ON RANKS OF QUADRATIC TWISTS OF A MORDELL CURVE

ABHISHEK JUYAL, DUSTIN MOODY AND BIDISHA ROY

Abstract. In this article, we consider the quadratic twists of the Mordell curve $E : y^2 = x^3 - 1$. For a square-free integer k, the quadratic twist of E is given by $E_k : y^2 = x^3 - k^3$. We prove that there exist infinitely many k for which the rank of E_k is 0, by modifying existing techniques. Moreover, using simple tools, we produce precise values of k for which the rank of E_k is 0. We also construct an infinite family of curves $\{E_k\}$ such that the rank of each E_k is positive.

It was conjectured by J. Silverman that there are infinitely many primes p for which $E_p(\mathbb{Q})$ has a positive rank as well as infinitely many primes q for which $E_q(\mathbb{Q})$ has rank 0. We show, assuming the Parity Conjecture, that Silverman's conjecture is true for this family of quadratic twists.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ given by the equation

$$E : y^2 = x^3 + Ax + B, \tag{1}$$

with $A, B \in \mathbb{Z}$ and $4A^3 + 27B^2 \neq 0$. We denote its Mordell–Weil rank as $rank(E)$. Let k be a square-free integer. Then the quadratic twist of E by k, denoted E_k, is an elliptic curve given by the equation

$$E_k : y^2 = x^3 + k^2Ax + k^3B. \tag{2}$$

One can naturally ask that for the family of quadratic twists of a given curve, how are those ranks distributed?

The celebrated conjecture of Goldfeld [13] (see below) asserts that in the quadratic twist family $\{E_k\}$, the *rank* should be 0 (respectively 1) for approximately half of all values of k. More precisely,

Conjecture 1 (Goldfeld [13])**.** *The average rank of the curves E_k is $\frac{1}{2}$, in the sense that*

$$\lim_{X\to\infty} \frac{\sum_{|k|<X} rank(E_k)}{\#\{k : |k| < X\}} = \frac{1}{2},$$

where k runs over all fundamental discriminants.

In particular, statistics of rank 0 quadratic twists of elliptic curves have been an interesting topic of study for some time. Under the Riemann hypothesis, Iwaniec and Sarnak [15] proved that half of the quadratic twists of an elliptic curve have rank 0. Unconditionally, such positive proportion results are only known for a few specific curves (see for instance, [16, 19, 28, 29]). Most of these type of results have taken the approach of utilizing the non-vanishing of L - functions; like the work of Kolyvagin [18]. In general, Goldfeld's conjecture is very much open. There is no evidence yet of any elliptic curve for which Conjecture 1 has been proved.

In recent times, several number theorists have contributed in this area. A. Smith made remarkable progress towards a Selmer-counterpart of Goldfeld's conjecture [26]. More precisely, he proved the following. Suppose $E/\mathbb{Q}$ is an elliptic curve with full rational 2-torsion such that E has no rational cyclic subgroup of order four. Then, if the Birch and Swinnerton-Dyer conjecture

2010 *Mathematics Subject Classification.* 11G05, 11G07, 11G10, 11G40.

Key words and phrases. Twists of curves; Mordell curves; Selmer groups; rank of elliptic curves; root numbers.

holds for the set of twists of E, Goldfeld's conjecture holds for E. For the proof, he estimated the density of natural integers k for which the corank of $Sel^{2^\infty}(E_k) \geq 2$. For a nice exposition on Goldfeld's conjecture for congruent number elliptic curves, one can read the article [4] by Burungale and Tian. The literature on quadratic twists is enriched by several other articles (see, for instances [6, 27]).

Looking at things from a different perspective, Ono and Skinner [22] used the theory of modular forms to estimate that for a fixed elliptic curve E, then $\#\{|k| \leq X : rank(E_k) = 0\} >> X/\log X$. Similarly along these lines, Hofstein and Luo [14] proved that for any fixed E, there exist infinitely many odd square-free integers k (with no more than three prime factors) such that $\text{rank}(E_k) = 0$.

In this article, we will prove some results to add to the aforementioned literature on rank zero quadratic twists. We focus on the family of Mordell curves, which are the curves of the form $y^2 = x^3 - m$, with $m \in \mathbb{Z}$. The family of Mordell curves has been well studied, and its various arithmetic properties (integral points, rational points, rank, etc.) have also been explored (see, for instance, [1, 12, 20, 23, 31]). We will begin with establishing the following theorem.

Theorem 1. *Let E be the elliptic curve $E : y^2 = x^3 - 1$. For any square-free integer k, we have the quadratic twist $E_k : y^2 = x^3 - k^3$. Let $\omega(k)$ be the number of distinct prime divisors of k. Then there exist infinitely many square-free integers k, with $\omega(k) > 1$, such that $rank(E_k) = 0$.*

It is natural to consider the restriction that k be a prime p. In [22], Ono and Skinner observed that when E has conductor ≤ 100, then E_p or E_{-p} is rank zero for a positive proportion of primes. In connection with this, we note the following conjecture of J. Silverman.

Conjecture 2 (Silverman [21], page 250)**.** *If E is an elliptic curve, then there are infinitely many primes p for which $E_p(\mathbb{Q})$ has positive rank, and there are infinitely many primes q for which $E_q(\mathbb{Q})$ has rank 0.*

By using 2-descents, one can prove part of this conjecture for the famous congruent number elliptic curve

$$E' : y^2 = x^3 - x. \tag{3}$$

This follows from the fact that for a prime p with $p \equiv 3 \pmod 8$, then E'_p has rank 0, and if $p \equiv 5 \pmod 8$, then E'_{2p} has rank 0 (for a proof, see [18, Theorem 3.1]). Despite such partial results, Conjecture 2 has not been fully proved.

In the remainder of this paper, we will focus on the family of elliptic curves introduced in Theorem 1.

For this family of curves $\{E_k\}$, we will see in Theorem 2 that Conjecture 2 holds under the assumption of the Parity Conjecture.

Conjecture 3 (Parity Conjecture [2])**.** *Let E be an elliptic curve defined over a number field K. Then*

$$(-1)^{rank(E/K)} = w(E/K),$$

where $w(E/K)$ is the global root number.

Theorem 2. *For the elliptic curve $E_p : y^2 = x^3 - p^3$, we have*

$$rank(E_p) = \begin{cases} 0 & \text{if } p \equiv 5 \pmod{12}, \\ 1 & \text{if } p \equiv 11 \pmod{12} \text{ (assuming the Parity Conjecture).} \end{cases} \tag{4}$$

In the next theorem, we provide some precise values of k for which $rank(E_k)$ is zero.

Theorem 3. *Let k be a square-free positive integer, which satisfies all of the following conditions:*

(a) $k \equiv 1, 5 \pmod{12}$.

(b) The class number h of $\mathbb{Q}(\sqrt{-k})$ is not divisible by 3.
(c) If (U,T) is the fundamental solution of the Pell equation $y^2 - 3kx^2 = 1$, then $U \not\equiv 0 \pmod 3$.

Then the rank(E_k) is 0.

As both Conjecture 1 and Conjecture 2 are concerned with elliptic curves with positive rank, we also establish a few results on curves with positive rank in the following theorem.

Theorem 4. *Let E_k be the curve given by $y^2 = x^3 - k^3$. Then*
(a) There exist infinitely many integers k such that rank(E_k) is positive.
(b) There is an infinite family of curves E_k, over the number field $\mathbb{Q}(m)$, with rank at least 2. Here k and m are related by the following equation:

$$k = \left(\frac{1-2m^2}{m^2+1}\right)^3 - 1.$$

The organization of this paper is as follows. In section 2, we will start by stating some useful known results on the Mordell curve followed by the proof of Theorem 1 and Theorem 2. In order to prove Theorems 1 and 2, we will use the standard 2- descent method via evaluating the solutions of several principal homogeneous spaces over local fields. In section 3, we will prove Theorem 3 by using the Scholz reflection principal [25] and basics of Pell-equations and Diophantine equations. Finally, in the last section, we conclude by constructing certain families of curves with positive rank as mentioned in Theorem 4. For this purpose, we use some of the well known results on elliptic curves.

2. Proofs of Theorem 1 and Theorem 2

Let k be a sixth-power-free integer such that E^k is given by the Weierstrass equation $E^k : y^2 = x^3 + k$. The torsion structure of the curves $E^k(\mathbb{Q})$ is well-known. The following lemma classifies the torsion of E.

Lemma 1 ([24])**.**

$$E^k(\mathbb{Q})_{tors} = \begin{cases} \mathbb{Z}/6\mathbb{Z} & \text{if } k = 1, \\ \mathbb{Z}/3\mathbb{Z} & \text{if } k \neq 1 \text{ is a square, or if } k = -432, \\ \mathbb{Z}/2\mathbb{Z} & \text{if } k \neq 1 \text{ is a cube,} \\ 1 & \text{otherwise.} \end{cases} \tag{5}$$

We will need the doubling formulas for a point on E^k, which are provided below. It is a straightforward calculation from the addition law.

Lemma 2 ([24])**.** *Let $P = (x,y)$ be a point on E^k. Then the double of P, i.e. $[2]P = P + P = (x_{[2]P}, y_{[2]P})$, has coordinates given by the following formulae:*

$$x_{[2]P} = \frac{9x^4 - 8y^2x}{4y^2},\ y_{[2]P} = \frac{-27x^6 + 36y^2x^3 - 8y^4}{8y^3}.$$

As the main ingredient to prove Theorem 1 and Theorem 2 is the 2-descent method, we briefly give the necessary background (for further details [24, Chapter X]).

We consider the quadratic twist $E_k : y^2 = x^3 - k^3$ of the Mordell curve $E : y^2 = x^3 - 1$. It is easy to check that E_k has a 2- torsion point, namely $(k, 0)$. Corresponding to the 2-torsion point, there is a 2-isogeny $\phi : E_k \longrightarrow E'_k$ which has the kernel $\{\mathcal{O}, (k,0)\}$. It can be checked that the image curve is

$$E'_k : y^2 = x^3 - 6kx^2 - 3k^2x,$$

with ϕ given by

$$\phi(x,y) = \left(\frac{y^2}{(x-k)^2}, \frac{y(3k^2-(x-k)^2)}{(x-k)^2} \right).$$

Using standard techniques of Galois cohomology, we obtain an exact sequence:

$$0 \to \frac{E'_k(\mathbb{Q})}{\phi(E_k(\mathbb{Q}))} \to Sel^{(\phi)}(E_k/\mathbb{Q}) \to Ш(E_k/\mathbb{Q})[\phi] \to 0,$$

where $Sel^{(\phi)}(E_k/\mathbb{Q})$ is the ϕ-Selmer group and $Ш(E_k/\mathbb{Q})[\phi]$ is the ϕ-torsion part of the Tate-Shafarevich group. The above is also true for the dual isogeny $\widehat{\phi}$

$$0 \to \frac{E_k(\mathbb{Q})}{\widehat{\phi}(E'_k(\mathbb{Q}))} \to Sel^{(\widehat{\phi})}(E'_k/\mathbb{Q}) \to Ш(E'_k/\mathbb{Q})[\widehat{\phi}] \to 0.$$

For a square-free positive integer k, define a finite set S of prime divisors of the rational numbers $\mathbb{Q}$ by

$$S = \{\infty\} \cup \{\text{primes } p : p|6k\}.$$

Let M be the multiplicative subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by -1 and the divisors of $6k$. For each $d \in M$ we have the homogeneous spaces C_d and C'_d defined by

$$C_d : dw^2 = d^2t^4 - 6dkt^2z^2 - 3k^2z^4,$$
$$C'_d : dw^2 = d^2t^4 + 3dkt^2z^2 - 3k^2z^4.$$

The Selmer group $Sel^{(\phi)}(E_k/\mathbb{Q})$ (respectively $Sel^{(\hat{\phi})}(E_k/\mathbb{Q})$) measures the possibility of C_d (or C'_d) having non-trivial solutions in the local field $\mathbb{Q}_v$ for all $v \in S$. Namely

$$Sel^{(\phi)}(E_k/\mathbb{Q}) = \{d \in M : C_d(\mathbb{Q}_v) \neq \emptyset \text{ for all } v \in S\},$$
$$Sel^{(\hat{\phi})}(E'_k/\mathbb{Q}) = \{d \in M : C'_d(\mathbb{Q}_v) \neq \emptyset \text{ for all } v \in S\},$$

where $C_d(\mathbb{Q}_v) \neq \emptyset$ or $(C'_d(\mathbb{Q}_v) \neq \emptyset)$ means that the homogeneous space C_d or (C'_d) has non-trivial solutions $(w,t,z) \neq (0,0,0)$ in $\mathbb{Q}_v$.

We note that $\{1,-3\} \subseteq Sel^{(\phi)}(E_k/\mathbb{Q})$ and $\{1,3\} \subseteq Sel^{(\widehat{\phi})}(E'_k/\mathbb{Q})$ because each of the homogeneous spaces C_1, C_{-3}, C'_1, C'_3 has a non-trivial solution in $\mathbb{Q}$ (proofs can be found in Lemma 4 and Lemma 5 below).

We will establish a series of results in the form of lemmas which will culminate in proving Theorem 1. The first lemma gives an upper bound on the rank of $E_k(\mathbb{Q})$ in terms of the size of the Selmer groups. The remaining lemmas will provide conditions on k such that these upper bounds for the desired ranks are 0.

Lemma 3 ([17])**.** *Let $E/\mathbb{Q}$ be an elliptic curve with a rational point of order 2. Let $\phi : E \to E'$ be an isogeny of degree 2, with $\widehat{\phi} : E' \to E$ the dual of ϕ. Then*

$$rank(E(\mathbb{Q})) \leq dim_{\mathbb{F}_2} Sel^{(\phi)}(E,\mathbb{Q}) + dim_{\mathbb{F}_2} Sel^{(\widehat{\phi})}(E',\mathbb{Q}) - 2.$$

We now turn to finding conditions on k such that the homogeneous spaces $C_d(\mathbb{Q}_v)$ and $C'_d(\mathbb{Q}_v)$ are non-empty for each local field $\mathbb{Q}_v$. The first lemma deals with $C'_d(\mathbb{Q}_v)$, and the second with $C_d(\mathbb{Q}_v)$.

Lemma 4. *Let k be a square-free integer with $\gcd(k,6) = 1$ and $M \subseteq \mathbb{Q}^*/\mathbb{Q}^{*^2}$ be the multiplicative subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by -1 and the prime divisors of $6k$. Let p be an odd prime. For any $d \in M$, we have the following cases:*

(1) $C'_d(\mathbb{Q}_2) = \emptyset \Leftrightarrow 2 \mid d$.
(2) If $3 \nmid d$, then $C'_d(\mathbb{Q}_3) = \emptyset \Leftrightarrow d \equiv 2 \pmod 3$.

(3) If $d = 3d'$, then $C'_d(\mathbb{Q}_3) = \emptyset \Leftrightarrow d' \equiv 2 \pmod 3$.

(4) If $p \mid d$, then $C'_d(\mathbb{Q}_p) \neq \emptyset \Leftrightarrow \begin{cases} \left(\frac{-3}{p}\right) = 1 \text{ and} \\ \text{either } \left(\frac{k/d(-6+2\sqrt{-3})}{p}\right) = 1 \text{ or } \left(\frac{k/d(-6-2\sqrt{-3})}{p}\right) = 1. \end{cases}$

(5) If $p \mid \frac{k}{d}$, then $C'_d(\mathbb{Q}_p) = \emptyset \Leftrightarrow \left(\frac{3}{p}\right) = 1 = -\left(\frac{d}{p}\right)$.

(6) For $d > 0$, $C_d(\mathbb{R}) \neq \emptyset$.

(7) $3 \in S^{(\widehat{\phi})}(E'_k, \mathbb{Q})$.

(8) $d < 0 \Leftrightarrow C'_d(\mathbb{Q}_\infty) = \emptyset$.

Proof. In this proof, for a prime p, we denote the standard p-adic valuation by v_p. Let us recall that $C'_d : dw^2 = d^2t^4 + 3kdt^2z^2 + 3k^2z^4$. The main goal is to determine solutions of this principal homogeneous space over certain p-adic fields. In each case '$\Leftarrow$' denotes the converse case and '$\Rightarrow$' denotes the forward case.

(1) $\Leftarrow$ Let $(w,t,z) \neq (0,0,0)$ be a solution of C'_d in $\mathbb{Q}_2$. For a d with $2 \mid\mid d$, $\min\{2 + 4v_2(t), 1 + 2v_2(t) + 2v_2(z), 4v_2(z)\} = 1 + 2v_2(w)$. Since $2 + 4v_2(t)$, $v_2(z)$ and $1 + 2v_2(w)$ are distinct modulo 4, the minimum of the above set is $2v_2(t) + 2v_2(z) + 1$. Hence we have $2(2v_2(t)+2v_2(z)+1) \leq 2+4v_2(t)+4v_2(z) \Rightarrow 2(2v_2(t)+v_2(z)) \leq 4v_2(t)+4v_2(z)-2$ which is a contradiction. Thus we conclude that for any d with $2 \mid d$, we have $C'_d = \emptyset$.
$\Rightarrow$ Suppose $v_2(d) = 0$. We claim that $C'_d(\mathbb{Q}_2) \neq \emptyset$. We choose $v_2(w) = v_2(t) = 0$ and $v_2(z) > 0$. As d is not even, $\sqrt{d} \in \mathbb{Q}_2$, therefore $(\sqrt{d}, 1, 0) \in \mathbb{Q}_2 \times \mathbb{Q}_2 \times \mathbb{Q}_2$ and it is a solution of $C'_d(\mathbb{Q}_2)$.

(2) $\Rightarrow$ Suppose $d \equiv 1 \pmod 3$ which implies $\left(\frac{d}{3}\right) = 1$. After putting $z = 0$ and $t = 1$, the reduced C'_d is $w^2 = d$ and it has a solution modulo 3 because $\left(\frac{d}{3}\right) = 1$. Now, using Hensel's lemma, $w^2 = d$ has a solution in $\mathbb{Q}_3$ and thus $C'_d(\mathbb{Q}_3) \neq \emptyset$.
$\Leftarrow$ Let $(w,t,z) \neq (0,0,0)$ be a solution of C'_d in $\mathbb{Q}_3$. Suppose $v_3(w) = \alpha$, $v_3(t) = \beta$ and $v_3(z) = \gamma$. As $3 \nmid d$, we get $v_3(dw^2) = 2\alpha = \min\{v_3(d^2t^4), v_3(3dkt^2z^2), v_3(3k^2z^4)\} = \{4\beta, 1+2\beta+2\gamma, 1+4\gamma\}$ which forces $\alpha = 2\beta$. Now we can assume $\alpha = \beta = 0$ and $\gamma \geq 0$. Using this information, the equation C'_d, modulo 3 gives $d \equiv \left(\frac{w}{t^2}\right)^2 \pmod 3 \Leftrightarrow \left(\frac{d}{3}\right) = 1$. This contradicts the fact that $d \equiv 2 \pmod 3$.

(3) $\Rightarrow$ Let (w,t,z) be a solution of C'_d such that $\alpha := v_3(w)$, $\beta := v_3(t), \gamma := v_3(z)$. Then we get $v_3(dw^2) = 1+2\alpha$, $v_3(d^2t^4) = 2+4\beta$, $v_3(3kdt^2z^2) = 2+2\beta+2\gamma$ and $v_3(3k^2z^4) = 1+4\gamma$. It says $1 + 2\alpha = \min\{2 + 4\beta, 2 + 2\beta + 2\gamma, 1 + 4\gamma\}$ and we can conclude further that $1+2\alpha = 1+4\gamma$. It is enough to assume $\alpha = \gamma = 0$. From the equation of C'_d, we conclude that

$$3d'w^2 = 3^2(d')^2t^4 + 3^2kd't^2z^2 + 3k^2z^4.$$

After dividing by 3 and taking modulo 3, we get $d'w^2 \equiv k^2z^4 \pmod 3$ which implies $d' \equiv 1 \pmod 3$.
$\Leftarrow$ Conversely, we assume that $d' \equiv 1 \pmod 3$ and consider the polynomial $G(w', 1, z) := -d'(w')^2 + 3(d')^2 + 3kd'z^2 + k^2z^4$. Note that $G(1,1,1) \equiv 0 \pmod 3$ as $d' \equiv 2 \pmod 3$. Also note that $3 \nmid \frac{\partial G}{\partial w}(1,1,1)$. By Hensel's Lemma, there exists an element $(w_0, t_0, z_0) \in (\mathbb{Z}_3)^3$ such that $G(w_0, t_0, z_0) = 0$ which provides a suitable solution for C'_d over $\mathbb{Q}_3$.

(4) $\Rightarrow$ Suppose $(w,t,z) \neq (0,0,0)$ is a solution of C'_p in $\mathbb{Q}_p$. Then comparing the p - adic valuation of two sides of C'_p, we get that $v_p(w) \geq 1$. Hence $\frac{w^2}{p} = t^4 + 3\frac{k}{d}t^2z^2 + 3\left(\frac{k}{d}z^2\right)^2$, gives

$$t^4 + 3\frac{k}{d}t^2z^2 + 3\left(\frac{k}{d}z^2\right)^2 \equiv 0 \pmod p;$$
$$d^2(t^2)^2 + 3kdz^2t^2 + 3(kz^2)^2 \equiv 0 \pmod p.$$

The above equation has a solution in $\mathbb{F}_p^*$ implies $t^2 = \frac{-2kdz^2(3\pm\sqrt{-3})}{4d^2} \Leftrightarrow t = \pm\sqrt{\frac{-2kdz^2(3\pm\sqrt{-3})}{4d^2}}$ are solutions in $\mathbb{F}_p^*$.

Thus $C'_p(\mathbb{Q}_p) \neq \emptyset$ implies $\left(\frac{-3}{p}\right) = 1$ and either $\left(\frac{k/d(-6+2\sqrt{-3})}{p}\right) = 1$ or $\left(\frac{k/d(-6-2\sqrt{-3})}{p}\right) = 1$ holds.

$\Leftarrow$ We take $w = 0$ and $t = 1$ to reduce C'_d as $d^2t^4 + 3dkt^2 + 3k^2 = 0$. Since $\left(\frac{-3}{p}\right) = 1$, we have $\sqrt{-3} \in \mathbb{Q}_p$. For having a solution in the reduced C'_d, we need to satisfy $t^2 = \frac{-2dk(3\pm\sqrt{-3})}{4d^2}$ which holds according to the assumption. Thus by Hensel's lemma, there exists $t = \alpha \in \mathbb{Q}_p$ such that $(w, z, t) = (0, 1, \alpha)$ is a solution of C'_d in $\mathbb{Q}_p$.

(5) $\Rightarrow$ After taking $z = 0$ and $t = 1$, we have $w^2 = d$ which has a solution in $\mathbb{Q}_p$ if $\left(\frac{d}{p}\right) = 1$ holds. Since $C'_d(\mathbb{Q}_p) = \emptyset$, we conclude $\left(\frac{d}{p}\right) = -1$. After choosing $z = 1$ and $t = 0$, we get $dw^2 = 3k^2$ and it has a solution in $\mathbb{Q}_p$ if $\left(\frac{3d}{p}\right) = 1$. Since $\left(\frac{d}{p}\right) = -1$, therefore we obtain $\left(\frac{3}{p}\right) = 1$.

$\Leftarrow$ We assume that $(w, t, z) \neq (0, 0, 0)$ be a solution of C_d in $\mathbb{Q}_p$. Suppose $v_3(w) = \alpha$, $v_3(t) = \beta$ and $v_3(z) = \gamma$. Since $p \nmid d$, we obtain

$$v_3(dw^2) = 2\alpha = \min\{v_3(d^2t^4), v_3(3dkt^2z^2), v_3(3k^2z^4)\} = \{4\beta, 1 + 2\beta + 2\gamma, 2 + 4\gamma\}$$

which forces that either $\alpha = 2\beta$ or $2\alpha = 2 + 4\gamma$. First, we consider $\alpha = 2\beta$ which implies $\alpha = \beta = 0$ and $\gamma \geq 0$. For this case, C'_p modulo p says $dw^2 \equiv d^2t^4 \pmod{p}$ which implies $\left(\frac{d}{p}\right) = 1$. This contradicts our assumption. In second, we consider $2\alpha = 2 + 4\gamma$. In this case, we can consider $\gamma = 0$ and $\alpha = 1$. Hence we obtain $\beta \geq 1$. Now, let $w = pw'$ and $t = pt'$ which tells $v_p(w') = 0 \leq v_p(t')$. Invoking this information in C'_p, we get

$$d(pw')^2 = d^2(pt')^4 + 3dk(pt')^2z^2 + 3k^2z^4$$

which is divisible by p^2 in both sides. Dividing both sides by p^2, we obtain

$$dw'^2 \equiv 3\left(\frac{k}{p}\right)^2 z^4 \pmod{p}.$$

Since $\left(\frac{3}{p}\right) = 1$, we get $\left(\frac{d}{p}\right) = 1$ which contradicts our assumption.

(6) As d is non zero, we can re-write C'_d as $w^2 = dt^4 + 3kt^2z^2 + \frac{3}{d}k^2z^4$. For $d > 0$, it has a solution in $\mathbb{R}$ namely $(\sqrt{d}, 1, 0)$.

(7) From (1), we get that $C'_3(\mathbb{Q}_2) \neq \emptyset$. Again using (3), we obtain $C'_3(\mathbb{Q}_3) \neq \emptyset$. For other primes also $C'_3(\mathbb{Q}_p) \neq \emptyset$ by (5). Hence we conclude this case by (6).

□

Lemma 5. *Let k be a square-free integer with $\gcd(k, 6) = 1$ and $M \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$ be the multiplicative subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by -1 and the prime divisors of $6k$. Let p be an odd prime. For any $d \in M$, we have the following cases:*

(1) If $2 \mid d$, then $C_d(\mathbb{Q}_2) = \emptyset$.
(2) If $\gcd(2, d) = 1$, then
  (i) $C_d(\mathbb{Q}_2) \neq \emptyset \Rightarrow d \equiv 1, -k, 2 - k \pmod{4}$
  (ii) $d \equiv 1 \pmod{4} \Rightarrow C_d(\mathbb{Q}_2) \neq \emptyset$.
(3) If $3 \nmid d$, then $C_d(\mathbb{Q}_3) = \emptyset \Leftrightarrow d \equiv 2 \pmod{3}$.
(4) If $d = 3d'$, then $C_d(\mathbb{Q}_3) = \emptyset \Leftrightarrow d' \equiv 1 \pmod{3}$.

(5) *For any* $p \mid d$, *we have* $C_d(\mathbb{Q}_p) = \emptyset \Leftrightarrow \begin{cases} \left(\frac{3}{p}\right) = -1 \text{ or} \\ \left(\frac{3}{p}\right) = \left(\frac{-1}{p}\right) = -\left(\frac{-3}{p}\right)_4 \left(\frac{k/d}{p}\right) = 1. \end{cases}$

$$\Updownarrow$$

For any $p \mid d$, *we have* $C_d(\mathbb{Q}_p) \neq \emptyset \Leftrightarrow \begin{cases} \left(\frac{3}{p}\right) = 1 \text{ and} \\ \text{either } \left(\frac{k/d(-3+2\sqrt{3})}{p}\right) = 1 \text{ or } \left(\frac{k/d(-3-2\sqrt{3})}{p}\right) = 1. \end{cases}$

(6) *If* $p \mid \frac{k}{d}$, *then* $C_d(\mathbb{Q}_p) = \emptyset \Leftrightarrow p \equiv 1 \pmod 3$ *and* $\left(\frac{d}{p}\right) = -1$.

(7) $C_d(\mathbb{R}) \neq \emptyset$.

(8) $-3 \in S^{(\phi)}(E_k, \mathbb{Q})$.

Proof. Let us recall that $C_d : dw^2 = d^2t^4 - 6kdt^2z^2 - 3k^2z^4$. Cases $(1), (3), (5), (6)$ have been proved in [12, Lemma 3], so we omit the details here.

(2) (i) Assume $(w, t, z) \in \mathbb{Q}_2 \times \mathbb{Q}_2 \times \mathbb{Q}_2$ which lies in $C_d(\mathbb{Q}_2)$. Also assume that $\alpha = v_2(w), \beta = v_2(t), \gamma = v_2(z)$ such that $w = 2^\alpha w_1$, $t = 2^\beta t_1$ and $z = 2^\gamma z_1$. Then $2\alpha = \min\{4\beta, 1 + 2\beta + 2\gamma, 4\gamma\}$. We first assume that $\alpha = \beta = 0$ and $\gamma > 0$. Reducing modulo 8, we get $d \equiv \frac{w^2}{t^4} \pmod 8$ which implies $d \equiv 1 \pmod 8$.

Next we assume $\beta > 0$ and $\gamma < 0$ which implies $\alpha = 2\gamma$. Using this, we get

$$2^{4\gamma} dw_1^2 = d^2 2^{4\beta} t_1^4 - 6kd 2^{2\beta} t_1^2 2^{2\gamma} z_1^2 - 3k^2 2^{4\gamma} z_1^4.$$

After dividing by $2^{4\gamma}$, we get

$$dw_1^2 = 2^{4\beta - 4\gamma} d^2 t_1^4 - 6kd 2^{2\beta - 2\gamma} t_1^2 z_1^2 - 3k^2 z_1^4.$$

Reducing modulo 8, we get $dw_1^2 \equiv -3k^2 z_1^4 \pmod 8$ which implies $d \equiv 5 \pmod 8$. If $\beta = \gamma = 0$, then $v_2(d^2t_1^4 - 6kdt_1^2z_1^2 - 3k^2z_1^4) > 0$ which implies $\alpha \geq 1$. Hence $2^{2\alpha}d \equiv 1 - 2kd - 3 \pmod 4 \equiv -2(1 + kd) \pmod 4 \Leftrightarrow kd \equiv -1 - 2^{2\alpha - 1}d \pmod 4$. Thus for $\alpha > 1$, $d \equiv -k \pmod 4$ and for $\alpha = 1$, $d \equiv 2 - k \pmod 4$.

(ii)

In this case, we can assume either $d \equiv 1 \pmod 8$ or $d \equiv 5 \pmod 8$. When $d \equiv 1 \pmod 8$, then consider

$$H_s(w, z) = -dw^2 + d^2 - 2^{1+2s} 3kdz^2 - 2^{4s} 3k^2 z^4.$$

Note that $H_s(1, 1) \equiv 0 \pmod 8$ because $s > 0$. Also note that $\frac{\partial H_s}{\partial w}(1, 1) = -2d \equiv 2 \pmod 4$. Since $v_2(H_s(1, 1)) > 2v_2(\frac{\partial H_s}{\partial y}(1, 1))$, we can use Hensel's lemma to get a solution (w_0, z_0) of $H_s(w, t)$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$. Then $(w_0, 1, 2^s z_0)$ be a solution of C_d over $\mathbb{Q}_2$.

When $d \equiv 5 \pmod 8$, then we consider

$$H'_s(w, z) = -dw^2 + 2^{4s} d^2 - 2^{1+2s} 3kdz^2 - 3k^2 z^4.$$

Again applying Hensel's lemma as above, we get $(2^{-2s} w_0, 2^s, 2^{-s}, z_0)$ as a solution od C_d over $\mathbb{Q}_2$.

(4) This case is exactly similar to Lemma 4 (case (3)). So, we omit the details here.

(7) Proof is similar to the proof of Lemma 4 (case (6)).

(8) This case is analogous to Lemma 4, (case (8)).

□

Using the above information, next we prove the following proposition.

Proposition 1. *let* $k = p_1 \cdots p_j$ *be a natural number such that* $p_i \equiv 5 \pmod{12}$, *for* $1 \leq i \leq j$. *Then* $Sel^{(\widehat{\phi})}(E'_k, \mathbb{Q}) = \{-1, 3\}$ *and* $Sel^{(\phi)}(E_k, \mathbb{Q}) = \{1, -3\}$.

Proof. For a prime p_i in the given form, we get $\left(\frac{-3}{p_i}\right) = -1$. We choose a $d \in M$ divisible by p_i, for some i. Thus we can use Lemma 4 (case (4)) to conclude the $C'_d(\mathbb{Q}_{p_i}) = \emptyset$ which implies that when some $p_i \mid d$, then d does not belong to $Sel^{(\widehat{\phi})}(E'_k, \mathbb{Q})$.

When d is even, then by Lemma 4 (case (1)), we get $C'_d(\mathbb{Q}_2) = \emptyset$. Since M is a subgroup of $\mathbb{Q}^*$ modulo the squares generated by $(S \setminus \{\infty\}) \cup \{-1\}$, the above implies that $Sel^{(\widehat{\phi})}(E'_k/\mathbb{Q}) \subseteq \{-1, 3\}$. Finally, the equality holds by Lemma 4 (case (7)).

Similarly, we can conclude $Sel^{(\phi)}(E_k, \mathbb{Q}) = \{1, -3\}$ by using Lemma 5 and analogously reasoning . □

We are now ready to give a proof of Theorem 1.

Proof of Theorem 1: By Proposition 1, we have seen that there are infinitely many non-square values of k such that the Selmer groups $Sel^{(\phi)}(E_k/\mathbb{Q})$ and $Sel^{(\widehat{\phi})}(E'_k/\mathbb{Q})$ are equal to $\{1, -3\}$ and $\{-1, 3\}$ respectively. Namely, any k which is a product of distinct primes each congruent to 5 mod 12. If we consider the Selmer groups as $\mathbb{F}_2$ vector spaces, then $dim_{\mathbb{F}_2} Sel^{(\widehat{\phi})}(E'_k, \mathbb{Q}) = 1$ and also $dim_{\mathbb{F}_2} Sel^{(\phi)}(E_k, \mathbb{Q}) = 1$. Thus by Lemma 3, for the curve $E_k/\mathbb{Q}$ we have that rank $(E_k(\mathbb{Q})) \leq 1 + 1 - 2 = 0$, which finishes the proof. □

In the next proposition we will see that what happens if we consider quadratic twists by primes. This will be useful towards proving Theorem 2.

Proposition 2. *Let p_1 be a prime, with the Selmer groups as defined above. Then*

$$S^{(\widehat{\phi})}(E'_{p_1}, \mathbb{Q}) = \begin{cases} \langle 3, p_1 \rangle; & \text{if } p_1 \equiv 7 \pmod{12}, \\ & \text{or } p_1 \equiv 1 \pmod{12} \text{ and } \left(\frac{-6-2\sqrt{-3}}{p_1}\right) = 1, \\ \langle 3 \rangle; & \text{if } p_1 \equiv 5, 11 \pmod{12}, \\ & \text{or } p_1 \equiv 1 \pmod{12} \text{ and } \left(\frac{-6-2\sqrt{-3}}{p_1}\right) = -1. \end{cases}$$

Proof. We begin by noting that $\{-1, 3\} \subseteq S^{(\widehat{\phi})}(E'_{p_1}, \mathbb{Q}) \subset \langle -1, 2, 3, p_1 \rangle$, using the definition of Selmer group and Lemma 4 (case (7)). We divide the proof into following two cases:

Case (1): Assume $p_1 \equiv 2 \pmod 3$. Now using Lemma 4 (case (1), (2) and (6)), we get that $S^{(\widehat{\phi})}(E^{(p_1)'}, \mathbb{Q}) \subset \langle 1, 3, p_1 \rangle$. Since -3 is a quadratic non-residue modulo p_1, we get $S^{(\widehat{\phi})}(E'_{p_1}, \mathbb{Q}) \not\supset \langle p_1 \rangle$, using Lemma 4 (case (4)). Since $p_1 \equiv 2 \pmod 3$ if and only if either $p_1 \equiv 5 \pmod{12}$ or $p_1 \equiv 11 \pmod{12}$, therefore in these two cases $S^{(\widehat{\phi})}(E'_{p_1}, \mathbb{Q}) = \langle 3 \rangle$.

Case (2): Next, we assume $p_1 \equiv 1 \pmod 3$. In this case $C'_{p_1}(\mathbb{Q}_3) \neq \emptyset$ and $C'_{p_1}(\mathbb{Q}_2) \neq \emptyset$, by Lemma 4 (case (3)) and Lemma 4 (case (1)) respectively. Next we consider the following two sub cases.

Subcase (i): We assume $p_1 \equiv 7 \pmod{12}$. For these choices of primes, we have $\left(\frac{-3}{p_1}\right) = 1$. Since $\left(\frac{-6+2\sqrt{-3}}{p_1}\right)\left(\frac{-6-2\sqrt{-3}}{p_1}\right) = \left(\frac{48}{p_1}\right) = \left(\frac{3}{p_1}\right) = -1$, we conclude either $\left(\frac{-6-2\sqrt{-3}}{p_1}\right) = 1$ or $\left(\frac{-6+2\sqrt{-3}}{p_1}\right) = 1$. Using Lemma 4 (case (4)), we obtain $\langle p_1, 3 \rangle = S^{(\widehat{\phi})}(E'_{p_1}, \mathbb{Q})$.

Subcase (ii): We assume $p_1 \equiv 1 \pmod{12}$. For these choices of primes, we have $\left(\frac{3}{p_1}\right) = 1$ and $\left(\frac{-1}{p_1}\right) = 1$ which imples $\left(\frac{-3}{p_1}\right) = 1$. Since $\left(\frac{-6+2\sqrt{-3}}{p_1}\right)\left(\frac{-6-2\sqrt{-3}}{p_1}\right) = \left(\frac{48}{p_1}\right) = \left(\frac{3}{p_1}\right) = 1$, therefore we observe that either $\left(\frac{-6-2\sqrt{-3}}{p_1}\right) = \left(\frac{-6+2\sqrt{-3}}{p_1}\right) = 1$ or $\left(\frac{-6-2\sqrt{-3}}{p_1}\right) = \left(\frac{-6+2\sqrt{-3}}{p_1}\right) = -1$. Using Lemma 4 (case (4)), we can conclude the proof.

□

Proposition 3. *Let p_2 be a prime, with the Selmer groups as defined above. Then*

$$S^{(\phi)}(E_{p_2},\mathbb{Q}) = \begin{cases} \langle -p_2,-3\rangle; & \text{if } p_2 \equiv 11 \pmod{12}, \\ \langle p_2,-3\rangle; & \text{or } p_2 \equiv 1 \pmod{12} \text{ and } \left(\frac{3+2\sqrt{3}}{p_2}\right)=1, \\ \langle -3\rangle; & \text{if } p_2 \equiv 5,7 \pmod{12}, \\ & \text{or } p_2 \equiv 1 \pmod{12} \text{ and } \left(\frac{3+2\sqrt{3}}{p_2}\right)=-1. \end{cases}.$$

Proof. By definition we note that $\{1,-3\} \subseteq S^{(\phi)}(E_{p_2},\mathbb{Q}) \subset \langle -1,2,3,p_2\rangle$. Again we split the proof into two following two cases:

Case (1): Assume $p_2 \equiv 2 \pmod 3$. Using Lemma 5 (cases (2)- (4)) we get that $S^{(\phi)}(E_{p_2},\mathbb{Q}) \subset \{1,-3,-p_2,3p_2\}$. Now, we consider two following sub-cases.

Subcase (i): At first, we assume $p_2 \equiv 5 \pmod{12}$. Since $\left(\frac{-1}{p_2}\right) = 1 \Leftrightarrow p_2 \equiv 1 \pmod 4$, in this case $\left(\frac{3}{p_2}\right) = -1$. By Lemma 5 (case (5)), we get $-p_2 \notin S^{(\phi)}(E_{p_2},\mathbb{Q})$ and hence $S^{(\phi)}(E_{p_2},\mathbb{Q}) = \langle -3\rangle$.

Subcase (ii): Next, we assume $p_2 \equiv 11 \pmod{12}$. In this case $\left(\frac{3}{p_2}\right) = 1$ and $\left(\frac{3+2\sqrt{3}}{p_2}\right)\left(\frac{3-2\sqrt{3}}{p_2}\right) = \left(\frac{-3}{p_2}\right) = -1$, since $\left(\frac{-1}{p_2}\right) = -1$. By Lemma 5 (5), we get $C_{-p_2}(\mathbb{Q}_{p_2}) \neq \emptyset$. Since $-p_2 \equiv 1 \pmod 4$, by Lemma 5 (2), $C_{-p_2}(\mathbb{Q}_2) \neq \emptyset$. Again $C_{-p_2}(\mathbb{Q}_3) \neq \emptyset$, by Lemma 5 (3). Hence $S^{\phi}(E_{p_2},\mathbb{Q}) = \langle -3,-p_2\rangle$, using Lemma 5 (case (7)).

Case (2): For $p_2 \equiv 1 \pmod 3$, we directly focus on the following two subcases.

Subcase (i): We assume $p_2 \equiv 7 \pmod{12}$. For these choices of prime, we get $\left(\frac{3}{p_2}\right) = -1$. Using Lemma 5 (5), we get $\langle -3\rangle = S^{(\phi)}(E_{p_2},\mathbb{Q})$.

Subcase (ii): We assume $p_2 \equiv 1 \pmod{12}$. For these choices of prime, we get $\left(\frac{3}{p_2}\right) = 1 = \left(\frac{-1}{p_2}\right)$. Since $\left(\frac{3\pm2\sqrt{3}}{p_2}\right) = \left(\frac{-3}{p_2}\right) = 1$, we observe that $\left(\frac{3+2\sqrt{3}}{p_2}\right) = 1 \Leftrightarrow \left(\frac{3-2\sqrt{3}}{p_2}\right) = 1$. By Lemma 5 (5), for $\left(\frac{3+2\sqrt{3}}{p_2}\right) = 1$, we get $C_{p_2}(\mathbb{Q}_{p_2}) \neq \emptyset$. Since $p_2 \equiv 1 \pmod 4$, by Lemma 5 (2), $C_{p_2}(\mathbb{Q}_2) \neq \emptyset$. Again $C_{p_2}(\mathbb{Q}_3) \neq \emptyset$, by Lemma 5 (3). Hence $S^{\phi}(E_{p_2},\mathbb{Q}) = \langle -3,p_2\rangle$, using Lemma 5 (7).

□

Now we are ready to prove Theorem 2.

Proof of Theorem 2: For $p := p_1 = p_2 \equiv 5 \pmod{12}$, we get $S^{(\widehat{\phi})}(E'_p,\mathbb{Q}) = \langle 3\rangle$, by Proposition 2 and $S^{(\phi)}(E_p,\mathbb{Q}) = \langle -3\rangle$, by Proposition 3. Hence using this information in Lemma 1, we have $rank(E_p(\mathbb{Q})) = 0$.

For $p := p_1 = p_2 \equiv 11 \pmod{12}$, we get $S^{(\widehat{\phi})}(E'_p,\mathbb{Q}) = \langle 3\rangle$, by Proposition 2 and $S^{(\phi)}(E_p,\mathbb{Q}) = \langle -3,-p\rangle$, by Proposition 3. Hence using this information in Lemma 1, we have $rank(E_p(\mathbb{Q})) \leq 2+1-2 = 1$. For this curve, the global root number is -1 which can be seen in [11]. From Conjecture 3, we observe that $rank(E_p(\mathbb{Q}))$ is odd and this concludes the proof. □

3. proof of Theorem 3

In this section we prove Theorem 3, which was stated in the introduction. Before giving the proof, we need the following result.

Theorem 5. [25, Schloz reflection principal] *Let $k > 1$ be square-free. Let r be the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{-k})$ and s the $3-$rank of the ideal class group of $\mathbb{Q}(\sqrt{3k})$. Then $r \leq s \leq r+1$.*

We will also need the following proposition.

Proposition 4. *Let k be a square-free positive integer. Suppose that the following conditions hold:*

(a) $k \equiv 1 \pmod 4$ *and* $k \not\equiv 0 \pmod 3$.
(b) The class number h of $\mathbb{Q}(\sqrt{-k})$ is not divisible by 3.
(c) If $(x, y) = (U, T)$ is the fundamental solution of the Pell equation $y^2 - 3kx^2 = 1$, then $U \not\equiv 0 \pmod 3$.

Then $\{(x, y) \in E_{k^3}(\mathbb{Q}) : \mathrm{ord}_p(y) \leq 0 \text{ for all prime factors } p|3k\} = \emptyset$.

Proof. It is clear that Proposition 4 is equivalent to showing that the equation

$$y^2 = x^3 - k^3 z^6 \tag{6}$$

with $\gcd(x, y, z) = 1$, has no integer solutions $(x, y, z) \in \mathbb{Z}^3$ such that $y \neq 0, z \neq 0$ and $\gcd(y, 3k) = 1$. Without loss of generality, we assume that $(x, y, z) \in \mathbb{Z}^3$ is a solution of the equation (6) with $z > 0, y > 0, \gcd(y, 3k) = 1$ and z is minimal. We first prove the following claim.

Claim: x is odd.

If x is even, then we conclude z is odd otherwise $2 \mid x$ and $2 \mid z$ imply that $2 \mid y$ which contradicts the fact $\gcd(x, y, z) = 1$. Thus we obtain $z \equiv 1 \pmod 2$ which implies $y^2 \equiv -k^3 \pmod 4$. We know square of an integer modulo 4 is either 1 (mod 4) or 0 (mod 4). Hence we have $y^2 \equiv 1$ or 0 (mod 4) which gives $-k^3 \equiv 1$ or 0 (mod 4) $\Leftrightarrow k^3 \equiv 3$ or 0 (mod 4). This contradicts the condition (a) and the claim follows.

From (6) we have

$$y^2 - (-k)^3 z^6 = x^3 \Leftrightarrow (y - kz^3\sqrt{-k})(y + kz^3\sqrt{-k}) = x^3 \tag{7}$$

Next we claim that the two factors of left side of equation (7) have no common divisors. To see this, let p be a prime number which divides both the factors. Then p must be divide $-2k\sqrt{-k}z^3$. Now if p divides z^3 then from (6), p will divide y which will imply that p is a common divisor of (x, y, z) and we get a contradiction. Hence $p| - 2k$, and since $p \not| 2$, it follows that $p|k$ which implies $p|y$ and we obtain again a contradiction. Therefore the two factors of the left hand side of the equation (7) have no common divisors.

Now, we will solve the equation (7) over the imaginary quadratic field $\mathbb{Q}(\sqrt{-k})$. By the condition (b), the class number h of $\mathbb{Q}(\sqrt{-k})$ cannot be divided by 3, and we have $y + kz^3\sqrt{-k} = (A + B\sqrt{-k})^3$ with $\gcd(A, B) = 1$. Hence, we get

$$y = A^3 - 3kAB^2, \tag{8}$$

$$kz^3 = 3A^2B - kB^3. \tag{9}$$

From (9), we get $k|3A^2B$. Since $\gcd(3, k) = 1$, we get $3 \mid A^2B$. Again as k is square-free, it gives $k|AB$. If $\gcd(k, A) \neq 1$, then there exists a prime p such that $p|k$ and $p|A$. By (8), $p|y$, so $p| \gcd(k, y)$, which contradicts the assumption $\gcd(k, y) = 1$. Therefore, $k|B$. Hence, we can consider that $B = B_1 k$. Then the equation (9) can be modified to

$$z^3 = 3A^2B_1 - k^3B_1^3 = B_1(3A^2 - k^3B_1^2). \tag{10}$$

Now (10) gives us $z^3 + k^3B_1^3 \equiv 0 \pmod 3$, i.e. $(z + kB_1)(z^2 - zkB_1 + k^2B_1^2) \equiv 0 \pmod 3$. Both the factors gives $z + kB_1 \equiv 0 \pmod 3$ because

$$z^2 + k^2B_1^2 \equiv zkB_1 \pmod 3 \Leftrightarrow z^2 + 2zkB_1 + k^2B_1^2 \equiv 3zkB \pmod 3$$

$$\Leftrightarrow (z + kB_1)^2 \equiv 0 \pmod 3 \Leftrightarrow z + kB_1 \equiv 0 \pmod 3.$$

As a consequence, $z \equiv z^3 \equiv -k^3B_1^3 \equiv -kB_1 \pmod 3$, and hence $z^3 \equiv -k^3B_1^3 \pmod 9$. From (10), we obtain $3A^2B_1 \equiv 0 \pmod 9$, and thus $AB_1 \equiv 0 \pmod 3$.

Note that (8) implies $A \not\equiv 0 \pmod 3$ otherwise, $y \equiv 0 \pmod 3$, which contradicts the fact that $\gcd(y,3) = 1$. Hence, $B_1 \equiv 0 \pmod 3$. By (10), we get $27 \mid 3B_1A^2$ which implies $9|B_1$, using $\gcd(3, A) = 1$. Therefore

$$B_1 = 9B_2^3 \quad \text{which allows to write} \quad z = 3B_2z_1 \quad \text{and finally gives} \quad z_1^3 = A^2 - 27k^3B_2^6. \tag{11}$$

It is obvious that $z_1 \not\equiv 0 \pmod 3$ since $(A, B_1) = 1$. Next we prove that following claim.
Claim: z_1 is odd.
If z_1 is even, then the equality (11) and $1 = (A, B) = (A, kB_1) = (A, 9kB_2^3)$ imply that A, B, k are all odd. Thus, we obtain that y by (8) and z are even (9). Therefore, x is also even by (6). This contradicts the assumption $\gcd(x, y, z) = 1$. Hence claim follows.

Next the equation (11) can be changed as

$$(A + 3kB_2^3\sqrt{3k})(A - 3kB_2^3\sqrt{3k}) = z_1^3, \tag{12}$$

where the two factors of left side of (12) have no common factors.

In the remaining part, we merge the condition (c) with our aforementioned arguments. Let r be the 3-rank of the ideal class group of the number field $\mathbb{Q}(\sqrt{3k})$ and s the 3-rank of the ideal class group of $\mathbb{Q}(\sqrt{-k})$. We use Theorem 5 at his point and have $r \leq s \leq r+1$. By the condition (b) (equivalent to $s = 0$), we obtain $r = 0$, i.e., the class number h of the quadratic field $\mathbb{Q}(\sqrt{3k})$ is co-prime with 3. Hence, we obtain

$$A + 3kB_2^3\sqrt{3k} = \eta(C + D\sqrt{3k})^3, \tag{13}$$

where η is a unit in the real quadratic field $\mathbb{Q}(\sqrt{3k})$, and $\gcd(C, D) = 1$ since we have $(A, B_2) = 1$ (came from the fact that $\gcd(A, B_1) = \gcd(A, 3) = 1$). Let $(X, Y) = (U, T)$ be the fundamental solution of the Pell equation $Y^2 - 3kX^2 = 1$. Since $k \equiv 1 \pmod 4$, we see that $\epsilon = T + U\sqrt{3k}$ is the fundamental unit of the quadratic number field $\mathbb{Q}(\sqrt{3k})$. Therefore, we get either $\eta = \epsilon^{3n}$ or $\eta = \epsilon^{3n+1}$ or $\eta = \epsilon^{3n-1}$. For simplifying our solution, we may suppose that either $\eta = 1$ or ϵ or ϵ^{-1}.

First we suppose that $\eta = \epsilon$ or ϵ^{-1}. Then, we have

$$\eta = T \pm U\sqrt{3k}, \quad \text{and (13) gives}$$

$$A + 3kB_2^3\sqrt{3k} = (T \pm U\sqrt{3k})(C + D\sqrt{3k})^3$$
$$A + 3kB_2^3\sqrt{3k} = (T \pm U\sqrt{3k})(C^3 + 3C^2D\sqrt{3k} + 3CD^2.3k + D^3.3k\sqrt{3k}).$$

After comparing both sides, we obtain

$$A = T(C^3 + 9kCD^2) \pm 9kU(kD^3 + C^2D), \tag{14}$$

$$3kB_2^3 = T(3C^2D + 3kD^3) \pm U(C^3 + 9kCD^2). \tag{15}$$

Note that (14) implies $C \not\equiv 0 \pmod 3$ otherwise we will get $A \equiv 0 \pmod 3$, but we have proved that $\gcd(A, 3) = 1$. By (15), $C^3U \equiv 0 \pmod 3$. As $C \not\equiv 0 \pmod 3$, we get $U \equiv 0 \pmod 3$. This contradicts the condition (c) of the statement.

Now it remains to consider $\eta = 1$. Then again using (13), $A+3kB_2^3\sqrt{3k} = (C+D\sqrt{3k})^3$ holds with $(C, D) = 1$. Again we compare both sides and get

$$A = C^3 + 9kCD^2, \text{ and} \tag{16}$$

$$3kB_2^3 = 3C^2D + 3kD^3. \tag{17}$$

If $k \not| D$, then using (16), we get $k \mid C^2$ and it implies $k \mid A$. Along with the fact that $k \mid B$, we get $\gcd(A, B) \neq 1$ which is a contradiction. Hence $k \mid D$ and we can write $D = kD_1$, for some D_1. Hence, the equation (17) is changed to

$$B_2^3 = C^2 D_1 + k^3 D_1^3 = D_1(C^2 + k^3 D_1^2).$$

Using similar arguments to the previous proofs of (10) and (11), we again obtain

$$D_1 = D_2^3, B_2 = B_3 D_2, B_3^3 = C^2 + k^3 D_2^6.$$

Finally, we achieve another solution (B_3, C, D_2) of the equation (6). Now, it is a fact that (16) implies $(C, 3k) = 1$. Moreover, we conclude $D_2 \neq 0$ and $|D_2| \leq |B_2| \leq \frac{1}{3}z$. This is a contradiction to the minimality of z and completes the proof.

□

Proof of Theorem 3. Note that for a prime p with $p \equiv 1 \pmod 4 \Leftrightarrow p \equiv 1 \text{ or } 5 \pmod{12}$.

It is enough to show that $E_{k^3}(\mathbb{Q}) = E_{k^3}(\mathbb{Q})_{tors}$, because $E_{k^3}(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E_{k^3}(\mathbb{Q})_{tors}$, where r is called the rank of E_{k^3} over the set of all rational numbers. From Proposition 4, it is clear that

$$E_{k^3}(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 - k^3 \text{ with } ord_p(y) \geq 1, \text{ for some } p \mid 3k^3\}. \tag{18}$$

It is enough to show that the above set is finite. Suppose $E_{k^3}(\mathbb{Q}) \neq E_{k^3}(\mathbb{Q})_{tors}$. Then there exists an element $Q := (x, y) \in E_{k^3}(\mathbb{Q}) \setminus E_{k^3}(\mathbb{Q})_{tors}$ and a prime p such that $p \mid 3k^3$ and $ord_p(y) \geq 1$.

Next for a fixed (x, y) in $E_{k^3}(\mathbb{Q})$, we observe that if $p = 3$, then

$$ord_3(y) \geq 1 \Leftrightarrow ord_3(x) = 0, \text{ using } \gcd(3, k) = 1.$$

If $p \neq 3$, then

$$ord_p(y) \geq 1 \Leftrightarrow ord_p(x) = 1,$$

using the fact that k is square-free. Using these two facts in Lemma 1, we get the following

$$\text{If } p \neq 3, \text{ then } ord_p(y([2]Q)) \leq 0,$$
$$\text{If } p = 3, \text{ then } ord_p(y([2^2]Q)) \leq 0.$$

This acts as a base case of induction and finally, we have that

$$\text{If } p \neq 3, \text{ then } ord_p(y([2^n]Q)) \leq 0, \text{ for all } n \geq 1$$
$$\text{If } p = 3, \text{ then } ord_p(y([2^n]Q)) \leq 0 \text{ for all } n \geq 2.$$

It is enough to suppose $k = p_1 \cdots p_r$, with $p_1 \equiv 1 \pmod 4$, for all $1 \leq i \leq r$ and further suppose $n = 2^{r+2}$. Then for any $p \mid 3k^3$, we get $ord_p(y([2^n]Q)) \leq 0$. Using equation (18), we get $[2^n]P \notin E_{k^3}(\mathbb{Q})$ which contradicts the assumption that Q is not a torsion point. □

From [8], it is known that

$$\frac{\#\{-x < -k < 0 : \text{class number}(\mathbb{Q}(\sqrt{-k})) \not\equiv 0 \pmod 3\}}{\#\{-X < -k < 0\}} \geq \frac{1}{2} - \epsilon.$$

So there are infinitely many k satisfying first two conditions of Theorem 3. By [5], it is clear that if a fundamental solution of $y^2 - 3kx^2 = 1$ is (U, T) then U may or may not be divisible by 3.

We did a computational experiment on square-free positive integers $k \equiv 1, 5 \pmod{12}$. For the range of k tested, more than half also satisfied the second and third conditions of Theorem 3. It appeared as well that if k satisfied the first two conditions, then it satisfied the third condition approximately one sixth of the time. We list a few examples of values of k which satisfy the hypotheses of the Theorem 3.

Example 1: Suppose $k = 13$. Then we compute that the class number of $\mathbb{Q}(\sqrt{-13}) = 2$. A fundamental solution of the equation $Y^2 - 39X^2 = 1$ is $(4, 25)$, and the rank of the elliptic curve $y^2 = x^3 - 2197$ is 0.

Example 2: Suppose $k = 77$. Then we compute that the class number of $\mathbb{Q}(\sqrt{-77}) = 8$. A fundamental solution of the equation $Y^2 - 231X^2 = 1$ is $(5, 76)$, and the rank of the elliptic curve $y^2 = x^3 - 4913$ is 0.

Example 3: Suppose $k = 173$. Then we compute that the class number of $\mathbb{Q}(\sqrt{-173}) = 14$. A fundamental solution of the equation $Y^2 - 519X^2 = 1$ is $(651925, 14851876)$, and the rank of the elliptic curve $y^2 = x^3 - 5177717$ is 0.

4. Families with positive rank

In the previous sections we have focused on values of k for which the curve E_k has rank zero. In this section, we construct subfamilies of $\{E_k\}$ which have positive rank. This will establish something similar to Silverman's Conjecture for the quadratic twists of the Mordell curve $y^2 = x^3 - 1$. Our results were formally stated as Theorem 4 in the Introduction. Each of the two parts of the theorem will be proved here in a separate proposition.

Proposition 5. *There exist infinitely many integers k such that the curve $E_k : y^2 = x^3 - k^3$ has positive rank.*

Proof. We begin by assuming that $x = 2$ is the x-coordinate of a rational point on E_k. This means there is some rational y' such that $y'^2 = 8 - k^3$. This equation is an elliptic curve $Y^2 = -K^3 + 8$, with rank 1, being generated by the point $(K, Y) = (-1, 3)$. This means that there are infinitely many rational values of K (and hence k) such that $x = 2$ is the x-coordinate of a rational point on E_k.

If such a k is rational, say $k = r/s$ for some integers r, s with $(r, s) = 1$ and $s > 0$, then consider the isomorphism $(x, y) \to (s^2x, s^3, y)$. The resulting curve is $E_{rs} : y^2 = x^3 - (rs)^3$. For each point (x, y) on E_k, the point (s^2x, s^3y) will lie on E_{rs}. Thus we will have a rational point Q with x-coordinate $2s^2$ on E_{rs}, with rs integral.

We can prove Q has infinite order. It is straightforward to calculate the x-coordinate of $2Q$ is

$$x_{2Q} = -4s^2 \frac{r^3 + s^3}{r^3 - 8s^3}.$$

Setting $x_{2Q} = x_Q = 2s^2$ or $x_{2Q} = 0$, we find the only solutions are when $s = 0$, or when $k = r/s = -1$. Excluding these, then $2Q \neq -Q$ or 0 and so Q does not have order 2 or 3. It must therefore have infinite order by Lemma 1.

Each such curve (with $k \neq 0, 1$) will therefore have positive rank, as we have a point of infinite order. We have shown there are an infinite number of integers k such that E_k has positive rank. □

Concretely, using the construction above, we compute the first several multiples of $P = (-1, 3)$. We have

$$2P = (7/4, -13/8), \quad 3P = (-433/121, -9765/1331), \qquad \text{and}$$
$$4P = (-31073/2704, 5491823/140608).$$

The corresponding values of k are $7/4, -433/121$, and $-31073/2704$. Re-scaling using the isomorphism leads to $k = 28, -52393$, and -84021392. Each of these values of k yield curves E_k with positive rank.

Note: There are many other values t we could have chosen besides $x = 2$ in the above proof. The key criteria is that the curve $Y^2 = -K^3 + t^3$ has positive rank. For example, choosing $t = -6$ or $t = 7$ would also work. Each such t leads to infinitely many integers k as shown in the lemma.

Combining the above proposition and Theorem 2, we immediately obtain the following corollary. Note this is similar to Silverman's Conjecture (i.e. Conjecture 1), for the Mordell curve

$y^2 = x^3 - 1$, except we have shown infinitely many integers, though not necessarily prime integers. Recall we showed earlier, that assuming the Parity Conjecture, Silverman's Conjecture is true for curves E_k. Corollary 1 does not need the Parity Assumption.

Corollary 1. *There are infinitely many integers n such that E_n has positive rank. There are infinitely many integers such that E_n has rank zero.*

We are also able to construct a subfamily with higher rank. There is a well-established line of research aiming to find infinite families of curves (with various properties) that have high rank. See [9, 10] for a summary of the highest known ranks for many such families.

Proposition 6. *There is an infinite family of curves E_k over $\mathbb{Q}(m)$ with rank at least 2.*

Proof. Let a be a rational value, and set $k = a^3 - 1$. Then a simple computation checks that the point $P_1 = (ak, k^2)$ is a rational point on $E_k : y^2 = x^3 - k^3$. We consider a second point P_2 with x-coordinate $x_2 = -(a+1)k$. This will lead to a rational point if $-(a-1)(a+2)$ is a square. We can parameterize solutions to this equation by setting $a = (1-2m^2)/(m^2+1)$.

Concretely, we have

$$k = a^3 - 1 = -9m^2 \frac{(m^4 - m^2 + 1)}{(m^2+1)^3},$$

with

$$P_1 = \left(-9m^2 \frac{(1-2m^2)(m^4 - m^2 + 1)}{(m^2+1)^4}, 81m^4 \frac{(m^4 - m^2 + 1)^2}{(m^2+1)^6} \right),$$
$$P_2 = \left(-9m^2 \frac{(m^2-2)(m^4 - m^2 + 1)}{(m^2+1)^4}, 81m^3 \frac{(m^4 - m^2 + 1)^2}{(m^2+1)^6} \right).$$

Specializing the points at $m = 1$ yields $a = -7/5$ and $k = -468/125$. The points P_1 and P_2 are $P_1 = (3276/625, 219024/15625)$ and $P_2 = (-936/625, 109512/15625)$. Using SAGE, it is easily checked the determinant of their height pairing matrix is $1.796 \neq 0$, and thus they are linearly independent points of infinite order. The rank is computed to be 2. By the Silverman specialization theorem [24, Theorem 11.4], P_1 and P_2 will be independent for all but finitely many values of m, and the rank of the family of curves E_n over $\mathbb{Q}(m)$ is at least two. We note the formulas above could be simplified by using an isomorphism to re-scale and eliminate denominators. □

We did a computation to find specific curves of this rank 2 family with higher rank. The highest rank found was 4, which corresponds to the values $m = 34, 72, 5/6, 11/18, 3/26, 9/40, 17/56, 17/28$, and $46/79$.

Acknowledgement. *We would like to thank the referee for their helpful comments and suggestions. First author's research is supported by NBHM post-doctoral fellowship (54603/2021/NBHM).*

References

[1] A. Baker, Contributions to the theory of Diophantine equations, I. On the representation of integers by binary quadratic forms; II. The Diophantine equation $y^2 = x^3 + k$; *Philos. Trans. Roy. Soc. London* (Ser. A) **263** (1967 -1968) 173-191; 193-208.

[2] B. J. Birch and N. M. Stephens (1996), The parity of the rank of the Mordell-Weil group, *Topology*, **5**, 295–299.

[3] C. Breuil, B. Conrad, F. Diamond and R. Taylor, On the modularity of ellipitc curves over $\mathbb{Q}$, *J. Amer. Math. Soc.* **14** (2001), 843-939.

[4] A. Burungale and Y. Tian, The even parity Goldfeld conjecture: congruent number elliptic curves, *J. Number Theory*, **230** 161–195.

[5] J. Chahal and N. Priddis, Some congruence properties of the Pell equation. *Ann. Sci. Math. Québec*, **35** no. 2 (2011), 175–184.

[6] J. Coates, Y. Li, Y. Tian and S. Zhai, Quadratic twists of elliptic curves, *Proc. Lond. Math. Soc,* (3) **110** (2015), no. 2, 357–394.

[7] A. Dabrowskis, On the proportion of rank 0 twists of elliptic curve; *C. R. Acad. Sci. Paris, Ser.* I, **346** (2008).
[8] H. Davenport, H. Heilbronn, On the density of discriminants of cubic fields II,*Proc. Roy. Soc. Lond. A*, **322**, (1971), 405-420.
[9] A. Dujella, High rank elliptic curves with prescribed torsion, `http://web.math.hr/~duje/tors/tors.html` (accessed December 2020).
[10] A. Dujella, Infinite families of elliptic curves with high rank and prescribed torsion, `https://web.math.pmf.unizg.hr/~duje/tors/generic.html` (accessed December 2020).
[11] E. Liverance, A formula for the root number of a family of elliptic curves, *J. Number Theory*, **51** (1995), no. 2, 288–305.
[12] K. Feng and M. Xiong, On Selmer groups and Tate-Shafarevich groups for elliptic curves $y^2 = x^3 - n^3$, *Mathematica*, **58** (2012), no.2, 236-274.
[13] D. Goldfeld, Conjectures on elliptic curves over quadratic fields, in *Number Theory Carbondale 1979*, Lecture Notes in Mathematics, Vol. **751** (Springer, Berlin, 1979), pp. 108-118.
[14] J. Hofstein and W. Luo, Nonvanishing of L-series and the combinatorial sieve, *Math. Res. Lett.* **4** (1997), 435-444.
[15] H. Iwaniec and P. Sarnak, The non-vanishing of central values of automorphic L-functions and Landau–Siegel zeros, *Israel J. Math.* **120** (2000), 155-177.
[16] K. James, L-series with non-zero central critical value, *J. Amer. Math. Soc.* **11** (1998), 635-641.
[17] T. Jedrzejak, On Twists of the Fermat cubic $x^3 + y^3 = 2$, *International Journal of Number Theory*, **10**, No.1 (2014) 55-72.
[18] V. A. Kolyvagin, Finiteness of $E(\mathbb{Q})$ and Ш$(E;\mathbb{Q})$ for a subclass of Weil curves, *Izv. Acad. Nauk* USSR **52** (1988), 522-540 (in Russian).
[19] W. Kohnen, On the proportion of quadratic twists of L-functions attached to cusp forms not vanishing at the central point,*J. reine angew. Math.* **508** (1999), 179-187.
[20] L. J. Mordell, On some Diophantine equations $y^2 = x^3 + k$ with no rational solutions (II), in: *Number Theory and Analysis*, Springer, Boston, MA, 1969, pp. 224-232.
[21] K. Ono, Twists Of Elliptic Curves, *Compositio Math.* **106** (1997), no. 3, 349-360.
[22] K. Ono and C. Skinner, Non-vanishing of quadratic twists of modular L-functions, *Invent. Math.* **34** (1998), 651-660.
[23] H. R. Qin, Anomalous primes of the elliptic curve $E_D : y^2 = x^3 + D$, *Proc. London Math. Soc.* **112** (3) (2016) 415-453.
[24] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York-Berlin- Heidelberg-tokyo, 1986.
[25] A. Scholz, Uber die Beziehung der Klassenzahlen quadratischer Krper zueinander, *J. reine angew. Math.* **166** (1932), 201-203.
[26] A. Smith, 2^∞-Selmer groups, 2^∞-class groups, and Goldfeld's conjecture. arxiv.org/abs/1702.02325.
[27] Y. Tian, X. Yuan and S. Zhang, Genus periods, genus points and congruent number problem, *Asian J. Math.* **21** (2017), no. 4, 721–773.
[28] G. Yu, On the quadratic twists of a family of elliptic curves, *Mathematika* **52** (1-2) (2005), 139–154.
[29] V. Vatsal, Rank-one twists of a certain elliptic curve, *Math. Ann.* 311 (1998), 791-794.
[30] J. L. Waldspurger, Sur les coefficients de Fourier des formes modulaires de poids demi-entier, *J. Math. Pures Appl.* (9) **60** (1981), 375-484.
[31] X. Wu and Y. Qin, Rational Points of Elliptic Curve $y^2 = x^3 + k^3$, *Algebra Colloquium*, **25** : 1 (2018) 133-138.

(Abhishek Juyal) Stat-Math Unit, Indian Statistical Institute, Bangalore Centre, 8-th Mile Mysore Road, Bangalore, India, 560059.
Email address: `abhinfo1402@gmail.com`

(Dustin Moody) Computer Security Division, National Institute of Standards & Technology, Gaithersburg, Maryland, USA.
Email address: `dustin.moody@nist.gov`

(Bidisha Roy) Institute of Mathematics of the Polish Academy of Sciences, Jana i Jędrzeja Śniadeckich 8, Warsaw 00-656, Poland.
Email address: `brroy123456@gmail.com`