ holds as well. For that we will need the following criteria for equality of local conditions after twist (see Lemma 2.10 and Lemma 2.11 in [MR10]).

**Lemma 3.8.** Let $\tilde{E}/\mathbb{Q}$ be an elliptic curve. Let $v$ be a place of $\mathbb{Q}$ and $d$ a squarefree integer. If at least one of the following conditions holds

a) $v$ splits in $\mathbb{Q}(\sqrt{d})$,

b) $v$ is a prime of good reduction of $\tilde{E}$ and $v$ is unramified in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$,
then $H^1_f(Q_v, \tilde{E}[2]) = H^1_f(Q_v, \tilde{E}^d[2])$. Moreover, if $\tilde{E}$ has good reduction at $v$, and $v$ is ramified in $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$, then

$$H^1_f(Q_v, \tilde{E}[2]) \cap H^1_f(Q_v, \tilde{E}^d[2]) = 0.$$  

Since primes of bad reduction of $E^d$ are $\{2, 3, 13, p\}$, and since 13 splits in $\mathbb{Q}(\sqrt{d})$, it follows from Lemma $3.3$ that local conditions $H^1_f(Q_v, E^d[2])$ and $H^1_f(Q_v, E[2])$ are equal outside the set $T = \{2, 3, p, \infty\}$.

**Proof of Proposition 3.4** Lower bound for the $\operatorname{dim}_F \operatorname{Sel}^d(E^d)$ in both cases follows from Lemma $3.3$ and Proposition $2.3$. Note that if $d > 0$, classes $F_1^{-d}$ and $F_2^{-d}$ are ELS if $d < 0$ and $d \equiv 7 \pmod{8}$, and classes $F_1^{-d}$ and $H_1^{-d}$ are ELS if $d < 0$ and $d \equiv 5 \pmod{8}$.

For the upper bound we first consider the case $d \in T$. From the definition of $T$ it follows that for $|d| > 3$ primes 2 and 3 split in $\mathbb{Q}(\sqrt{d})$, thus Lemma $3.3$ implies that local conditions $H^1_f(Q_v, E^d[2])$ and $H^1_f(Q_v, E[2])$ differ only at $v = p$ (and possibly at $v = \infty$ if $d < 0$ - note that if $d > 0$ elliptic curves $E$ and $E^d$ are isomorphic over $\mathbb{R}$).

Assume that $d > 0$ and set $T = \{p\}$. Define a strict 2-Selmer group $S_T := S_T(E)$ by the exactness of

$$0 \rightarrow S_T \rightarrow T^T \rightarrow \bigoplus_{v \in T} H^1(Q_v, E[2]),$$

where the second arrow is the sum of the localization maps.

From the construction, it follows that $S_T \subset \operatorname{Sel}^d(E^d) \subset T^T$, and $S_T \subset \operatorname{Sel}^d(E) \subset T^T$. We will show that $S_T = \operatorname{Sel}^d(E)$. One can compute that $E(\mathbb{Q})$ is generated by 2-torsion points

$$S_1 = (18, 0), S_2 = (8, 0) \text{ and point } S_3 = (45/4, -117/8) \text{ of infinite order, and that } \operatorname{Sel}^d(E) \text{ is generated by the } \kappa(S_i), i = 1, 2, 3, \text{ where } \kappa : E(\mathbb{Q})/2E(\mathbb{Q}) \rightarrow \operatorname{Sel}^d(E) \text{ is the Kummer map }$$

- thus $\operatorname{dim}_F \operatorname{Sel}^d(E^d) = 3$. It is enough to show that the image of the $\kappa(S_i)$ in $H^1(Q_p, E[2])$ is trivial. Choose $Q_i \in E(\mathbb{Q})$ such that $2Q_i = S_i$. The fields of definitions $K_i$ of points $Q_i$ are $K_1 = \mathbb{Q}(\alpha_1)$ where $\alpha_1^4 + 106\alpha_1^2 + 1 = 0$, $K_2 = \mathbb{Q}(\alpha_2)$ where $\alpha_2^4 - 50\alpha_2^2 + 729 = 0$ and $K_3 = \mathbb{Q}(\alpha_3)$ where $\alpha_3^3 - 3\alpha_3 - 43/4 = 0$. It happens that $p$ splits completely in all the fields, hence the claim follows.

Lemma 3.2 in [MR10] implies that $\dim_F \mathcal{S}^T - \dim_F \mathcal{S}_T = \dim_F H^1(Q_p, E[2])$. By Lemma $3.6$ and inclusion $\operatorname{Sel}^d(E^d) \subset \mathcal{S}_T$, it follows $\dim_F \operatorname{Sel}^d(E^d) \leq 3 + 2 = 5$, and the claim follows.

The case $d < 0$ is analogous - to get the equality of local conditions at $v = \infty$ one replaces $E$ with $E^{-1}$, and then proceeds as in the $d > 0$ case.

Now assume that $d \notin T$. Consider the case $d < 0$. In the case $d > 0$ one repeats the same argument with $E^{-1}$ replaced by $E$. Primes 2 and 3 do not need to split in $\mathbb{Q}(\sqrt{d})$ any more, hence we set $T = \{2, 3, p\}$ and $\mathcal{S}^T := \mathcal{S}^T(E^{-1})$ and $\mathcal{S}_T := \mathcal{S}_T(E^{-1})$ (we replaced $E$ with $E^{-1}$ in definitions to ensure the equality of local conditions at $v = \infty$). Lemma 3.2 in [MR10] and Lemma $3.6$ imply that $\dim_F \mathcal{S}^T = \dim_F \mathcal{S}_T = \dim_F H^1_f(Q_2, E^{-1}[2]) + \dim_F H^1_f(Q_3, E^{-1}[2]) + \dim_F H^1_f(Q_p, E^{-1}[2]) = 3 + 2 + 2 = 7$. Since $\mathcal{S}_T \subset \operatorname{Sel}^d(E^{-1})$, if we show that the image of each class in $\operatorname{Sel}^d(E^{-1})$ (which is generated by $H^{-1}, F_1$ and $F_3$) under the localization $\operatorname{loc}_2 : \operatorname{Sel}^d(E^{-1}) \rightarrow H^1(Q_2, E^{-1}[2])$ is different than zero, then it follows that $\mathcal{S}_T = 0$. One can check that, for any $P \in E^{-1}(\mathbb{Q})/2E^{-1}(\mathbb{Q})$ and $Q \in E^{-1}(\mathbb{Q})$ such that $2Q = P$, 2 is ramified in the field of definition of $Q$, hence the localization of $\kappa(P)$ at $v = 2$ is nontrivial, and $\mathcal{S}_T = 0$. It follows that $\dim_F \mathcal{S}_T = 7$.

Lemma $3.3$ b) provides us with the generators of $\mathcal{S}_T$ once we show that the torsion classes together with classes $H, F_1, H_1, F_2, F_4 \in H^1(Q, E)$ satisfy local conditions $H^1_f(Q_v, E^{-1}[2])$ for $v$ outside the set $T$. Equivalently, one can check that the quartics $H^{-1}, F_1, H_1^{-1}, F_2$ and $F_4^2$ (as two covers of $E^{-1}$) are locally solvable outside the set $T$. Local solvability at the finite
places outside the set \( \{2, 3, 13\} \) follows immediately from the Hensel lemma argument (as in the proof of Proposition \ref{prop:1}) since these are the bad primes of \( E^{-1} \), while solvability at \( v = \infty \) (i.e. existence of the real points on quadratic twists) follows from the observation that polynomials of degree 4 defining \( H \) and \( H_1 \) have real roots. The local solvability at \( v = 13 \) follows from the fact that \( \left( \frac{p}{13} \right) = 1 \), which implies that \( p \) is a square in \( \mathbb{Q}_{13} \), thus quadratic twist by \( \mathbb{Q}(\sqrt{7}) \) or \( \mathbb{Q}(\sqrt{-d}) \) of any quartic from Lemma \ref{lem:3} (b) is isomorphic over \( \mathbb{Q}_{13} \) to that quartic. Hence, we only need to check that \( F_1^d \) is locally solvable at \( v = 13 \) which is checked readily.

We will prove that \( \dim_{F_2} \text{Sel}^2(E^d) \leq 4 \), which will imply that \( \dim_{F_2} \text{Sel}^2(E^d) = 3 \) since \( \dim_{F_2} \text{Sel}^2(E^d) \) is odd (by \cite{DDI10} \((-1)^{\dim_{F_2} \text{Sel}^2(E^d)} = w(E^d) = -1 \)) and greater or equal to 3 (since \( H^d \) and the torsion classes of \( E^d \) are linearly independent in \( \text{Sel}^2(E^d) \)). Essentially, for each class in \( S^T \) (generators are given by Lemma \ref{lem:3} (b)), we will check if it satisfies the local conditions \( H_1^T(\mathbb{Q}_v, E^d[2]) \).

Observe that the local condition at \( v = p \), \( H_1^T(\mathbb{Q}_p, E^d[2]) \), for \( p \neq \{2, 3, 13\} \) is determined with the image of 2-torsion \( \chi(P_1)(\sigma) = \chi_3(\sigma)P_1 + \chi_d(\sigma)P_3, \chi(P_2) = \chi_{-13d}(\sigma)P_1 + \chi_2(\sigma)P_3 \) (since the elements are independent and dimension of the local condition is 2). As the remaining generators of \( S^T \), \( H : \sigma \mapsto \chi_1(\sigma)P_3, F_1 : \sigma \mapsto \chi_2(\sigma)P_3, H_1 : \sigma \mapsto \chi_3(\sigma)P_1, F_3 : \sigma \mapsto \chi_6(\sigma)P_3 \) and \( F_2 + H_1 \equiv \chi_{-1}(\sigma)P_2 \) do not depend on \( d \) (here \( \chi_9 \) denotes the nontrivial character of \( \mathbb{Q}(\sqrt{7}) \)), the local condition at \( v = p \) can be satisfied by some class from the subspace generated by \( H, H_1, F_1, F_4 \) and \( F_2 \) only if the localization of that class at \( v = p \) is trivial. If \( p = 5 \) (mod 8), then \(-1, 3 \) are squares in \( \mathbb{Q}_p \) while \( 2 \) and \( 3 \) are not, thus \( H, F_2 + H_1 \) and \( F_4 \) generate the subspace of \( S^T \) with required property, while if \( p = 7 \) (mod 8), then \( 13 \) are squares in \( \mathbb{Q}_p \) while \(-1 \) and \( 3 \) are not, thus \( H, F_1 + F_4 \) and \( F_1 + F_2 + H_1 \) generate the subspace of \( S^T \) consisting of elements whose localization at \( v = p \) is trivial.

Next, to rule out remaining classes, focus on the local condition at \( v = 3 \). If \( p = 5 \) (mod 8), then \( d \) is a square in \( \mathbb{Q}_3 \), and the classes \( \text{loc}_3 \chi(P_1)(\sigma) = \chi_3(\sigma)P_1 \) and \( \text{loc}_3 \chi(P_2)(\sigma) = \chi_{-1}(\sigma)P_1 \) linearly independent, thus they generate 2-dimensional \( F_2 \)-vector space \( H_1^T(\mathbb{Q}_3, E^d[2]) \). Since, \( \text{loc}_3(F_1)(\sigma) = \chi_6(\sigma)P_3 = \chi_{-3}(\sigma)P_3 \not\in H_1^T(\mathbb{Q}_3, E^d[2]) \), we conclude that in this case \( \dim_{F_2} \text{Sel}^2(E^d) \leq 4 \), hence equal to 3.

If \( p = 7 \) (mod 8), then \( \text{loc}_3 \chi(P_1)(\sigma) = \chi_3(\sigma)P_1 + \chi_{-1}(\sigma)P_3 \) and \( \text{loc}_3 \chi(P_2)(\sigma) = 0 \) generate a 1-dimensional subspace of the 2-dimensional vector space \( H_1^T(\mathbb{Q}_3, E^d[2]) \). Note that not all the localisations of the classes of interest \( \text{loc}_3(F_1 + F_4)(\sigma) = \chi_{-3}(\sigma)P_3 \) and \( \text{loc}_3(F_1 + F_2 + H_1)(\sigma) = \chi_{-1}(\sigma)P_3 \) can lie in \( H_1^T(\mathbb{Q}_3, E^d[2]) \) (since the subspace they generated does not contain \( \text{loc}_3 \chi(P_1)(\sigma) \)), hence \( \dim_{F_2} \text{Sel}^2(E^d) \leq 4 \), and the claim follows.

The following proposition follows immediately from the explicit description of \( \text{Sel}^2(E^d) \) given in Proposition \ref{prop:1}.

**Proposition 3.9.** Let \( d \in T \) (hence \( \dim_{F_2} \text{Sel}^2(E^d) = 5 \)). We have that \( \text{III}(E^d)[2] = 2\text{III}(E^d)[4] \) if and only if

a) \( \langle H_1^T H_1^d \rangle_{CT} = 0 \) and \( \langle H^d, H_1^d \rangle_{CT} = 0 \) for \( i = 1, 2 \) if \( d > 0 \),

b) \( \langle F^{-d}_i, F_2^{-d} \rangle_{CT} = 0 \) and \( \langle H^d, F_i^{-d} \rangle_{CT} = 0 \) for \( i = 1, 2 \) if \( d < 0 \) and \( d \equiv 7 \) (mod 8),

**Proof.** If \( \text{III}(E^d)[2] = 2\text{III}(E^d)[4] \), then the Cassels-Tate pairing on \( \text{Sel}^2(E^d) \) is trivial (since it is non-degenerate on \( \text{III}(E^d)[2]/2\text{III}(E^d)[4] \)), hence the claim follows. Similarly, if a),b) hold, then Proposition \ref{prop:1} implies the Cassels-Tate pairing on \( \text{Sel}^2(E^d) \) is trivial, hence \( \text{III}(E^d)[2] = 2\text{III}(E^d)[4] \). Note that in the case \( d < 0 \) and \( d \equiv 5 \) (mod 8), we always have \( \langle H^d, F_1^{-d} \rangle_{CT} = 1 \) (see Theorem \ref{thm:1}b)), hence \( \text{III}(E^d)[2] \neq 2\text{III}(E^d)[4] \). \( \square \)
4. Cassels-Tate pairing and governing fields

Our main tool for studying Cassels-Tate pairing of quadratic twists of elements of 2-Selmer groups is the following specialisation of the theorem of Smith (see Section 3 in [Smi16]).

**Theorem 4.1 (Smith).** Let $\tilde{E}$ be an elliptic curve over $\mathbb{Q}$ with full 2-torsion over $\mathbb{Q}$. Let $F, F' \in H^1(\mathbb{Q}, \tilde{E}[2])$, and let $K$ be the minimal field over which $F$ and $F'$ are trivial. Next, let $S$ be any set of places of $\mathbb{Q}$ which contains all places of bad reduction of $\tilde{E}$, the archimedean place and 2. Take $D$ to be the set of pairs $(d_1, d_2)$ of elements in $\mathbb{Q}^\times$ such that $d_1/d_2$ is square at all places of $S$, and $F_{d_1}$ and $F_{d_2}$ are elements of 2-Selmer group of $\tilde{E}_{d_1}$ and $\tilde{E}_{d_2}$ respectively.

If $F \cup F'$ is alternating (as defined in Section 3 of [Smi16]), then $(F_{d_1}, F_{d_1})_{CT} = (F_{d_2}, F_{d_2})_{CT}$ for all $(d_1, d_2) \in D$. Otherwise, there is a quadratic extension $L$ of $K$ that is ramified only at primes in $S$ such that

$$(F_{d_1}, F_{d_1})_{CT} = (F_{d_2}, F_{d_2})_{CT} + \left\lceil \frac{L/K}{d} \right\rceil,$$

for all $(d_1, d_2) \in D$, where the Galois group $\text{Gal}(L/K)$ is identified with $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$. Here $d$ is any ideal of $K$ coprime to the conductor of $L/K$ that has norm in $\mathbb{Q}^\times/\mathbb{Q}^\times$ equal to $(d_1/d_2)$. Such $d$ exists for all $(d_1, d_2) \in D$. We denote by $\left\lceil \cdot \right\rceil$ the Artin symbol.

**Remark 4.2.** We will call field $L$ from the statement of Theorem 4.1 a governing field of $F$ and $F'$. It needs not to be unique.

Next, we compute the governing fields of some pairs of classes defined by quartics from (1.2) (see Table 1).

In general, following Section 3.1. in [Smi16], for $F, F' \in H^1(\mathbb{Q}, E[2])$ let $\omega_s(F) = (a_1, a_2, a_3)$ and $\omega_s(F') = (a'_1, a'_2, a'_3)$. For every place $v$ we have the following relation of Hilbert symbols $(a_1, a'_1)_v, (a_2, a'_2)_v, (a_3, a'_3)_v = 1$. We can choose $b \in \mathbb{Q}^\times$ such that $(a_1, ba'_1)_v = (a_2, ba'_2)_v = (a_3, ba'_3)_v = 1$ which implies that we can find $x_i, y_i, z_i \in \mathbb{Q}^\times$ such that $x_i^2 - a_i y_i^2 = ba'_i z_i^2$ for $i = 1, 2, 3$. We can further scale $x_i, y_i$ and $z_i$ by a common factor so that the field

$$L_{F,F'} = K_{F,F'} \left( \sqrt{(x_1 + y_1\sqrt{a_1})(x_2 + y_2\sqrt{a_2})(x_3 + y_3\sqrt{a_3})} \right)$$

avoids ramification at places unramified in the common field of definition

$$K_{F,F'} := \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \sqrt{a_1}, \sqrt{a_2}).$$

**Lemma 4.3 (Smith).** If $F \cup F'$ is not alternating and $\deg K_{F,F'}/\mathbb{Q} = 16$, then $L_{F,F'}$ is a governing field of $F$ and $F'$. Although in our case $\deg K_{F,F'}/\mathbb{Q}$ is either four or eight, we can still compute governing fields using the following lemma which follows from the proof of Proposition 2.1. in [Smi16].

**Lemma 4.4.** For integers $a$ and $b$ such that $ab$ is not a perfect square let $L_{a,b}/\mathbb{Q}(\sqrt{a}, \sqrt{b})$ be quadratic extension such that $L_{a,b}/\mathbb{Q}$ is Galois with Galois group isomorphic to dihedral group $D_8$. There exist a map

$$\gamma_{a,b} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \xrightarrow{\text{res}} \text{Gal}(L_{a,b}/\mathbb{Q}) \to \mu_2$$

which satisfies $d\gamma_{a,b} = \chi_a \cup \chi_b \in H^2(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mu_2)$. Here $\mu_2 = \{\pm 1\}$ and the cup product $\chi_a \cup \chi_b$ is induced by the natural bilinear map $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ (hence for $\sigma, \tau \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we have that $(\chi_a \cup \chi_b)(\sigma, \tau) = -1$ if and only if $\sqrt{a} = -\sqrt{a}$ and $\sqrt{b} = -\sqrt{b}$).
4.1. $L_{H^{-1}, F_2} = Q(\sqrt{13}, \sqrt{-1}, \sqrt{-3})(\sqrt{3(1 + \sqrt{13}) (3 + \sqrt{13})})$. It follows from Lemma 3.3 that $H^{-1}(\sigma) = \chi_{13}(\sigma) P_1 + \chi_{13}(\sigma) P_2$ and $F_2(\sigma) = \chi_{-3}(\sigma) P_1 + \chi_{-1}(\sigma) P_2$ for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. If we define the cup product $\cup : H^1(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E[2]) \times H^1(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), E[2]) \to H^2(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}), \mu_2)$ using the Weil pairing $e_2 : E[2] \times E[2] \to \mu_2$, it follows that $H^{-1} \cup F_2 = \chi_{13} \cup \chi_{-1} \cdot \chi_{13} \cup \chi_{-3} = \chi_{13} \cup \chi_{3}$. The field $L_{H, F_2}$ has a property that it contains subfield $L/\mathbb{Q}(\sqrt{13}, \sqrt{3})$ such that $L/\mathbb{Q}$ is $D_8$ extension. Lemma 4.4 implies that there exists a map $\Gamma : \text{Gal}(\mathbb{Q}) \to \mu_2$ defined over $L_{H, F_2}$ such that $d\Gamma = \chi_{13} \cup \chi_{3} = H^{-1} \cup F_2$. One can check that $L_{H, F_2}/\mathbb{Q}$ is unramified outside the set $\{2, 3, 13\}$ of primes of bad reduction of $E$, hence it follows from the proof of Theorem 3.2 in [Sm16] that $L_{H, F_2}$ is governing field of $H^{-1}$ and $F_2$. The choice of field $L_{H^{-1}, F_2}$ is particularly nice since it is easy to check that for prime $p$ the Cassels-Tate pairing $\langle H^{-p}, F_2^{p}\rangle_{CT}$ is equal to 0 if and only if $p$ splits completely in $L_{H^{-1}, F_2}$, provided that $H^{-p}$ and $F_2^p$ define an element in $\text{Sel}^{(2)}(E^{-p})$. It follows from Proposition 2.3 that $H^{-p}$ and $F_2^p$ are ELS if and only if $p = 13$ or $p$ splits completely in the field of definition $K_{H^{-1}, F_2} = Q(\sqrt{13}, \sqrt{-1}, \sqrt{-3})$.

4.2. $L_{H_1, H_2} = Q(\sqrt{3}, \sqrt{-1}, \sqrt{2})(\sqrt{8(1 + \sqrt{3})(4 + 2\sqrt{3})})$. It follows from Lemma 3.3 that $H_1(\sigma) = \chi_{13}(\sigma) P_1$ and $H_2(\sigma) = \chi_{-1}(\sigma) P_1 + \chi_{-2}(\sigma) P_2$ for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, thus $H_1 \cup H_2 = \chi_{13} \cup \chi_{-1}$. Since $L_{H_1, H_2}$ is unramified outside the set $\{2, 3, 13\}$ and since $L_{H_1, H_2}$ contains a degree two extension $L/\mathbb{Q}(\sqrt{3}, \sqrt{-2})$ such that $L/\mathbb{Q}$ is Galois with Galois group $D_8$, same as in 4.1 we can conclude that $L_{H_1, H_2}$ is governing field of $H_1$ and $H_2$. Moreover, for $p$ prime such that $H_1^p$ and $H_2^p$ define an element in $\text{Sel}^{(2)}(E^p)$ (or equivalently for prime $p$ which splits completely in $K_{H_1, H_2} = Q(\sqrt{3}, \sqrt{-1}, \sqrt{2})$), we have that $\langle H_1^p, H_2^p\rangle_{CT}$ is equal to 0 if and only if $p$ splits completely in $L_{H_1, H_2}$.

4.3. $L_{F_1, F_2} = Q(\sqrt{3}, \sqrt{-1}, \sqrt{2})(\sqrt{8(1 + \sqrt{3})(4 + 2\sqrt{3})})$. Here conclusion is the same as in 4.2 for $p$ prime such that $F_1^p$ and $F_2^p$ define an element in $\text{Sel}^{(2)}(E^{-p})$ (or equivalently for prime $p$ which splits completely in $K_{F_1, F_2} = Q(\sqrt{3}, \sqrt{-1}, \sqrt{2})$), we have that $\langle F_1^p, F_2^p\rangle_{CT}$ is equal to 0 if and only if $p$ splits completely in $L_{F_1, F_2}$.

4.4. $L_{H, H_2} = Q(\sqrt{-1}, \sqrt{2}, \sqrt{13})(\sqrt{4 + 2\sqrt{13}})$. Lemma 3.3 implies that $H(\sigma) = \chi_{13}(\sigma) P_1$ and $H(\sigma) = \chi_{-1}(\sigma) P_1 + \chi_{-2}(\sigma) P_2$ for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, thus $H \cup H_2 = \chi_{13} \cup \chi_{-1}$. Since $L_{H, H_2}$ is unramified outside the set $\{2, 3, 13\}$ and since $L_{H, H_2}$ contains a degree two extension $L/\mathbb{Q}(\sqrt{-1}, \sqrt{13})$ such that $L/\mathbb{Q}$ is Galois with Galois group $D_8$, same as in 4.1 we can conclude that $L_{H, H_2}$ is governing field of $H$ and $H_2$. Also, for $p$ prime such that $H^p$ and $H_2^p$ define an element in $\text{Sel}^{(2)}(E^p)$ (or equivalently for prime $p$ which splits completely in $K_{H, H_2} = Q(\sqrt{13}, \sqrt{-1}, \sqrt{2})$), we have that $\langle H^p, H_2^p\rangle_{CT}$ is equal to 0 if and only if $p$ splits completely in $L_{H, H_2}$.

4.5. $L_{H, H_1} = Q(\sqrt{3}, \sqrt{13})(\sqrt{4 + \sqrt{13}})$. Lemma 3.3 implies that $H(\sigma) = \chi_{13}(\sigma) P_1$ and $H(\sigma) = \chi_{3}(\sigma) P_1$ for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, thus $H \cup H_1 = \chi_{13} \cup \chi_{3}$. Since $L_{H, H_1}$ is unramified outside the set $\{2, 3, 13\}$ and since $L_{H, H_1}/\mathbb{Q}$ is $D_8$ extension same as in 4.1 we conclude that $L_{H, H_1}$ is governing field of $H$ and $H_1$. Also, for $p$ prime such that $H^p$ and $H_1^p$ define an element in $\text{Sel}^{(2)}(E^p)$, we have that $\langle H^p, H_1^p\rangle_{CT}$ is equal to 0 if and only if $p$ splits completely in $L_{H, H_1}$. Note that $H^p$ and $H_1^p$ are ELS if and only if $p = 13$ or $p$ splits completely in $K_{H, H_1} = Q(\sqrt{13}, \sqrt{-1}, \sqrt{-3})$ and $p \equiv 1$ (mod 4).

4.6. $L_{H^{-1}, F_1} = Q(\sqrt{-2}, \sqrt{13})(\sqrt{-1})$. It follows from Lemma 3.3 that for all $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ we have that $H^{-1}(\sigma) = \chi_{13}(\sigma) P_1 + \chi_{13}(\sigma) P_2 = \chi_{-3}(\sigma) P_3$ and $F_1(\sigma) = \chi_{-2}(\sigma) P_1 + \chi_{-2}(\sigma) P_2 = \chi_{-2}(\sigma) P_3$, thus $e_2(H^{-1}(\sigma), F_1(\sigma)) = 1$. Therefore $H^{-1} \cup F_1$ is alternating (see Lemma 4.1 in [Sm16]) and $\langle H^{-d_1}, F_1^{d_1}\rangle_{CT} = \langle H^{-d_2}, F_1^{d_2}\rangle_{CT}$ for all pairs $(d_1, d_2) \in \mathcal{D}$ from Theorem 4.1. For $p$ prime such that $H^{-p}$ and $F_1^p$ define an element in $\text{Sel}^{(2)}(E^{-p})$, we can check by computing set $\mathcal{D}$ that $\langle H^{-p}, F_1^p\rangle_{CT}$ is equal to 0 if and only if $p$ splits completely in $L_{H^{-1}, F_1}$. Note that $H^{-p}$
and $F'_1$ are ELS if and only if $p$ splits completely in $K_{H^{-1},F_1} = \mathbb{Q}(\sqrt{13}, \sqrt{-2})$, thus, as before, the splitting behaviour of $p$ in $L_{H^{-1},F_1}$ determines Cassels-Tate pairing even though $L_{H^{-1},F_1}$ is not a governing field of $H^{-1}$ and $F_1$.

5. Proofs of Main Results

Proof of Theorem 1.7 From Section 4 (see also Table 1), we see that the governing field of the pair $(H^{-1}, F_1)$ is $L_{H^{-1},F_1} = \mathbb{Q}(\sqrt{-2}, \sqrt{13})(\sqrt{-1})$. In particular,

$$\langle H^d, F_1^{-d}\rangle_{CT} = \begin{cases} 0 & \text{if } |d| \text{ splits completely in } L_{H^{-1},F_1}, \\ 1 & \text{otherwise}. \end{cases}$$

For $d < 0$, it follows from the description of set $T$ that $\langle H^d, F_1^{-d}\rangle_{CT} = 1$ if $d \equiv 1 \pmod{4}$ and $\langle H^d, F_1^{-d}\rangle_{CT} = 0$ if $d \equiv 3 \pmod{4}$. Hence a) follows. For b), assume that $d \equiv 3 \pmod{4}$ and $\varepsilon(H^d) \neq 0$. As argued in the introduction, there is $L \in \text{Sel}^{(2)}(E^d)$ such that $\langle H^d, L\rangle_{CT} = 1$. Since $\langle H^d, F_1^{-d}\rangle_{CT} = 0$, from the bilinearity of the Cassels-Tate pairing it follows that $\langle H^d, F_2^{-d}\rangle_{CT} = 1$ (as $F_2$ is remaining generator of $\text{Sel}^{(2)}(E^d)$). The other implication in b) is obvious. C) is proved similarly. The only difference here is that in $d > 0$ case, $\text{Sel}^{(2)}(E^d)$ is, in addition to torsion classes, generated by $H^d$, $H_1^d$, and $H_2^d$.

Proof of Corollary 1.6 First we count the contribution to $S(X)$ of $d = \pm p$ for which $d \notin T$. It follows from Conjectures 1 and 2 and Propositions 3.4 and 3.1 that the only significant case is when $w(E^d) = -1$ (assuming $H^d$ is ELS) in which case $\text{III}(E^d)[2]$ is trivial. It follows from Propositions 2.1, 2.3 and 3.1 that this is equivalent to $\left(\frac{d}{13}\right) = 1$, $\left(\frac{d}{7}\right) \cdot \left(\frac{d}{11}\right) = \text{sgn}(d)$ and $d \equiv 0 \pmod{8}$ if $d > 0$ or $d \equiv 6 \pmod{8}$ if $d < 0$. Thus if

$$d \equiv 29, 35, 53, 55, 77, 79, 101, 103, 107, 127, 131, 155, 173, 179, 199, 251, 269, 295 \pmod{8 \cdot 3 \cdot 13}$$

when $d > 0$ or if $d < 0$ and

$$d \equiv 5, 17, 43, 113, 139, 185, 209, 211, 233, 235, 257, 259, 283 \pmod{8 \cdot 3 \cdot 13},$$

then $H^d(\mathbb{Q}) \neq \emptyset$. There are 18 residue classes in the first case, and 12 in the second, thus by Dirichlet’s theorem on arithmetic progressions, the contribution to $C_1$ is $\frac{30}{25(8 \cdot 3 \cdot 13)} = \frac{5}{32}$. 

Next, consider the case $d > 0$, $d \in T$ and $\text{III}(E^d)[2] \neq 2\text{III}(E^d)[4]$. Corollary 1.2 together with Proposition 5.9 implies that in this case $H^d(\mathbb{Q}) \neq \emptyset$ if and only if $d$ does not split completely in $L_{H, H_1}$ and $L_{H, H_2}$. One can check that the assumption $d > 0$ and $d \in T$ is equivalent to the requirement that $d$ splits completely in $K_{H, H_1}$ and $K_{H, H_2}$, thus we need to find a density of $d$’s such that $d$ splits completely in composition $K = L_{H, H_1} L_{H, H_2} K_{H_1, H_2}$ but not in its degree two extension $L = L_{H, H_1} L_{H, H_2} L_{H_1, H_2}$. By Chebotarev density theorem the density of such $d$’s is $\frac{1}{\deg K} \cdot \frac{1}{2}$. From Table 1 we see that $K_{H_1, H_2}$ is contained in $L_{H, H_1} L_{H, H_2}$. Moreover, one can check that $\deg L_{H, H_1} L_{H, H_2} = 64$, thus in this case the contribution to $C_1$ is equal to $\frac{1}{2} \cdot \frac{1}{128}$ (we have extra $\frac{1}{2}$ since $C_1$ is a lower bound for $\frac{S(X)}{2\pi(X)}$ and not $\frac{S(X)}{\pi(X)}$).

Finally, consider the case $d < 0$, $d \in T$ and $\text{III}(E^d)[2] \neq 2\text{III}(E^d)[4]$. Corollary 1.2 together with Proposition 5.9 implies that $H^d(\mathbb{Q}) \neq \emptyset$ if and only if $d = -p$, where $p \equiv 1 \pmod{4}$, does not split completely in $L_{F_1, F_2}$ and splits completely in $L_{H^{-1}, F_2}$. One can check that assumption $p \equiv 1 \pmod{4}$ and $-p \in T$ is equivalent to $p$ splits completely in $K_{H^{-1}, F_2}$ (we see in Table 1 that $Q(\sqrt{-T}) \subset K_{H^{-1}, F_2}$). As in the previous case, we need to compute the density of primes which split completely in composition $L_{H^{-1}, F_2} K_{F_1, F_2}$, but not in its degree two extension $L_{H^{-1}, F_2} L_{F_1, F_2}$. Since $\deg L_{H^{-1}, F_2} K_{F_1, F_2} = 32$, in this case the contribution to $C_1$ is equal to $\frac{1}{2} \cdot \frac{1}{64}$. Hence it follows that $C_1 = \frac{5}{32} + \frac{1}{256} + \frac{1}{128} = \frac{63}{256}$. 


To compute the upper bound $C_2$, we need to find the density of the remaining case, $d \in T$ and $\text{III}(E^d)[2] = 2\text{III}(E^d)[4]$, in which our method does not provide us an answer. If $d > 0$, by Proposition 3.9, it is enough to compute the density of primes $p$ which splits completely in $L_{H,H_1, H_2}$ and $L_{H,H_2}$. From Table I, we see that the composition of these three fields have degree 128, hence by Chebotarev density theorem the density of primes with this splitting property is $1/128$, hence contribution to $C_2 - C_1$ is $1/256$.

If $d < 0$ and $d \equiv 7 \pmod{8}$, then $p$ must split completely in $L_{F_1,F_2}, L_{H,F_2}$ and $K = \mathbb{Q}(\sqrt{-2}, \sqrt{13})$ (see Table I), and furthermore it must either split completely in $L = \mathbb{Q}(\sqrt{-2}, \sqrt{13})(\sqrt{4 + 2\sqrt{13}})$ or none of its factors in $K$ splits further in $L$ (note that $L/\mathbb{Q}$ is not Galois extension). One can check that this condition is equivalent for $p$ to split completely in composition $L_{F_1,F_2}L_{H,F_2}$ which is of degree 64, hence the density of such primes is $1/64$, and contribution to $C_2 - C_1$ is equal to $1/128$. Hence $C_2 = C_1 + 1/256 + 1/128 = 46/256$. □

6. Future work

This paper left us with some interesting questions which may be addressed in the future projects:

a) What information can be obtained about $H^d(\mathbb{Q})$ in the case when $\text{III}(E^d)[2] = 2\text{III}(E^d)[4]$?

b) What can one say about $H^d(\mathbb{Q}) \neq \emptyset$ for some larger class of $d$’s? The main reason why we considered only $d$’s for which $|d|$ is prime is that in this case we can control the 2-Selmer group of quadratic twists $E^d$ - we have explicit generators. This might also be the case, for example, for the set of $d$’s which are the products of two primes.

c) Can one obtain similar results for the quartics other that $H$? It seems this could be within the reach of this method provided that, as in b), we have explicit description of 2-Selmer groups of quadratic twists.

Acknowledgments

The author was supported by the Croatian Science Foundation under the project no. IP-2018-01-1313, and by the QuantiXLie Center of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004).

References

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. J. Symbolic Comput., 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BD10] George Boxer and Peter Diao. 2-Selmer groups of quadratic twists of elliptic curves. Proc. Amer. Math. Soc., 138(6):1969–1978, 2010.

[CO15] Mirela Çiperian and Ekin Ozman. Local to global trace questions and twists of genus one curves. Proc. Amer. Math. Soc., 143(9):3815–3826, 2015.

[DD10] Tim Dokchitser and Vladimir Dokchitser. On the Birch-Swinnerton-Dyer quotients modulo squares. Ann. of Math. (2), 172(1):567–596, 2010.

[Des20] Julie Desjardins. Root number of twists of an elliptic curve. J. Théor. Nombres Bordeaux, 32(1):73–101, 2020.

[DF12] Andrej Dujella and Clemens Fuchs. On a problem of Diophantus for rationals. J. Number Theory, 132(10):2075–2083, 2012.

[DKMS17] Andrej Dujella, Matija Kazalicki, Miljen Mikić, and Márton Szikszai. There are infinitely many rational Diophantine sextuples. Int. Math. Res. Not. IMRN, (2):490–508, 2017.

[Dra22] Goran Dražić. Rational $D(q)$-quintuples. Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM, 116(1):Paper No. 9, 18, 2022.
QUADRATIC TWISTS OF GENUS ONE CURVES AND DIOPHANTINE QUINTUPLES

[Duj99] Andrej Dujella. An extension of an old problem of Diophantus and Euler. Fibonacci Quart., 37(4):312–314, 1999.

[Duj02] Andrej Dujella. An extension of an old problem of Diophantus and Euler. II. Fibonacci Quart., 40(2):118–123, 2002.

[Duj16] Andrej Dujella. What is . . . a Diophantine m-tuple? Notices Amer. Math. Soc., 63(7):772–774, 2016.

[Hal98] Emmanuel Halberstadt. Signes locaux des courbes elliptiques en 2 et 3. C. R. Acad. Sci. Paris Sér. I Math., 326(9):1047–1052, 1998.

[Kra81] Kenneth Kramer. Arithmetic of elliptic curves upon quadratic extension. Trans. Amer. Math. Soc., 264(1):121–135, 1981.

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

[Nov22] Lukas Novak. Lokalna rješivost kvadratnih zavrtaja krivulja genusa 1. Diplomski rad, 2022.

[Roh93] David E. Rohrlich. Variation of the root number in families of elliptic curves. Compositio Math., 87(2):119–151, 1993.

[Sil09] Joseph H. Silverman. The arithmetic of elliptic curves, volume 106 of Graduate Texts in Mathematics. Springer, Dordrecht, second edition, 2009.

[Smi16] Alexander Smith. Governing fields and statistics for 4-Selmer groups and 8-class groups. arXiv:1607.07860, 2016.

[Smi22a] Alexander Smith. The distribution of $\ell^\infty$-Selmer groups in degree $\ell$ twist families. arXiv:2207.05674, 2022.

[Smi22b] Alexander Smith. The distribution of fixed point Selmer groups in twist families. arXiv:2207.05143, 2022.

[Sto12] Michael Stoll. Descent on elliptic curves. In Explicit methods in number theory, volume 36 of Panor. Synthèses, pages 51–80. Soc. Math. France, Paris, 2012.

Email address: matija.kazalicki@math.hr