ELLIPTIC CURVES WITH POSITIVE RANK AND NO INTEGRAL POINTS

ELENI AGATHOCLEOUS

Abstract [1]

We study the family of elliptic curves $E_{D'} : y^2 = x^3 + 16D'$, where $D' = -3D$ and $D < -4$ is a negative squarefree integer, with $3 \nmid D$, that satisfies two simple congruence conditions. By assuming finiteness of their Tate-Shafarevich group, we show that these curves must have odd rank. We then focus on the subfamily of those elliptic curves $E_{D'}$ that correspond to the fundamental discriminants D' with the property that the rank $r_3(D)$ of the 3-part of the ideal class group of $\mathbb{Q}(\sqrt{D})$ is not equal to the rank $r_3(D')$ of the 3-part of the ideal class group of $\mathbb{Q}(\sqrt{D'})$, and therefore $r_3(D) = r_3(D') + 1$ by Scholz's Reflection Theorem. By using the connection between the points of $E_{D'}(\mathbb{Q})$ and the so-called 3-virtual units of $\mathbb{Q}(\sqrt{D'})$, we show that the elliptic curves of this subfamily, even though they have non-trivial rank, they cannot have any integral points. We also discuss the case of positive squarefree integer $D > 4$ and derive a result for this case as well.

AMS Mathematics Subject Classification: Primary: 11R29, 11G05.

Keywords: Elliptic Curves, Selmer group, Rank, Ideal Class Group, Integral Points.

Eleni Agathocleous
CISPA Helmholtz Center for Information Security
Stuhlsatzenhaus 5, Saarland Informatics Campus, 66123 Saarbrücken, Germany.
email: eleni.agathocleous@cispa.de

1. Introduction

As it is well known, if an elliptic curve has non-trivial rank, then it has infinitely many rational points. However, as it was proved by Siegel [13], an elliptic curve can have only finitely many integral points. Siegel's theorem is not effective and given an elliptic curve, it is in general hard to determine how many integral points this curve might have, or if it has any integral points at all. Other techniques that have been developed over the years, in order to study this problem, concentrate on finding bounds for the number of these integral points. Some of these bounds depend for example on the rank of the elliptic curve, the number of distinct prime divisors of the discriminant, or the primes of bad multiplicative reduction (see for example [2], [10], [14] and references therein).

In this paper we study the family of elliptic curves of j-invariant zero $E_{D'} : y^2 = x^3 + 16D'$, where $D' = -3D$ is a positive squarefree integer that satisfies two simple congruence conditions. The basic definitions and important properties of these curves are given in Section 2. In Section 3, by assuming finiteness of their Tate-Shafarevich group, we show that these curves must have odd rank. In Section 4, we focus on the subfamily of those elliptic curves $E_{D'}$ that correspond to the fundamental discriminants D' with the property that the rank $r_3(D)$ of the 3-part of the ideal class group

[1] This work has been supported by the European Union's H2020 Programme under grant agreement number ERC-669891.

of $\mathbb{Q}(\sqrt{D})$ is not equal to the rank $r_3(D')$ of the 3-part of the ideal class group of $\mathbb{Q}(\sqrt{D'})$, and therefore $r_3(D) = r_3(D') + 1$ by Scholz's Reflection Theorem. By using the connection between the points of $E_{D'}(\mathbb{Q})$ and the so-called 3-virtual units of $\mathbb{Q}(\sqrt{D'})$, we show that the elliptic curves of this subfamily, even though they have non-trivial rank, they cannot have any integral points. In the final section we discuss the case of positive fundamental discriminant D and derive a result for this case as well.

2. Definitions and Preliminaries

The notation and definitions of this section will carry throughout the paper. For the theory and proofs of the facts that we present here, the interested reader may refer for example to [12], [15, Chapter X.4 and Appendix B], [17] and [5, Chapter IV].

For any number field $M/\mathbb{Q}$, denote by $E(M)$ the group of points of the elliptic curve E defined over M. Let $\overline{M}$ denote the algebraic closure of M. We denote by $D < -4$ every squarefree integer which satisfies the following two congruence relations

$$D \equiv 1 \bmod 4 \text{ and } D \equiv 2 \bmod 3. \tag{1}$$

We denote be D' the, also squarefree, integer $D' = -3D$ and by K_D the imaginary quadratic field $K_D = \mathbb{Q}(\sqrt{D})$ with $K_{D'} = \mathbb{Q}(\sqrt{D'})$ its so-called quadratic resolvent.

Let us note here that, given the congruence conditions in (1), the following congruences always hold:

$$D \equiv 5 \bmod 12 \text{ and } D' \equiv 9 \bmod 12.$$

We define the j-invariant zero elliptic curves

$$E_{D'} : y^2 = x^3 + 16D'. \tag{2}$$

The torsion group

$$\mathcal{T}_{D'} = \{O, (0, \pm 4\sqrt{D'})\} \subseteq E_{D'}(\overline{\mathbb{Q}})$$

is a subgroup of $E_{D'}(\overline{\mathbb{Q}})$ of order 3 and is invariant under the action of $G_{\mathbb{Q}} = Gal(\overline{\mathbb{Q}}/\mathbb{Q})$. The quotient of $E_{D'}$ over $\mathcal{T}_{D'}$ defines a family of isogenous elliptic curves, which are defined as

$$\hat{E}_D : Y^2 = X^3 + 16 \cdot 3^4 D. \tag{3}$$

As expected, the torsion group for these curves is

$$\hat{\mathcal{T}}_D = \{O, (0, \pm 36\sqrt{D})\} \subseteq \hat{E}_D(\overline{\mathbb{Q}}).$$

Let ϕ denote the rational 3-isogeny

$$\phi : E_{D'} \to \hat{E}_D$$

with kernel $\ker_\phi(\overline{\mathbb{Q}}) = \mathcal{T}_{D'}$. The isogeny ϕ is given by the map ([7, Proposition 8.4.3])

$$(X, Y) = \phi((x, y)) = \Big(\frac{x^3 + 4^3 3^4 D}{x^2}, \frac{y(x^3 - 2 \cdot 4^3 3^4 D)}{x^3}\Big). \tag{4}$$

The dual isogeny $\hat{\phi}$ is such that $\phi \circ \hat{\phi} = \times 3$, where $\times 3$ is the multiplication-by-3 map. The map defined by the dual isogeny $\hat{\phi}$ is given in the proof of Lemma 4.5.

Consider now the exact sequence ([15, Section X.4, Remark 4.7])

$$0 \to \hat{E}_D(\mathbb{Q})[\hat{\phi}]/\phi(E_{D'}(\mathbb{Q})[3]) \to \hat{E}_D(\mathbb{Q})/\phi(E_{D'}(\mathbb{Q})) \xrightarrow{\hat{\phi}} \tag{5}$$

$$\xrightarrow{\hat{\phi}} E_{D'}(\mathbb{Q})/3E_{D'}(\mathbb{Q}) \to E_{D'}(\mathbb{Q})/\hat{\phi}(\hat{E}_D(\mathbb{Q})) \to 0.$$

Since both $\ker_{\phi}(\overline{\mathbb{Q}}) = \mathcal{T}_{D'}$ and $\ker_{\hat{\phi}}(\overline{\mathbb{Q}}) = \hat{\mathcal{T}}_D$ contain no non-trivial rational point of order 3, the first quotient group of (5) vanishes and the rank $r(E_{D'})$ of $E_{D'}(\mathbb{Q})$ equals

$$r(E_{D'}) = \dim_{\mathbb{F}_3}(E_{D'}(\mathbb{Q})/3E_{D'}(\mathbb{Q})). \tag{6}$$

Consider the short exact sequence

$$0 \to \mathcal{T}_{D'} \to E_{D'}(\overline{\mathbb{Q}}) \xrightarrow{\phi} \hat{E}_D(\overline{\mathbb{Q}}) \to 0. \tag{7}$$

From this, we obtain the long exact cohomology sequence which gives in particular the following

$$0 \to \hat{E}_D(\mathbb{Q})/\phi(E_{D'}(\mathbb{Q})) \xrightarrow{\delta} H^1(G_{\mathbb{Q}}, \mathcal{T}_{D'}) \to H^1(G_{\mathbb{Q}}, E_{D'}(\overline{\mathbb{Q}}))[\phi] \to 0. \tag{8}$$

By localising at each prime p, we obtain the following commutative diagram, where res_p is the usual restriction map:

$$\begin{tikzcd}
0 \arrow[r] & \hat{E}_D(\mathbb{Q})/\phi(E_{D'}(\mathbb{Q})) \arrow[r] \arrow[d] & H^1(G_{\mathbb{Q}}, \mathcal{T}_{D'}) \arrow[r] \arrow[d, "res_p"] & H^1(G_{\mathbb{Q}}, E_{D'}(\overline{\mathbb{Q}}))[\phi] \arrow[r] \arrow[d, "res_p"] & 0 \\
0 \arrow[r] & \hat{E}_D(\mathbb{Q}_p)/\phi(E_{D'}(\mathbb{Q}_p)) \arrow[r] & H^1(G_{\mathbb{Q}_p}, \mathcal{T}_{D'}) \arrow[r] & H^1(G_{\mathbb{Q}_p}, E_{D'}(\overline{\mathbb{Q}}_p))[\phi] \arrow[r] & 0
\end{tikzcd}$$

Definition 2.1. *The Selmer group of $E_{D'}$ relative to the isogeny ϕ is*

$$\mathcal{S}_{\phi}(E_{D'}) = \{x \in H^1(G_{\mathbb{Q}}, \mathcal{T}_{D'}) \mid res_p(x) \in \mathrm{Im}(\hat{E}_D(\mathbb{Q}_p)/\phi(E_{D'}(\mathbb{Q}_p))) \textit{ for all } p\}.$$

The Tate-Shafarevich group of $E_{D'}$ can now be defined as

$$Ш(E_{D'}) = \{x \in H^1(G_{\mathbb{Q}}, E_{D'}(\overline{\mathbb{Q}})) \mid res_p(x) = 0 \textit{ for all } p\}.$$

These two groups are connected together as follows:

$$0 \to \hat{E}_D(\mathbb{Q})/\phi(E_{D'}(\mathbb{Q})) \to \mathcal{S}_{\phi}(E_{D'}) \to Ш(E_{D'})[\phi] \to 0. \tag{9}$$

Remark 2.2. *By considering the dual isogeny $\hat{\phi}$ instead, we get exact sequences analogous to (7), (8) and (9) which in turn give us the analogous definitions for $\mathcal{S}_{\hat{\phi}}(\hat{E}_D)$, $Ш(\hat{E}_D)$ and $Ш(E_D)[\hat{\phi}]$.*

Remark 2.3. *We also obtain exact sequences analogous to (7), (8) and (9) for $\times 3 = \phi \circ \hat{\phi}$ which in turn give us the analogous definitions for $\mathcal{S}_3(E_{D'})$, $Ш(E_{D'})$ and $Ш(E_{D'})[3]$, and similarly for $\hat{E}_D$.*

With D satisfying the conditions in (1), let $r(\mathcal{S}_\phi(E_{D'}))$ and $r(\mathcal{S}_{\hat{\phi}}(\hat{E}_D))$ denote the rank, as $\mathbb{F}_3$-vector spaces, of the Selmer groups $\mathcal{S}_\phi(E_{D'})$ and $\mathcal{S}_{\hat{\phi}}(\hat{E}_D)$, relative to the isogenies ϕ and $\hat{\phi}$, of the curves $E_{D'}$ and $\hat{E}_D$ respectively, over $\mathbb{Q}$. Denote by $r_3(D)$ and $r_3(D')$ the rank of the 3-part of the ideal class group $\mathcal{CL}(K_D)$ and $\mathcal{CL}(K_{D'})$ of K_D and $K_{D'}$ respectively. In the next section we will compute the precise rank for the Selmer groups $\mathcal{S}_\phi(E_{D'})$ and $\mathcal{S}_{\hat{\phi}}(\hat{E}_D)$ and obtain a parity result regarding the rank of the curves $E_{D'}$.

3. On the 3-Selmer group and rank of the elliptic curves $E_{D'}$

By employing the results of Satgé [12, Section 3], we compute below the precise rank for the Selmer groups $\mathcal{S}_\phi$ and $\mathcal{S}_{\hat{\phi}}$:

Proposition 3.1. *With D satisfying the congruence conditions in (1), the rank of the Selmer groups $\mathcal{S}_\phi(E_{D'})$ and $\mathcal{S}_{\hat{\phi}}(\hat{E}_D)$ of the curves $E_{D'}$ and $\hat{E}_D$ are as follows:*

$$r(\mathcal{S}_\phi(E_{D'})) = r_3(D')$$

$$r(\mathcal{S}_{\hat{\phi}}(\hat{E}_D)) = r_3(D') + 1.$$

Proof. Our elliptic curves $E_{D'}$ have a constant term equal to $16D' > 0$. With D' squarefree and with $2^4 || 16D'$, Lemma 3.1 in [12] is vacuously true. Now $3 || 16D'$ and, given the congruence condition $D \equiv 2 \bmod 3$, we have that $-16D \equiv 1 \bmod 3$. Therefore, from Proposition 3.2(1) of [12] we have that $r(\mathcal{S}_\phi(E_{D'})) = r_3(D')$. Finally, since $16D' > 0$, Proposition 3.3.(1) of [12] gives $r(\mathcal{S}_{\hat{\phi}}(\hat{E}_D)) = r_3(D') + 1$. □

As in Remark 2.3, we denote by $\mathcal{S}_3(\hat{E}_D)$ and $\mathcal{S}_3(E_{D'})$ the 3-Selmer group of the corresponding elliptic curves. Its rank will be denoted by $r(\mathcal{S}_3(E_{D'}))$ and similarly for $\hat{E}_D$. We now consider the exact sequence ([11, Corollary 1])

$$0 \to \frac{\hat{E}_D(\mathbb{Q})[\hat{\phi}]}{\phi(E_{D'}(\mathbb{Q})[3])} \to \mathcal{S}_\phi(E_{D'}) \to \mathcal{S}_3(E_{D'}) \to \mathcal{S}_{\hat{\phi}}(\hat{E}_D) \to \frac{\text{Ш}(\hat{E}_D)[\hat{\phi}]}{\phi(\text{Ш}(E_{D'})[3])} \to 0. \tag{10}$$

Since our curves have no rational 3-torsion points, the first term of (10) is trivial. As it is known, because of the non-degenerate alternating pairing on $\frac{\text{Ш}(\hat{E}_D)[\hat{\phi}]}{\phi(\text{Ш}(E_{D'})[3])}$ (defined by Cassels in [4]), this last term is an even-dimensional $\mathbb{F}_3$-vector space (assuming finiteness of the Tate-Shafarevich group). Therefore, we obtain the following result regarding the parity of the rank of the 3-Selmer group and the ranks of the two Selmer groups $\mathcal{S}_\phi(E_{D'})$ and $\mathcal{S}_{\hat{\phi}}(\hat{E}_D)$:

$$r(\mathcal{S}_3(E_{D'})) \equiv r(\mathcal{S}_\phi(E_{D'})) + r(\mathcal{S}_{\hat{\phi}}(\hat{E}_D)) \bmod 2. \tag{11}$$

Corollary 3.2. *The elliptic curves $E_{D'}$ have odd rank.*

Proof. Given Remark 2.3, the exact sequence analogous to (9) is

$$0 \to \hat{E}_D(\mathbb{Q})/3(E_{D'}(\mathbb{Q})) \to \mathcal{S}_3(E_{D'}(\mathbb{Q})) \to \text{Ш}(E_{D'}(\mathbb{Q}))[3] \to 0. \tag{12}$$

Again, by assuming finiteness of the Tate-Shafarevich group, the non-degenerate alternating pairing on $\text{Ш}(E_{D'})[3]$ implies that this group is of even dimension as an $\mathbb{F}_3$-vector space and we obtain the congruence relation

$$r(E_{D'}) \equiv r(\mathcal{S}_3(E_{D'})) \equiv r(\mathcal{S}_\phi(E_{D'})) + r(\mathcal{S}_{\hat{\phi}}(\hat{E}_D)) \equiv 1 \bmod 2. \tag{13}$$

The last two equivalences follow from (11) and Proposition 3.1. □

4. The Escalatory Case and No Integral Points

In the previous section we established that the elliptic curves $E_{D'}$ have odd rank. In this section, we will define a subfamily of these curves and show that this subfamily cannot have integral points.

Let us first recall a classical result of Scholz regarding the rank of the 3-part of the ideal class group of quadratic number fields. The interested reader may refer to [18, Section 10.2] for more details on Scholz's Theorem.

Theorem 4.1. ***Reflection Theorem of Scholz***
Let $d > 1$ be square-free. Let $F = \mathbb{Q}(\sqrt{d})$ and $K = \mathbb{Q}(\sqrt{-3d})$. If $3|d$ then let $K = \mathbb{Q}(\sqrt{-d/3})$. Then $r_F \le r_K \le r_F + 1$. □

Definition 4.2. *With notation as in Theorem 4.1, we define as* escalatory *the case where $r_K = r_F + 1$ and as* non-escalatory *the case where $r_K = r_F$.*

The terms *escalatory* and *non-escalatory* are used for example in [9, Chapter 4]. Specifically, in Section 4.10 of [9], it is shown that in the case of negative fundamental discriminant d, the escalatory case is equivalent to the non-existence of cubic fields of discriminant $3^4 d$. Translating this to our notation, we have

Remark 4.3. *If $r_3(D) = r_3(D') + 1$ then there are no cubic fields of discriminant $3^4 D$.*

We will not explain in this paper the proof of this result. We only need to mention that the proof requires the use of the so-called 3-*virtual units*, which we also use here and we define right before Proposition 4.8. These 3-virtual units live in the quadratic resolvent $K_{D'}$ and give rise to cubic extensions of K_D. The interested reader will find all the necessary theory in [9, Chapter 4] and [6, Section 5.2.2], and may find more on the relation between 3-virtual units, ideal class groups and elliptic curves in [1].

Before we go on to prove that the subfamily of elliptic curves $E_{D'}$ with $r_3(D) = r_3(D') + 1$ have no integral points, let us show the relation between the non-escalatory case $r_3(D) = r_3(D')$ and the existence of a cubic field of discriminant $3^4 D$, via elliptic curves, with the following example. Let us note that the discriminant $D = -1355$ of the example does not belong to the set of discriminants that we consider in this paper, since $-1355 \equiv 1 \bmod 3$. This is not important though since it does not affect the purpose of the example.

Example 4.4. *Consider the negative fundamental discriminant $D = -1355$. We have $r_3(D) = r_3(D') = 1$ and so we are in the non-escalatory case. To show the existence of a cubic field of discriminant equal to $3^4 D$, which is* *expected according to [9, Section 4.10], we can look for an irreducible polynomial of discriminant 3^4D or equivalently for rational solutions u, v such that*

$$\mathrm{disc}(x^3 - ux + v) = 4u^3 - 27v^2 = 3^4D \iff (4v)^2 = (\frac{4}{3}u)^3 - 3 \cdot 16D.$$

Therefore, we looked for rational points on the elliptic curve

$$E_{D'} : y^2 = x^3 + 16D'.$$

The integral point $P = (64, 572)$ gives $u = 48$ and $v = 143$ and indeed the cubic polynomial $g(x) = x^3 - 48x + 143$ is irreducible in $\mathbb{Q}[x]$ and has discriminant equal to 3^4D.

Lemma 4.5. *Let $D < -4$ be any squarefree integer which satisfies the congruence relations in (1). Let $E_{D'}$ be the elliptic curves that we have defined above. If there is an* integral *point $P \in E_{D'}(\mathbb{Z})$, then this point cannot be the image of any point $Q = (\hat{x}, \hat{y}) \in \hat{E}_D(\mathbb{Q})$.*

Proof. We can write Q as

$$Q = (\hat{x}, \hat{y}) = (\frac{X}{Z^2}, \frac{Y}{Z^3}) = (\frac{x}{3^{(2c-a)}z^2}, \frac{y}{3^{(3c-b)}z^3}),$$

where $a, b, c \geq 0$, $3^a||X$, $3^b||Y$, $3^c||Z$, and the symbol '$||$' means *divides exactly.* Since $Q \in \hat{E}_D(\mathbb{Q})$ we must have

$$3^{(2b-3a)}y^2 = x^3 + 3^{(6c-3a+4)}16Dz^6.$$

We immediately see that we cannot have $6c - 3a + 4 = 0$ because, if either a or b is not zero then $3|4$ which is absurd, and if $a = c = 0$ then $4 = 0$, also absurd.

Case (a): Let us call Case (a) the case where $a = b = c = 0$.

If at least one of the a, b or c is not zero, we need to examine the following cases:

Case (b): If $6c - 3a + 4 = 2b - 3a$ (which implies that $2b - 3a \neq 0$), then $b = 3c + 2$ and therefore $\hat{y} = \frac{3^2y}{z^3}$. Plugging it into the equation of $\hat{E}_D$ this implies that $\hat{x} = \frac{3^2x}{z^2}$. In this case we must also have that $a = 2c + 2$.

Case (c): If $6c - 3a + 4 \neq 2b - 3a$ and $2b - 3a \neq 0$, then we arrive at a contradiction since we always have that 3 must divide one of the terms y, x or $16 \cdot Dz^6$, hence this case cannot happen.

Case (d): If $2b - 3a = 0$ (and therefore $6c - 3a + 4 \neq 2b - 3a$) then $b = 3a/2$ and a must be even.

Assume now that $P = \hat{\phi}(Q)$, where $\hat{\phi}$ is defined as ([7, Proposition 8.4.3]):

$$(A, B) = \hat{\phi}(\hat{x}, \hat{y}) = \Big(\frac{\hat{x}^3 + 4^3 3^4 D}{9\hat{x}^2}, \frac{\hat{y}(\hat{x}^3 - 2 \cdot 4^3 3^4 D)}{27\hat{x}^3}\Big). \tag{14}$$

Substituting Q in (14), the y-coordinate in particular gives the relation

$$3^{(3+3c-b)}Bx^3z^3 + 3^{(4+6c-3a)}2^7yz^6D = yx^3. \tag{15}$$

In Case (a), $a = b = c = 0$ and equation (15) implies that $3|yx^3$, impossible. Hence, if Case (a) holds, then P cannot be the image of any point $Q \in \hat{E}_D(\mathbb{Q})$.

In Case (b), where $b = 3c + 2$ and $a = 2c + 2$, equation (15) implies that $3|2^7yz^6D$ which is impossible. Hence, if Case (b) holds, then P cannot be the image of any point $Q \in \hat{E}_D(\mathbb{Q})$.

In Case (c) we have nothing to show since this case cannot happen.

In Case (d), $b = 3a/2$ and a must be even. We rewrite equation (15) as

$$3^{2+(3c-b+1)}(Bx^3z^3 + 3^{(3c-b+1)}2^7z^6yD) = yx^3. \tag{16}$$

Denote by ε the common exponent $\varepsilon = 3c - b + 1$.

If $\varepsilon \geq 0$, equation (16) implies that $3|yx^3$, a contradiction.

If $\varepsilon = -1$ then $b = 3c + 2$ and we are in Case a.

If $\varepsilon \leq -2$, equation (16) implies that $3|2^7z^6yD$, a contradiction.

Hence, if Case (d) holds, then P cannot be the image of any point $Q \in \hat{E}_D(\mathbb{Q})$.

Having exhausted all possible cases, we see that P cannot be the image of any point $Q \in \hat{E}_D(\mathbb{Q})$ and the lemma is proved. □

Before we move on to Proposition 4.8, we need the following two definitions.

Definition 4.6. *Given an order $\mathcal{O}$, we say that a proper $\mathcal{O}$-ideal $\mathfrak{a}$ is primitive if it is not of the form $k\mathfrak{a}$ for $1 < k \in \mathbb{Z}$ and $\mathfrak{a}$ a proper ideal ([8, §11.D, pg.214]). We will call an element π primitive if (π) is a primitive ideal.*

The second definition is a very brief definition of what we call a 3-virtual unit. The reader may find more on 3-virtual units in [1], and on l-virtual units in general in [6, Section 5.2.2].

Definition 4.7. *An element $\alpha \in K_{D'}^{\times}$ is a 3-virtual unit of $K_{D'}$ if there exists an ideal $\mathfrak{a}$ in the maximal order $\mathcal{O}_{D'}$ of $K_{D'}$ such that $\alpha\mathcal{O}_{D'} = \mathfrak{a}^3$.*

Proposition 4.8. *As before, D is a negative fundamental discriminant satisfying the congruence relations in (1). The subfamily of elliptic curves $E_{D'}$ for which $r_3(D) = r_3(D') + 1$ holds, have odd rank and no integral points.*

Proof. The fact that the whole family of elliptic curves $E_{D'}$ has odd rank was proved in Corollary 3.2. Assume now that we are in the escalatory case and assume by way of contradiction that an elliptic curve $E_{D'}$ in this subfamily has an *integral* point $P = (A, B) \in E_{D'}(\mathbb{Z})$. Plugging the point back in $E_{D'}$ and modifying the coefficients a little we obtain

$$3^4D = 4(\frac{3A}{4})^3 - 27(\frac{B}{4})^2.$$

Case (a): From the equation of $E_{D'}$, we see that if either A or B is even then so must be the other one, since $B^2 = A^3 - 3 \cdot 16D$. From the same equation we see that B must actually be divisible by 4 exactly, since $2 \nmid D$. Let $A = 2a$ and $B = 4b$. Cancelling out the 16 we end up with $2a^3 = b^2 + 3D$. Since $D \equiv 1 \bmod 4$ and b is odd, we have a contradiction unless $2|a$. Therefore, if both A and B are even then we must have that $4||B$ and $4|A$. This implies that the monic polynomial

$$g(x) = x^3 - \frac{3A}{4}x + \frac{B}{4} = x^3 - 3ax + b$$

is in $\mathbb{Z}[x]$ and is of discriminant exactly 3^4D.

Consider the element $\lambda = \frac{\frac{B}{4}+\sqrt{D'}}{2} = \frac{b+\sqrt{D'}}{2} \in \mathcal{O}_{D'}$. We see that

$$\lambda\bar{\lambda} = (\frac{A}{4})^3 = a^3$$

and

$$\lambda + \bar{\lambda} = \frac{B}{4} = b.$$

Given the polynomial $g(x) \in \mathbb{Z}(x)$ above, [9, Proposition 4.1(1)] implies that λ is a 3-virtual unit.

Denote by Λ the element of $K_{D'}^{\times}$:

$$\Lambda = 2^3\lambda = \frac{2B+8\sqrt{D'}}{2} = B + 4\sqrt{D'} \in K_{D'}^{\times}.$$

We recognise that Λ is the image of the point $P = (A, B)$ under the Fundamental 3-Descent Map Ψ, as this map is described for example in [7, §8.4.4] or [1]. Since by [7, Proposition 8.4.8]

$$\Psi(E_{D'}(\mathbb{Q}))/\hat{\phi}(\hat{E}_D(\mathbb{Q})) \cong\subseteq K_{D'}^{\times}/(K_{D'}^{\times})^3,$$

then indeed, by Lemma 4.5, $\Psi(P) = \Lambda \equiv \lambda \in K_{D'}^{\times}/(K_{D'}^{\times})^3$. Then, by [9, Proposition 4.1 (2)], $g(x)$ is irreducible over $\mathbb{Q}$. Finally, we see that λ is a primitive 3-virtual unit and therefore, by [9, Theorem 4.4], $g(x)$ generates a cubic field of discriminant 3^4D, which leads to a contradiction since we are in the escalatory case.

Case (b): Both A and B are odd. Then $g(x) \notin \mathbb{Z}[x]$ but the following polynomial $f(x)$ does have integer coefficients and it is of discriminant 8^23^4D:

$$f(x) = x^3 - 3Ax + 2B \in \mathbb{Z}[x].$$

As above, let

$$\Lambda = 2^3\lambda = \frac{2B+8\sqrt{D'}}{2} = B + 4\sqrt{D'} \in K_{D'}^{\times}/(K_{D'}^{\times})^3.$$

We see that $\Lambda\bar{\Lambda} = A^3$ and $\Lambda + \bar{\Lambda} = 2B$ and therefore, by [9, Proposition 4.1, (1) and (2)], Λ is a 3-virtual unit and $f(x)$ is irreducible in $\mathbb{Q}[x]$. Furthermore, since B is odd, Λ is a primitive 3-virtual unit and again, by [9, Theorem 4.4], $f(x)$ generates a cubic field of discriminant 3^4D, which leads to a contradiction since we are in the escalatory case. □

Let us remark here that if 3 divides either A or B, then $9|16D'$ which is impossible. Hence, in both Cases (a) and (b) of Propositon 4.8 above, the irreducible polynomials $g(x)$ and $f(x)$, both in $\mathbb{Z}[x]$, are in *standard* form, as this is defined in [9, Section 4.4].

5. The case of positive squarefree D and Final Remarks

A natural question to ask is what happens when we consider discriminants $D > 4$ where the same equivalence relations (1) hold. In this case, the constant term $16D' = -16 \cdot 3D$ of our elliptic curves $E_{D'}$ would be negative. By following the same steps of the proof of Proposition 3.1 and by employing the same result of Satgé for this case of negative constant term, we obtain

$$r(\mathcal{S}_{\phi}(E_{D'})) = r_3(D') = r(\mathcal{S}_{\hat{\phi}}(\hat{E}_D)).$$

Hence, from the same discussion that follows Proposition 3.1, including the proof of Corollary 3.2, we obtain the following parity relation between the rank of our curves with positive squarefree D and their Selmer group

$$r(E_{D'}) \equiv 2r_3(D') \equiv 0 \bmod 2.$$

So the rank of our elliptic curves must be even in this case and might even be zero. The equivalent of Remark 4.3 for $D > 4$ is that there are no cubic fields of discriminant $3^4 D$ when we are in the non-escalator case, i.e. when $r_3(D) = r_3(D')$. Since Lemma 4.5 and Proposition 4.8 hold for this case as well, we see that the subfamily of curves $E_{D'}$ with $D > 4$ and $r_3(D) = r_3(D')$ has no integral points.

A final question, which constitutes the topic of an upcoming paper of ours, concerns the study of the the group $Ш(E_{D'})[\phi]$, for both $D < -4$ and $D > 4$. By studying the exact sequence in (9) and by following a constructive approach via binary quadratic forms, similar to that in [1], we show how to construct curves that violate the local-global principle in the case that $Ш(E_{D'})[\phi]$ is not empty.

References

[1] E. Agathocleous: On the Selmer group and rank of a family of elliptic curves and curves of genus one violating the Hasse principle, (Under Review) (2022).

[2] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, Y. Zhao: (2017) Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves, https://doi.org/10.48550/arXiv.1701.02458.

[3] W. Bosma, J. Cannon and C. Playoust: The Magma algebra system. I. The user language, *J. Symbolic Comput.*, **24** (1997), 235–265.

[4] J. W. S. Cassels, Arithmetic on curves of genus 1, IV, Proof of the Hauptvermutung, *J. Reine Angew. Math.* **211**, (1962), 95-112.

[5] J.W.S. Cassels and A. Fröhlich: Algebraic Number Theory Proceedings of an Instructional Conference Organized by the London Mathematical Society (a NATO Advanced Study Institute) with the Support of the International Mathematical Union, London Mathematical Society, 2010.

[6] H. Cohen: *Advanced Topics in Computational Number Theory*, Springer-Verlag New York, 2000.

[7] H. Cohen: *Number Theory Volume I: Tools and Diophantine Equations*, Springer-Verlag, 2007.

[8] D.A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, Class Field Theory and Complex Multiplication*, Wiley, 1989.

[9] S. Hambleton and H. Williams: *Cubic Fields with Geometry*, Springer Nature Switzerland Ag, 2018.

[10] H. A. Helfgott, A. Venkatesh: Integral Points on Elliptic Curves and 3-torsion in Class Groups, *Journal of the American Mathematical Society* **19(3)**, (2006), 527-550.

[11] R. Kloosterman and E. Schaefer, Selmer groups of elliptic curves that can be arbitrarily large, *J. Number Theory* **99(1)** (2003), 148-163.

[12] Ph. Satgé, Groupes de Selmer et corps cubiques, *J.NumberTheory*, **23** (1986), 294–317.

[13] C. L. Siegel, Über einige Anwendungen diophantischer Approximationen, *Abh. Preuss. Akad. Wiss.* (1929), 1-41.

[14] J. H. Silverman: A quantitative version of Siegel's theorem: integral points on elliptic curves and Catalan curves, *Journal für die reine und angewandte Mathematik*, **378** (1987), 60-100.

[15] J. Silverman: *The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics (2nd Edition)*, Springer-Verlag, New York, 2009.

[16] W. A. Stein et al.: Sage Mathematics Software (Version x.y.z), The Sage Development Team, YYYY, http://www.sagemath.org.

[17] J. Top, *Descent by 3-isogeny and the 3-rank of quadratic fields*, Advances in Number Theory: The Proceedings of the Third Conference of the Canadian Number Theory Association (1993), 303–317.

[18] L.C. Washington, *Introduction to Cyclotomic Fields; second edition*, Springer-Verlag, Berlin Heidelberg New York, 1997.