



ANNALES DE L'INSTITUT FOURIER

Julie DESJARDINS & Bartosz NASKRĘCKI

Geometry of the del Pezzo surface $y^2 = x^3 + Am^6 + Bn^6$

Article à paraître, mis en ligne le 17 mai 2024, 44 p.

Article mis à disposition par ses auteurs selon les termes de la licence
CREATIVE COMMONS ATTRIBUTION – PAS DE MODIFICATION 3.0 FRANCE



<http://creativecommons.org/licenses/by-nd/3.0/fr/>



Les *Annales de l'Institut Fourier* sont membres du
Centre Mersenne pour l'édition scientifique ouverte

www.centre-mersenne.org

e-ISSN : 1777-5310

GEOMETRY OF THE DEL PEZZO SURFACE

$$y^2 = x^3 + Am^6 + Bn^6$$

by Julie DESJARDINS & Bartosz NASKRĘCKI (*)

ABSTRACT. — In this paper, we give an effective and efficient algorithm which on input takes non-zero integers A and B and on output produces the generators of the Mordell–Weil group of the elliptic curve over $\mathbb{Q}(t)$ given by an equation of the form $y^2 = x^3 + At^6 + B$. Our method uses the correspondence between the 240 lines of a del Pezzo surface of degree 1 and the sections of minimal canonical height on the corresponding elliptic surface over $\overline{\mathbb{Q}}$.

For most rational elliptic surfaces, the density of the rational points is proven by various authors, but the results are partial in case when the surface has a minimal model that is a del Pezzo surface of degree 1. In particular, the ones given by the Weierstrass equation $y^2 = x^3 + At^6 + B$, are among the few for which the question is unsolved, because the root number of the fibres can be constant. Our result proves the density of the rational points in many of these cases where it was previously unknown.

RÉSUMÉ. — Dans cet article, nous donnons un algorithme efficace et efficient qui en entrée prend des entiers non nuls A et B et en sortie produit les générateurs du groupe Mordell–Weil de la courbe elliptique sur $\mathbb{Q}(t)$ donnée par une équation de la forme $y^2 = x^3 + At^6 + B$. Notre méthode utilise la correspondance entre les 240 courbes exceptionnelles d’une surface del Pezzo de degré 1 et les sections de hauteur de Shioda minimale sur la surface elliptique correspondante sur $\overline{\mathbb{Q}}$. Pour la plupart des surfaces elliptiques rationnelles, la densité des points rationnels est démontrée par diverses personnes, mais les résultats sont partiels dans le cas où la surface a un modèle minimal qui est une surface del Pezzo de degré 1. En particulier, les surfaces données par l’équation de Weierstrass $y^2 = x^3 + A^6 + B$, sont parmi les rares pour lesquelles la question n’est pas résolue, parce que le signe de l’équation fonctionnelle des fibres peut être constant. Notre résultat prouve la densité des points rationnels dans beaucoup de ces cas où elle était auparavant inconnue.

Keywords: del Pezzo surfaces; density of rational points; elliptic surfaces; Mordell–Weil groups.

2020 *Mathematics Subject Classification:* 14G05, 14J26, 14J27, 14D10, 11G05.

(*) Bartosz Naskręcki acknowledges the support by Dioscuri program initiated by the Max Planck Society, jointly managed with the National Science Centre (Poland), and mutually funded by the Polish Ministry of Science and Higher Education and the German Federal Ministry of Education and Research. Julie Desjardins is partially supported by an NSERC discovery grant.

1. Introduction

Del Pezzo surfaces and rational elliptic surfaces

A del Pezzo surface over a field k is a smooth, projective, geometrically integral surface X over k with an ample anticanonical divisor $-K_X$. Del Pezzo surfaces are classified by their degree $d := K_X^2$, an integer $1 \leq d \leq 9$. It has been proven that if X is not geometrically \bar{k} -isomorphic to $\mathbb{P}^1 \times \mathbb{P}^1$, then X is \bar{k} -isomorphic to the blowup of \mathbb{P}^2 in $9 - d$ points in “general position”, cf. [9, Chapter 8.1].

An elliptic surface over k with base \mathbb{P}^1 is a smooth projective surface \mathcal{E} together with a map $\pi : \mathcal{E} \rightarrow \mathbb{P}^1$ such that the general fibre of π is a smooth connected curve E of genus one. We assume that π has a section: \mathcal{E} is thus a family of elliptic curves away from finitely many fibres, and admits a Weierstrass equation as an elliptic curve over $k(t)$. We say that \mathcal{E} is rational if it is birational to \mathbb{P}^2 .

A rational elliptic surface is \bar{k} -isomorphic to \mathbb{P}^2 blown-up in the fundamental locus of a pencil of plane cubics: thus by choosing carefully d points on a del Pezzo surface, one obtains a rational elliptic surface \mathcal{E} .

In particular if $d = 1$, then the blowup of the base point of the anticanonical linear system of X allows to obtain a rational elliptic surface \mathcal{E} . In terms of equation: X is isomorphic to a smooth sextic hypersurface in the weighted projective space $\mathbb{P}^1(1, 1, 2, 3)$ defined by the equation

$$y^2 = x^3 + F(m, n)x + G(m, n),$$

with F, G homogeneous polynomials of degree respectively 4 and 6 ([13, Theorem III.3.5]). The converse is also true. The base point of the anticanonical system is $P := [0, 0, 1, 1]$: and the blow-up of X at P gives the surface \mathcal{E} in \mathbb{P}^3 with equation $y^2 = x^3 + f(t)x + g(t)$ where $f(t) = F(t, 1)$ and $g(t) = G(t, 1)$. Then \mathcal{E} is a rational elliptic surface [17].

A rational elliptic surface obtained through this process has only irreducible fibres (of Kodaira type I_1 or II). Moreover, it reaches the maximum of 8 independent rational sections over \bar{k} of the Mordell–Weil lattice and the torsion subgroup of the generic fibre is trivial, cf. [18].

In this paper, we are interested in certain rational elliptic surfaces \mathcal{E}_G with a generic fibre of the form

$$E_G : y^2 = x^3 + G(t),$$

where $G(t) \in \mathbb{Z}[t]$ is such that $1 \leq \deg G(t) \leq 6$. These elliptic surfaces have many particularities:

- (1) if $G(t)$ is a squarefree polynomial of degree ≥ 5 , then the contraction of the image of the zero section gives a del Pezzo surface of degree 1, cf. [9, Section 8.8.3];
- (2) $\mathcal{E} = \mathcal{E}_G$ is isotrivial, i.e. its fibres \mathcal{E}_t are isomorphic to one another. Indeed, the j -invariant function $t \rightarrow j(\mathcal{E}_t)$ equals 0.

Main theorem

THEOREM 1.1. — *Let $A, B \in \mathbb{Z}$ be non-zero rational integers and define $\mathcal{E} = \mathcal{E}_{A,B}$ to be the elliptic surface given by the equation*

$$(1.1) \quad E_{A,B} : y^2 = x^3 + At^6 + B.$$

The rank of the generic fibre $E_{A,B}$ over $\overline{\mathbb{Q}}(t)$ is 8 and the rank $r_{\mathcal{E}}$ of the group $E_{A,B}(\mathbb{Q}(t))$ is at most equal to 3. There exists an effective and efficient algorithm which on input takes two non-zero integers A and B and produces on output the generators of the group $E_{A,B}(\mathbb{Q}(t))$.

Remark 1.2. — The algorithm of Theorem 1.1 is effective and efficient in the following sense. For two integers A, B on the input, in order to compute the rank of the group $E_{A,B}(\mathbb{Q}(t))$, the algorithm only requires the answer to the following questions

- (1) Is A (resp. B) a square or -3 times a square?
- (2) Is A (resp. B , resp. $4AB$) a cube?

For each task in the list there is an algorithm which given the input integer N returns the answer in $O(\log(N)^{1+o(1)})$ steps, [1].

We denote by $r_{\mathcal{E}}$ the rank of the group $E_{A,B}(\mathbb{Q}(t))$ and call it the *generic rank* of \mathcal{E} over \mathbb{Q} .

For instance, in order for the group $E_{A,B}(\mathbb{Q}(t))$ to have the maximum possible rank ($r_{\mathcal{E}} = 3$), the coefficients A and B need both to be either a square or -3 times a square, $4AB$ needs to be a cube and either A or B needs to be a cube as well. That follows directly from the algorithm presented in Figure 1.1. A detailed proof of the algorithm and the further steps which resolve questions about the generic rank $r \leq 2$ are described in Section 4.

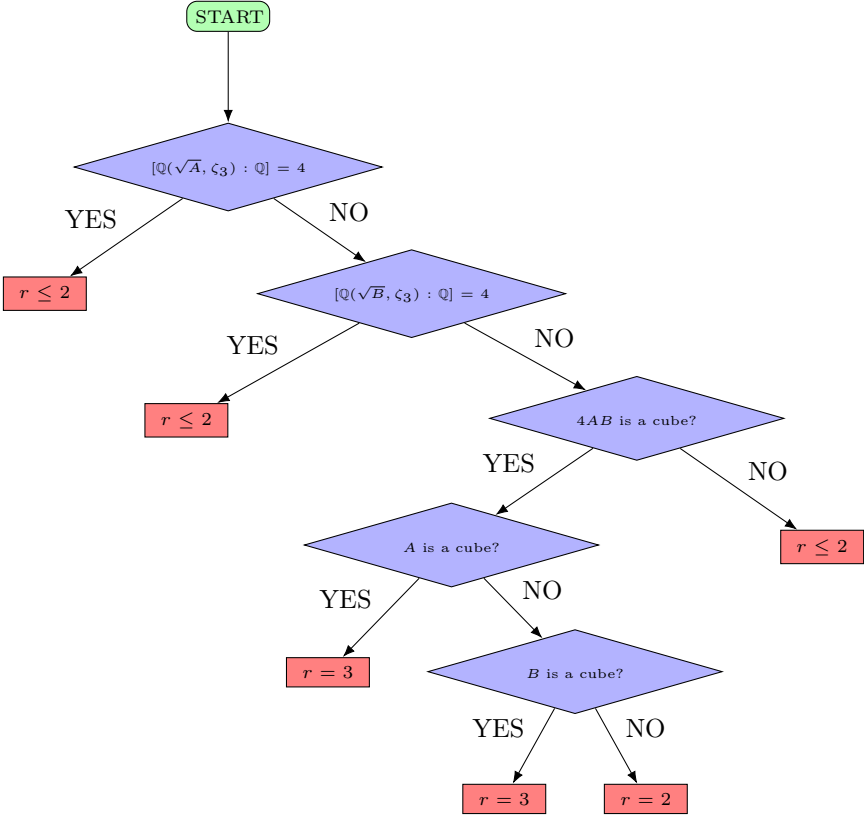


Figure 1.1. Simplified version of the rank decision algorithm. Each diamond box is a query with possible yes or no answer. Red boxes explain what is the value of the generic rank $r = r_{\mathcal{E}}$ after each step.

THEOREM 1.3. — Let \mathcal{E} be the elliptic surface given by the equation $y^2 = x^3 + At^6 + B$. Then \mathcal{E} has generic rank $r_{\mathcal{E}} = 3$ if there exists some $\alpha, \beta \in \mathbb{Z}$ such that one of the following holds:

- $A = \alpha^6$ and $B = 2^4\beta^6$;
- $A = -3^3\alpha^6$ and $B = 2^4\beta^6$;
- $A = -3^3\alpha^6$ and $B = -3^32^4\beta^6$;
- $A = \alpha^6$ and $B = -2^43^3\beta^6$;
- or one of the four previous cases, with roles of A and B interchanged.

Otherwise, \mathcal{E} has rank $r_{\mathcal{E}} \leq 2$.

Remark 1.4. — Theorem 1.1 implies on an elliptic surface with generic rank 0 that any minimal model of \mathcal{E} is a del Pezzo surface of degree 1. This is due to the fact that Galois invariant part of the Picard group of \mathcal{E} has rank 2 (spanned by the image of the general fibre and the image of the zero section). The surface obtained by contraction of the zero section, has the Picard group over \mathbb{Q} of rank 1 and is minimal. This theory can be found in [16].

Remark 1.5. — In our main theorem, we choose $G(t) = C(AG_1(t)^2 + BG_2(t)^2)$ with $G_1(t) = t^3$ and $G_2(t) = 1$. An important remark to make is that our result will still hold for any $G_1(t) = L_1(t)^3$, $G_2(t) = L_2(t)^3$ for $L_1, L_2 \in \mathbb{Z}[t]$ non proportional linear polynomials. The basis will be given by similar points, with a change of variable, cf. Corollary 1.6. However, given general polynomials $G_1(t), G_2(t) \in \mathbb{Z}[t]$, the situation differs. The Galois action on the Mordell–Weil lattice is maximal for a generic choice of G_1 and G_2 . Points of the Néron–Tate height 2 form a big orbit of size 240 in that case. We recall in Section 3.1 how to compute these heights à la Shioda. For particular choices of G_1 and G_2 , it is possible to split this orbit further, for instance into three Galois orbits of size respectively 6, 72 and 162 for most values of A, B . These orbits can be decomposed even further by choosing appropriate values of A and B until finding a rational section.

A fractional linear change of coordinates $\phi : t \mapsto (at + b)/(ct + d)$ for $ad - bc \neq 0$ on the base \mathbb{P}^1 produces from the elliptic surface $\pi : \mathcal{E}_G \rightarrow \mathbb{P}^1$ a new elliptic surface $\pi' : \mathcal{E} \rightarrow \mathbb{P}^1$ where $\pi' = \phi \circ \pi$. The map ϕ is an automorphism of \mathbb{P}^1 which induces the automorphism of elliptic surface \mathcal{E}_G and \mathcal{E} . The effect of this change of coordinates on the generic fibre is visible by replacing the polynomial $G(t)$ with the polynomial $H(t) = (ct + d)^6 G\left(\frac{at+b}{ct+d}\right)$. Both elliptic surfaces have the same arithmetic properties which is visible in the following corollary.

COROLLARY 1.6. — *Let $a, b, c, d \in \mathbb{Z}$ such that $ad - bc \neq 0$ and let $A, B \in \mathbb{Z} \setminus \{0\}$. Define \mathcal{E} to be the elliptic surface given by the equation*

$$E : y^2 = x^3 + A(at + b)^6 + B(ct + d)^6.$$

The rank of the generic fibre E over $\overline{\mathbb{Q}}(t)$ is 8 and the rank of the group $E(\mathbb{Q}(t))$ is at most equal to 3. The algorithm described in section 4.2 gives the rank of the group $E(\mathbb{Q}(t))$.

Motivation and method

The motivation for Theorem 1.1 is Corollary 2.6 that lists the elliptic surfaces \mathcal{E}_{3a^2, b^2} ($a, b \in \mathbb{Z} \setminus \{0\}$) and their generic rank. As explained in Section 2, on those rational elliptic surfaces the Zariski density of the rational points (and \mathbb{Q} -unirationality) is uncertain: there exists no geometric proof, and the study of the variation of the root number on the fibres is indecisive: it always takes the value $+1$, so according to the parity conjecture (weak BSD) the rank is even - but possibly zero on all the fibres.

Our method uses the correspondence between the 240 lines of a del Pezzo surface of degree 1 and the sections of minimal canonical height ($= 2$) on the corresponding elliptic surface over $\overline{\mathbb{Q}}$. After finding a basis of the Mordell–Weil lattice over $\overline{\mathbb{Q}}$ we study the Galois action on those lines and the submodules their orbits generate in order to determine a basis (and so the rank) of the Mordell–Weil lattice over the rationals.

Contents of the paper

First, in Section 2, we discuss some previous approaches towards proving the density of points on del Pezzo surfaces. Next, we study when the root number of the family \mathcal{E}_G is positive. In those cases we can apply the algorithm from further sections to find instances when the Mordell–Weil rank over $\mathbb{Q}(t)$ is positive, hence obtaining a density of rational points on the surface \mathcal{E}_G . We discuss in Section 2.3 for which polynomials G we obtain a new density result.

In Section 3 we compute the structure of the group $\Lambda = E_G(\overline{\mathbb{Q}}(t))$ for $G = At^6 + B$, $A, B \in \mathbb{Q}^\times$. We obtain it by studying the explicit set of points in Λ which have height 2. From the setup, there are 240 such points and under the natural action of the absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ they decompose into at least 8 orbits which we explicitly classify.

In Section 4, based on the results of the previous section, we determine the structure of Λ as the natural Galois module with respect to the group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Since the group Λ has no non-zero torsion elements it forms with a height pairing a positive definite lattice. We find a sublattice Λ' of index 81 in Λ which allows us to compute the subgroup $\Lambda_{\mathbb{Q}}$ of points defined over $\mathbb{Q}(t)$ for any choice of $A, B \in \mathbb{Z} \setminus \{0\}$. The rank of $\Lambda_{\mathbb{Q}}$ varies between 0 and 3 and for each choice of A and B we provide a complete answer, packaged in a decision diagram in Section 4.2. Next, we compute in Section 4.3 the minimal height generators for the group $\Lambda_{\mathbb{Q}}$.

Finally, in Section 5 we briefly discuss what are the possible extensions of our work to the cases when the rank of $\Lambda_{\mathbb{Q}}$ is 0.

In each section of the paper we verify certain statements with MAGMA computer algebra system. The source code of our programs is available online on the website of one of the authors, [6]

Acknowledgments

We thank Marc Hindry for his suggestion of the proof of Proposition 2.3 and for his valuable comments on the preliminary version of this paper. We thank the anonymous referee for valuable suggestions which improved the quality of the paper. We also thank Dino Festi, Ronald van Luijk and Rosa Winter for their helpful comments and suggestions which improved the exposition of this paper. We are grateful to the Hausdorff Center Mathematics in Bonn for the excellent working conditions in April 2018 and to the organizers of the workshop “Arithmetic of Hyperelliptic Curves” in September 2017 during which we have initiated our project. The second author is grateful to the University of Bristol for providing us with the access to Magma cluster CREAM.

2. Previous and new approaches to density of points

2.1. Geometric methods

Let \mathcal{E} be a rational elliptic surface defined over \mathbb{Q} . A famous theorem of Iskovskikh [11] then says that \mathcal{E} has a minimal model over \mathbb{Q} , denoted X , that is either a conic bundle of degree ≥ 1 , or a Del Pezzo surface.

We say that a surface S is k -unirational if there is a dominant rational map $\mathbb{P}^2 \dashrightarrow S$. Be aware that for k an algebraically closed field, being k -unirational is equivalent to being rational. However, it is not clear that it is the case for other fields. Moreover, k -unirationality is *a priori* a stronger property, implying the density of the rational points.

THEOREM 2.1 ([14, 16, 20]). — *Let \mathcal{E} be a rational elliptic surface over a field k whose generic rank is non-zero, then the surface is k -unirational.*

Proof. — Kollár and Mella [14] proves k -unirationality when X is a conic bundle⁽¹⁾ when $\text{char } k \neq 2$, by Segre and Manin [16] when X is a del Pezzo surface of degree $d \geq 3$ with at least one rational point, by Salgado, Testa and Várilly-Alvarado [20], based on a work of Manin [16, Theorem 29.4], when X is a del Pezzo surface of degree 2 provided that it contains a rational point that neither lies on four exceptional curves nor the ramification quartic curve. Thus in that case, k -unirationality holds on both surfaces.

In the case of a del Pezzo surface of degree 2 that is obtained by contracting an exceptional curve of a del Pezzo surface of degree 1 to a point p , [20, Corollary 14] guarantees that p is rational and does not lie in an exceptional curve or the ramification curve. \square

COROLLARY 2.2. — *For the surfaces in our paper, this means Theorem 1.1 proves \mathbb{Q} -unirationality on $\mathcal{E}_{A,B}$ provided that the rank is ≥ 1 .*

If the minimal model X is a del Pezzo surface of degree 1, the surface X has automatically a rational point: the base point of the anticanonical system. However, the results concerning density of rational points are still partial.

In papers of Ulas [24, 25] and Jabara [12], the density of rational points on certain families of isotrivial rational elliptic surfaces with j -invariant 0 and 1728 is proved by constructing a multisection with infinitely many rational points on those families. An article of Salgado and van Luijk [19] improves this construction, and proves the Zariski density of the set of rational points of a del Pezzo surface of degree 1 satisfying certain conditions. However, those conditions were hard to check and moreover, the multisection they constructed sometimes failed to have infinitely many rational points - and so it did not prove the Zariski density.

Recently, Bulthuis and van Luijk [3] proved that given a point on a del Pezzo surface of degree 1 which is of finite order in the fibre, there exists an pencil of elliptic curves through this point: each of the elliptic curves of the fibration is a multisection of the surface. In order to prove the density of points one has to prove that one of these elliptic curves has positive Mordell–Weil rank over \mathbb{Q} . However, this last step is not always an easy task.

In an article by Winter and the first author [7], one proves the density of the rational points on elliptic surfaces of the form (1.1) via the construction of an “elliptic multisection” passing through a non-torsion point, cf. Section 5.

⁽¹⁾ In this case, the surface is \mathbb{Q} -unirational, i.e. it is dominated by the projective plane $\mathbb{P}^2 \dashrightarrow X$

2.2. Root number method

To prove that the set of rational points $\mathcal{E}(\mathbb{Q})$ of an elliptic surface \mathcal{E} is Zariski dense, it suffices to show that for infinitely many $t \in \mathbb{P}^1(\mathbb{Q})$ the fibre \mathcal{E}_t is an elliptic curve with positive Mordell–Weil rank, cf. [19, Lemma 7.4]. For this reason, it is useful to study the *root number*, denoted by $W(E) \in \{\pm 1\}$. The root number $W(E)$ is conjecturally equal to the parity $(-1)^{rk(E)}$ of the Mordell–Weil rank⁽²⁾. Under this Parity Conjecture, it is thus sufficient to find infinitely many fibres with negative root number in order to prove the Zariski density.

Building on ideas of [10, 15] and [27], the first author [5] confirms (conditionally⁽³⁾) that non-isotrivial elliptic surfaces have a dense set of rational point through the study of the variation of the root number. For isotrivial elliptic surfaces, it can happen that a family has a constant root number, but [4] proves (unconditionally) that they have a dense set of rational points given that the surface has j -invariant $j \neq 0$. If $W(E_t) = +1$ for all $t \in \mathbb{P}^1(\mathbb{Q})$ and that the j -invariant is 0, then it is not yet known whether the rational points are Zariski dense.

A rational elliptic surface with $j = 0$ has a Weierstrass equation $y^2 = x^3 + G(t)$ for some $G \in \mathbb{Q}[t]$ with $\deg G \leq 6$; the difficult case correspond to a Del Pezzo surface of degree 1, i.e. when $\deg G = 5$ or 6. For these Várilly-Alvarado [27, Theorem 2.1] proved that the root number varies, provided that G has a irreducible factor G_i such that $\sqrt{-3} \notin \mathbb{Q}[t]/(G_i)$. It is therefore natural to look at polynomials not satisfying this condition.

The following proposition holds true: clearly, many of the elliptic surfaces covered in Theorem 1.1 fall in this pattern.

PROPOSITION 2.3. — *A square free polynomial $G(t) = c \prod_i f_i$, $f_i \in \mathbb{Z}[t]$ irreducible, satisfies the condition*

$$\mu_3 \subset \mathbb{Q}[t]/f_i(t) \quad \text{for all } i,$$

(where μ_3 is the group of third roots of unity) if and only if there exist non-zero polynomials $G_1, G_2 \in \mathbb{Z}[t]$ and a constant $C \in \mathbb{Z}$ such that:

$$G(t) = C(3G_1(t)^2 + G_2(t)^2).$$

⁽²⁾ The parity conjecture $W(E) = (-1)^{rk E(\mathbb{Q})}$ is equivalent to the congruence modulo 2 of the algebraic rank with the analytic rank (the order of annulation of the L -function at $s = 1$), thus it is a weakening of the Birch and Swinnerton–Dyer conjecture which predicts the equality of the two ranks, cf. [8].

⁽³⁾ This result depends on the parity conjecture and two more analytic number theory conjectures

Proof. — Suppose there exist two polynomials $G_1, G_2 \in \mathbb{Z}[t]$ and a constant $C \in \mathbb{Z}$ such that $G(t) = C(3G_1(t)^2 + G_2(t)^2)$. Let $\alpha \in \overline{\mathbb{Q}}$ denote a root of a factor $f = f_i$. Then $G_1(\alpha) \neq 0$, otherwise it would follow that $f|G_2$ and $f^2|G$, contradicting the assumption on G . Hence $-3 = \left(\frac{G_2(\alpha)}{G_1(\alpha)}\right)^2$ and $\mu_3 \subset \mathbb{Q}(\alpha)$.

Let $G(t) = c \prod_i f_i$, where f_i are irreducible polynomials such that the fields $K_i = \mathbb{Q}[t]/f_i$ contain μ_3 . In particular, fields K_i have even degree $2d$ over \mathbb{Q} and $\sqrt{-3} \in K_i$. We fix one index i for now. Let $f = f_i$ and $K = K_i$. We denote by α a certain root α_i of f_i .

LEMMA 2.4. — *There exist two polynomials P and Q with integer coefficients such that $\deg P \leq d$ and $\deg Q \leq d - 1$ and*

$$(2.1) \quad \sqrt{-3} = \frac{P(\alpha)}{Q(\alpha)}.$$

Proof of Lemma 2.4. — Suppose we have an element $\delta = \sum_{k=0}^{2d-1} c_k \alpha^k$ in a number field $K = \mathbb{Q}(\alpha)$ of even degree $2d$. Let $\beta = \sum_{k=0}^{d-1} b_k \alpha^k$. Then

$$\delta\beta = \sum_{k=0}^{2d-1} \ell_k(b_0, \dots, b_{d-1}) \alpha^k$$

where the expressions ℓ_k are linear forms in b_0, \dots, b_{d-1} with coefficients in \mathbb{Z} which depend on $\{c_k\}$. The linear system

$$\ell_k(b_0, \dots, b_{d-1}) = 0, \quad d+1 \leq k \leq 2d-1$$

has d variables and $d-1$ equations, so has a nontrivial solution, which provides the coefficients $a_k = \ell_k(b_0, \dots, b_{d-1})$. \square

It follows from Lemma 2.4 that $P(\alpha)^2 + 3Q(\alpha)^2 = 0$ and thus f divides the polynomial $P^2 + 3Q^2$, so in fact they are proportional due to degree conditions. Hence, for each i we have $f_i = c_i(P_i^2 + 3Q_i^2)$ and that concludes the theorem. \square

Remark 2.5. — The polynomials such that $\delta = P(\alpha)/Q(\alpha)$ with $\deg P \leq d$, $\deg Q \leq d-1$ are not unique but the fraction P/Q is. Indeed, if $P(\alpha)/Q(\alpha) = \delta = R(\alpha)/S(\alpha)$, then $(PS - RQ)(\alpha) = 0$ and since the degree of $PS - RQ$ is smaller than $\deg f$, it follows that $PS - RQ = 0$, hence $P/Q = R/S \in \mathbb{Q}(t)$.

Family $\mathcal{E}_{A,B}$ coincides with \mathcal{E}_G up to linear change of variables if and only if G_1 and G_2 are coprime polynomials with $\max(\deg(G_1), \deg(G_2)) = 3$ and G_1, G_2 are constant times a cube and $A = 3c \cdot a^2$ and $B = c \cdot b^2$ ($a, b, c \in \mathbb{Z}$ constants such that a and b are coprime). In that case the family forms a

set of sextic twists for which it is not guaranteed that the root number of a fibre \mathcal{E}_t varies when t varies through $t \in \mathbb{P}(\mathbb{Q})$. In a previous paper [4, Theorem 6.1], the first author gives the precise conditions on a, b and c for which the root number takes the same values on every fibre.

We apply the algorithm from Theorem 1.1 to the elliptic surface with equation $\mathcal{E} : y^2 = x^3 + 3ca^2t^6 + cb^2$, where $a, b, c \in \mathbb{Z} \setminus \{0\}$ and $\gcd(a, b) = 1$. According to our decision algorithm:

- the generic rank $r_{\mathcal{E}}$ is 2 if c or $-3c$ (resp. $3c$ or $-c$) is a square and $4AB$ and A (resp. $4AB$ and B) are cubes;
- the rank $r_{\mathcal{E}}$ is 1 if c or $-3c$ (resp. $3c$ or $-c$) is a square and either $4AB$ or A (resp. $4AB$ or B) are cubes;
- the rank $r_{\mathcal{E}}$ is 0 otherwise.

This leads to the following result:

COROLLARY 2.6. — *Let \mathcal{E} be the elliptic surface given by the equation $y^2 = x^3 + At^6 + B$ where $A = 3ca^2$ and $B = cb^2$ for some $a, b, c \in \mathbb{Z} \setminus \{0\}$ with $\gcd(a, b) = 1$. Then \mathcal{E} has generic rank $r_{\mathcal{E}} = 2$ if there exist some $\alpha, \beta \in \mathbb{Z}$ satisfying one of the following:*

- $A = 3^3\alpha^6$ and $B = 2^4\beta^6$ (or A and B switched);
- $A = -\alpha^6$ and $B = -2^43^3\beta^6$ (or A and B switched);

Suppose that it is not the case. Then \mathcal{E} has generic rank $r_{\mathcal{E}} = 1$ if there exist some non-zero $p, q \in \mathbb{Z}$ coprime and not divisible by 2 and 3, such that A and B , written up to sixth power representative and possibly switched in the equation ⁽⁴⁾, are among

- $A = 3^3, B = p^2$;
- $A = -1, B = -3p^2$
- A and B have the same sign and appear in Table 2.1

In all the other cases of A and B , the generic rank is $r_{\mathcal{E}} = 0$.

Proof. — The proof is based on the decision algorithm and is purely combinatorial.

Suppose either that c or $-3c$ is a square, say $c = \gamma^2$. Then $A = 3(\gamma a)^2$ and $B = (\gamma b)^2$. If $c = -3\gamma^2$, then $A = -(3\gamma a)^2$ and $B = -3(\gamma b)^2$. In both cases, we take the path *YES, NO* in Figure 4.1, the initial point of the procedure. This leads us to continue the decision algorithm on Figure 4.2.

Suppose that $c = \gamma^2$. If $4AB$ is a cube, then $4AB = 2^23\gamma^4a^2b^2 = \delta^3$. In that case, we take the branch *YES*, and so :

⁽⁴⁾ Switched means that we look at $y^2 = x^3 + Bt^6 + A$.

Table 2.1. Possibilities for $|A|$ and $|B|$ written up to sixth power representatives. We assume p, q are cube-free, coprime and coprime to 6.

$ A $	$ B $
$3p^2q^4$	$2^43^2p^4q^2$
$3^3p^2q^4$	$2^4p^4q^2$
$3^5p^2q^4$	$2^43^4p^4q^2$
$2^23p^2q^4$	$2^23^2p^4q^2$
$2^23^3p^2q^4$	$2^2p^4q^2$
$2^23^5p^2q^4$	$2^23^4p^4q^2$
$2^43p^2q^4$	$3^2p^4q^2$
$2^43^3p^2q^4$	p^4q^2
$2^43^5p^2q^4$	$3^4p^4q^2$

- If A is a cube, we take the branch *YES* and thus $r_{\mathcal{E}} = 2$. Then we obtain that $A = 3^3\alpha^6$ and $B = 2^4\beta^6$. Those computations are very explicit and we emphasise that we do them separately for valuations at primes 2, 3 and $p \geq 5$.
- If A is not a cube, we take the branch *NO* and thus $r_{\mathcal{E}} = 1$. Then A can take any value among $2^{2e}3^{2f+1}p^2q^4\alpha^6$ with $e, f \in \{0, 1, 2\}$ as soon as it is not $e = 0, f = 1$ and $p = q$ - in which case it is a cube. These values are listed in Table 2.1. (We have $B = 2^{4-2e}3^{2(1+2f)}p^4q^2\beta^6$.)

Now, if $4AB$ is not a cube, we follow the path *NO* in the first step of Figure 4.2.

- If A is a cube, we take the branch *YES* and thus $r_{\mathcal{E}} = 1$. This happens if $A = 3^3\alpha^6$. The possibilities for B will be among those such that $B = 2^{2e}3^{2f}p^2\beta^6$ for all choices of $e, f \in \{0, 1, 2\}$ and $p \in \mathbb{Z}$ except the case $e = 0, f = 1$ and $p = \alpha^3$ - because in that case $4AB$ is a cube and hence we are not anymore on the right branch of the diagram: we rather have $r_{\mathcal{E}} = 2$.
- If A is not a cube, we take the branch *NO* and thus $r_{\mathcal{E}} = 0$.

We find the possibility for A and B when $c = -3\gamma^2$ in a very similar way, using the same path in the routine.

The cases for $-c$ square or $3c$ square can be obtained in a similar way - this time we take the path *NO, YES* in Figure 4.1 and we run through the different path of Figure 4.3. \square

2.3. New examples proved with the Main theorem

THEOREM 2.7. — *Every elliptic surface given by an equation of the form $\mathcal{E} : y^2 = x^3 + c(3a^2t^6 + b^2)$ with generic rank 2 has constant root number on their fibres: $W(\mathcal{E}_t) = +1$ for all $t \in \mathbb{Q}$.*

The complete list of elliptic surfaces with a generic fibre of the form $y^2 = x^3 + At^6 + B$ with constant root number on its fibres and generic rank 1 is given by Table 2.2. The table also states when $W(\mathcal{E}_t) = -1$ for all $t \in \mathbb{Q}$ and when $W(\mathcal{E}_t) = +1$ for all $t \in \mathbb{Q}$.

Table 2.2. List of elliptic surfaces of the form $y^2 = x^3 + At^6 + B$ with constant root number and of generic rank 1. A and B written up to sixth power representatives (and up to switching their role in the equation), and $\gcd(p, q) = 1$. Integer σ denotes the cardinality of the set {prime factors p_i of pq : $v_{p_i}(p^2q^4) \equiv 2, 4 \pmod 6, p_i \equiv 2 \pmod 3$ }.

A	B	Additional condition	Root number of the fibres
$3^3p^2q^4$	$2^4p^4q^2$	$p^2q^4 \equiv 4 \pmod 9$	$(-1)^{\sigma+1}$
		$p^4q^2 \equiv 1 \pmod 9$	$(-1)^\sigma$
3^3	$2^43^2p^2$	$p^2 \equiv 7 \pmod 9$	$+1$
$-2^43^3p^2q^4$	$-p^4q^2$	$p^2q^4 \equiv 1 \pmod 9$	$(-1)^{\sigma+1}$
		$p^4q^2 \equiv 4 \pmod 9$	$(-1)^\sigma$
$-2^43^3p^2$	-1	$p^2 \equiv 1 \pmod 9$	$+1$
$-2^43^5p^2$	-1	any p, q	$+1$

Remark 2.8. — For those of the surfaces listed above with $W(\mathcal{E}_t) = +1$ for all $t \in \mathbb{Q}$, Corollary 2.6 the first unconditional proof of the Zariski density of the rational points.

Remark 2.9. — Unfortunately, there are many surfaces for which neither our result nor the root number method is decisive. These cases are those with simultaneously

- (1) all root numbers are equal to $+1$ and
- (2) $rk_{\mathcal{E}_{A,B}}(\mathbb{Q}(t)) = 0$.

We refer to Section 5 for a longer discussion on these cases. Moreover, we prove the density on some examples with constant root number with different techniques: [27, Example 5.1] (also covered by our Theorem 1.1) and by first author and R. Winter [7].

Proof of Theorem 2.7. — This is a consequence of Corollary 2.6 combined with [4, Theorem 6.1.].

Let \mathcal{E} be an elliptic surface given by the equation $y^2 = x^3 + c(3a^2t^6 + b^2)$. Write $t = \frac{m}{n}$, where $m, n \in \mathbb{Z} \times \mathbb{Z}_{>0}$ are coprime integers. Then the root number of a fibre is obtained from the formula ([27, Proposition 4.8]):

$$(2.2) \quad W(\mathcal{E}_t) = -R(t) \prod_{\substack{p^2 | F(m,n) \\ p \geq 5}} \begin{cases} 1 & \text{if } v_p(F(m,n)) \equiv 0, 1, 3, 5 \pmod{6} \\ \left(\frac{-3}{p}\right) & \text{if } v_p(F(m,n)) \equiv 2, 4 \pmod{6} \end{cases}$$

where

$$R(t) = W_2(\mathcal{E}_t) \left(\frac{-1}{F(m,n)_{(2)}} \right) W_3(\mathcal{E}_t) (-1)^{v_3(F(m,n))},$$

where $F(m,n) = c(3a^2m^6 + b^2n^6)$. For a positive integer α , we denote by $\alpha_{(p)}$ the integer such that $\alpha = p^{v_p(\alpha)} \alpha_{(p)}$. The product over $p^2 | F(m,n)$ equals $(-1)^\sigma$, where $\sigma = \#\{p \mid c : p \equiv 2 \pmod{3}\}$ since our choice of $F(m,n)$ has the property that whenever $p \mid F(m,n)$ and $p \nmid c$ for a $p \geq 5$, we have

$$F(m,n) = c(3a^2m^6 + b^2n^6) \equiv 0 \pmod{p}$$

and thus

$$\left(\frac{bn^3}{am^3} \right)^2 \equiv -3 \pmod{p},$$

forcing $\left(\frac{-3}{p}\right) = +1$. Let us denote the function $\omega_2(t) = W_2(\mathcal{E}_t) \left(\frac{-1}{F(m,n)_{(2)}}\right)$ and $\omega_3(t) = W_3(\mathcal{E}_t) (-1)^{v_3(F(m,n))}$. Observe that we have:

$$W(\mathcal{E}_t) = (-1)^{\sigma+1} \omega_2(t) \omega_3(t).$$

The values of A and B for which the functions $\omega_2(t)$ and $\omega_3(t)$ are constant are listed in [4, Lemma A.1, Lemma A.2]. In the first case, this depends on the quantities $v_2(a), v_2(b), v_2(c)$ and $c_{(2)} \pmod{4}$. In the second case, this depends on the quantities $v_3(a), v_3(b), v_3(c) \pmod{6}$ and $c_{(3)}, a_{(3)}^2, b_{(3)}^2 \pmod{9}$. Let us illustrate the computation that needs to be done with a specific example (doing all cases exhaustively would be too long, and not necessary).

Let $\alpha, \beta \in \mathbb{Z}$, we study the surface given by the equation $y^2 = x^3 + 3^3\alpha^6t^6 + 2^4\beta^6$.

We have $v_2(a) = 0, v_2(b) = 2$ and $v_2(c) = 0$. Moreover $c_{(2)} \equiv 1 \pmod{4}$. It follows that $\omega_2(t) = +1$ for all $t \in \mathbb{Q}$ according to [4, Table 3]. We have $v_3(a) = 1, v_3(b) = 0$ and $v_3(c) = 0$. Moreover $c_{(3)} a_{(3)}^2 \equiv 1 \pmod{9}$. Thus,

$\omega_3(t) = -1$ for all $t \in \mathbb{Q}$ according to [4, Table 2]. Hence, for any $t \in \mathbb{Q}$ such that \mathcal{E}_t is non-singular, the root number of this fibre is

$$W(\mathcal{E}_t) = -(-1)(+1) = +1. \quad \square$$

3. The structure of the orbits

3.1. A basis of the Mordell–Weil group: the eight generators

Let k be a field of characteristic different from 2 and 3 and let $A, B \in k$ be two non-zero elements of k . Let $E_{A,B} : y^2z = x^3 + (At^6 + B)z^3$ denote an elliptic curve over a field of rational functions $k(t)$.

Let $\mathcal{E}_{A,B}$ denote an elliptic surface attached to $E_{A,B}$. It is a smooth projective surface with a morphism $\pi : \mathcal{E}_{A,B} \rightarrow \mathbb{P}^1$ which is the natural projection $(x, y, z, t) \mapsto t$. We denote by \mathcal{O} the zero section $\mathcal{O} : \mathbb{P}^1 \rightarrow \mathcal{E}_{A,B}$ obtained by extending the zero point on $E_{A,B}$.

To each point $P \in E_{A,B}(\bar{k}(t))$ we associate a section $\sigma_P : \mathbb{P}^1 \rightarrow \mathcal{E}_{A,B}$ and denote by \bar{P} the (-1) -curve which is the image of σ_P . We denote by $\bar{P}.\bar{Q}$ the intersection number of \bar{P} against \bar{Q} on $\mathcal{E}_{A,B}$. The intersection $\bar{P}.\bar{Q}$ (for $P \neq Q$) is computed as a sum of local intersection numbers ([22, III Section 7, Section 9])

$$\bar{P}.\bar{Q} = \sum_{t \in \mathbb{P}^1} (P, Q)_t.$$

In fact, the translation by point map on the generic fibre $E_{A,B}$ extends to an automorphism of $\mathcal{E}_{A,B}$, [22, III Proposition 9.1], hence $\bar{P}.\bar{Q} = \overline{P-Q}.\bar{\mathcal{O}}$.

The intersection number $\bar{P}.\bar{\mathcal{O}}$ is computed by the formula

$$\bar{P}.\bar{\mathcal{O}} = \deg(q(t)) + \delta$$

where $x(P) = \frac{p(t)}{q(t)^2}$ is the x -coordinate of P given in terms of two coprime polynomials p, q . A non-negative integer δ is computed in the integral model of $E_{A,B}$ at ∞ where $t = 1/s$ and the local model is $y^2 = x^3 + A + Bs^6$. Number δ satisfies the condition $\frac{p(1/s)}{q(1/s)^2} s^2 = \frac{\tilde{p}(s)}{\tilde{q}(s)^2 s^{2\delta}}$ where \tilde{p} and \tilde{q} are coprime to s and $\delta = \max\{0, \deg p/2 - \deg q - 1\}$.

Group $E_{A,B}(\bar{k}(t))$ is equipped with the height pairing ([22, III Section 4, Section 9]) defined for two given points P, Q by the formula [21]

$$\langle P, Q \rangle = 1 + \bar{P}.\bar{\mathcal{O}} + \bar{Q}.\bar{\mathcal{O}} - \bar{P}.\bar{Q}.$$

We denote by $\langle P, P \rangle$ the height of the point P and have the simplified formula $\langle P, P \rangle = 2 + 2\bar{P}.\bar{\mathcal{O}} \geq 0$. In particular, it implies that we have no

non-trivial torsion points and $\langle P, P \rangle = 2$ if and only if $\bar{P} \cdot \bar{O} = 0$. The latter condition means that the x -coordinate of P is a polynomial in t of degree at most 2. Group $E_{A,B}(\bar{k}(t))$ with the pairing $\langle \cdot, \cdot \rangle$ forms a positive definite lattice. This is a special case of the general theory of the Mordell–Weil lattices, cf. [21].

We use throughout the rest of the paper the symbols of standard lattices A_n , D_n and E_n which correspond to Dynkin diagrams with the same notation, cf. [2, Chapter 6].

PROPOSITION 3.1. — *Let $A, B \in k \setminus \{0\}$. The group $E_{A,B}(\bar{k}(t))$ has rank 8 and no non-trivial torsion elements. The generators are contained in the set of points P of the form*

$$P = (at^2 + bt + c, a_1t^3 + a_2t^2 + a_3t + a_4), \quad a, b, c, a_1, a_2, a_3, a_4 \in \bar{k}.$$

Proof. — The equation $E_{A,B}$ defines a smooth cubic over $\bar{k}(t)$ for $At^6 + B$ non-zero. When both A, B are non-zero the cubic equation $E_{A,B}$ is not isomorphic to a constant cubic defined over k . From [21, 10.14] it follows that $\mathcal{E}_{A,B}$ is a rational elliptic surface. The discriminant of $E_{A,B}$ equals $-432 (At^6 + B)^2$. For A, B non-zero the polynomial $At^6 + B$ is separable, hence from the Tate algorithm [23], [22, IV.9.4] it follows that the equation is minimal at all finite places of $\bar{k}(t)$ and at the places corresponding to the solutions of $At^6 + B = 0$ the reduction is of type *II*. To analyse the model at infinity $1/t$ we apply the change of coordinates $s = 1/t$ and compute the integral model $y^2 = x^3 + A + Bs^6$ which is smooth at $s = 0$ for $A \neq 0$.

From the Shioda–Tate formula [21, Theorem 7.4] and [21, Lemma 10.1] it follows that the rank of $E_{A,B}(\bar{k}(t))$ is 8. Classification of rational elliptic surfaces by Oguiso–Shioda [18] implies that the generators of the group $E_{A,B}(\bar{k}(t))$ have height 2 and there is no non-zero torsion point. The group $E_{A,B}(\bar{k}(t))$ with the height pairing $\langle \cdot, \cdot \rangle$ forms an integral lattice of type E_8 . Since the height of each generator P is 2, we obtain that in the model $E_{A,B}$ the coordinates of the point P are polynomials in $\bar{k}[t]$ of degrees 2 and 3, respectively. \square

PROPOSITION 3.2. — *Let $A, B \in \mathbb{Q}^\times$. The subset of $E_{A,B}(\bar{\mathbb{Q}}(t))$ of elements of height 2 decomposes into 8 disjoint subsets O_i for $i = 1, \dots, 8$. Each set O_i is stable under the action of the absolute Galois group $G_{\mathbb{Q}} = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ on the coordinates of the points.*

For A, B sufficiently generic the orbits O_i do not decompose into smaller $G_{\mathbb{Q}}$ -stable subsets.

Remark 3.3. — The term “sufficiently generic” refers to the detailed decision algorithm described in Section 4.

Proof. — Steps of the algorithm:

- (1) Form an ideal $I = (c_i)_{i=0}^6$ in the polynomial ring

$$S[a, b, c, a_1, a_2, a_3, a_4]$$

where $S = \mathbb{Q}(A, B)$, $x = x(P)$, $y = y(P)$ and

$$y^2 - (x^3 + At^6 + B) = \sum_{i=0}^6 c_i t^i.$$

We have

$$\begin{aligned} I = & (a_4^2 - B - c^3, 2a_3a_4 - 3bc^2, -3ac^2 + a_3^2 + 2a_2a_4 - 3b^2c, \\ & -6abc + 2a_2a_3 + 2a_1a_4 - b^3, \\ & -3a^2c - 3ab^2 + a_2^2 + 2a_1a_3, 2a_1a_2 - 3a^2b, -a^3 + a_1^2 - A). \end{aligned}$$

- (2) Compute the elimination ideal J in $S[a, b, c]$ with respect to a, b, c .
 (3) Compute the primary decomposition $\bigcap_i J_i$ of the ideal J .
 (4) Compute the Groebner basis $\{b_i\}$ with respect to the standard lexicographical order of the ideals spanned by $J_i \cup I$.
 (5) Form a scheme O_i which is the vanishing locus of the system $\{b_i\}$.

On the output we obtain the defining equations of the components O_i computed in the step 5. There are exactly eight of the them, so $S_{\text{red}} = \amalg_{i=1}^8 O_i$ where each scheme O_i is of dimension 0, reduced and irreducible over $\mathbb{Q}(A, B)$. For $1 \leq i \leq 8$ the degree of the scheme O_i equals 6, 6, 12, 18, 18, 36, 36, 108, respectively. \square

In the following paragraphs we discuss the structure of the smallest orbits O_1, O_2 and O_3 . The main result of this section is a proof that there exist 8 linearly independent points in those three orbits. Therefore it is enough to study those 8 points in order to determine the rank of the group $E_{A,B}(\mathbb{Q}(t))$ (since there are no torsion points).

We denote by $\mathcal{P}(O)$ the set of points in $E(\overline{\mathbb{Q}}(t))$ which correspond to the $O(\overline{\mathbb{Q}})$ -points of the scheme O in S_{red} . By abuse of notation we also say that the set O contains a point P , if $P \in \mathcal{P}(O)$. Let $\mathcal{L}(O)$ denote the \mathbb{Z} -span of the points in the set O .

Remark 3.4. — To verify that for each choice of non-zero elements A, B the statements below hold (there is no degeneration) we have used a computer and the package Magma. The computation essentially reduces to a calculation similar to the one presented in the proof of Proposition 3.11. In fact, for each proof below we verify the relations between points over the function field extension $\overline{\mathbb{Q}}(A^{1/6}, B^{1/6})$ of $\overline{\mathbb{Q}}(A, B)$ and check that the

lattice produced from the points in the orbit (and the Gram matrix of a given basis) are the same for every choice of nonzero A, B . The verification code is available on the website of one of the authors [6].

Remark 3.5. — To simplify our notation we have adopted the following convention. For a given non-zero rational number $A \in \mathbb{Q}$, we find a polynomial factorization $x^6 - A = \prod_i p_i(x)$, where $p_i(x) \in \mathbb{Q}[x]$ are monic, irreducible over \mathbb{Q} and ordered by the degree: $\deg p_1 \leq \deg p_2 \leq \dots$. We denote by $A^{1/6}$ any fixed root in $\overline{\mathbb{Q}}$ of the polynomial $p_1(x)$. We define in analogy the symbol $B^{1/6}$ for any non-zero rational number $B \in \mathbb{Q}$.

We denote by ζ_3 an arbitrarily fixed root in $\overline{\mathbb{Q}}$ of the polynomial $x^2 + x + 1$ and we define $\sqrt{-3}$ to be $1 + 2\zeta_3$.

We denote by $2^{1/3}$ an arbitrarily fixed root in $\overline{\mathbb{Q}}$ of the polynomial $x^3 - 2$. If either $(A^{1/6})^2$ or $(B^{1/6})^2$ is a root of $x^3 - 2$, we choose $2^{1/3}$ to be equal to one of these values.

In the sections below, we use expressions of the form $\sqrt[k]{cA^eB^f}$ with $k \in \{2, 3, 6\}$ and $e, f \in \{0, 1\}$. We define $\sqrt[k]{cA^eB^f}$ as $\sqrt[k]{c} \cdot (A^{1/6})^{6e/k} \cdot (B^{1/6})^{6f/k}$. We also fix that $\sqrt[3]{-1} = -1$.

3.1.1. Orbit O_1

The orbit O_1 is defined by the following conditions

$$\begin{aligned} a_1^2 &= A, & c^3 &= -B, \\ a_2 &= a_3 = a_4 = a = b = 0 \end{aligned}$$

and determines a list of the following points

$$\mathcal{P}(O_1) = \left\{ \left(-\zeta_3^i \sqrt[3]{B}, \pm \sqrt{At^3} \right) : i \in \{0, 1, 2\} \right\}.$$

The set $\mathcal{P}(O_1)$ consists of 6 points, each of height 2 (under assumption that $AB \neq 0$). A configuration of the curves in the orbit O_1 is described in Figure 3.1.

Let K denote the field $\mathbb{Q}(\sqrt{A}, \sqrt[3]{B}, \zeta_3)$, $\zeta_3^3 = 1$ and $\zeta_3 \neq 1$. Consider a map $\sigma_K : \sqrt[3]{B} \mapsto \zeta_3 \sqrt[3]{B}$ which fixes the other generators of K . If it extends to an automorphism of K , it fixes the subfield $\mathbb{Q}(\sqrt{A}, \zeta_3)$.

Remark 3.6. — In the case when A and B are such that the corresponding automorphism does not exist we denote by T^σ the point obtained from T by substitution of $\zeta_3 \sqrt[3]{\alpha}$ in place of $\sqrt[3]{\alpha}$.

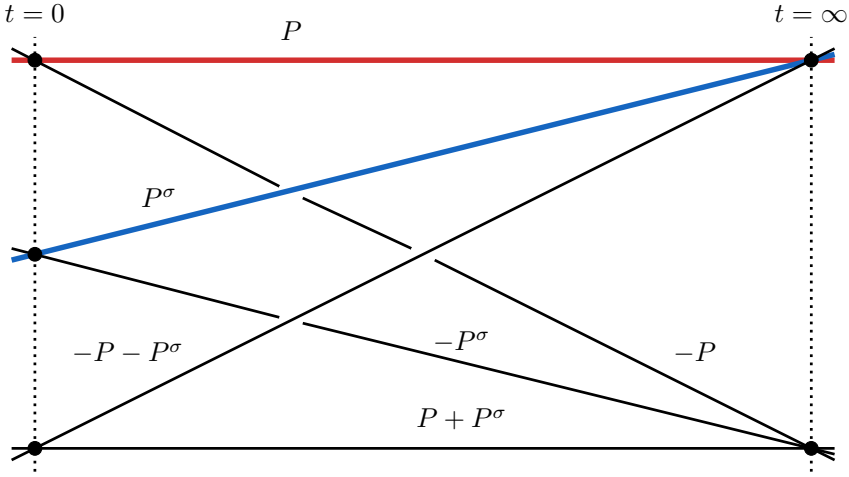


Figure 3.1. Configuration of the lines in $\mathcal{P}(O_1)$ on the surface.

PROPOSITION 3.7. — Let A, B be non-zero elements in \mathbb{Q} . Then a point $P = (-\sqrt[3]{B}, \sqrt{At^3})$ lies on the elliptic curve $E = E_{A,B}$ and

$$P + P^{\sigma\kappa} + P^{\sigma\kappa^2} = 0.$$

Moreover, the height $\langle P, P \rangle$ equals 2 and the height pairing matrix of the points $P, P^{\sigma\kappa}$ is

$$M := \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}.$$

In particular, the points $P, P^{\sigma\kappa}$ are linearly independent in $E(\overline{\mathbb{Q}}(t))$. Moreover, the \mathbb{Z} -linear span $\mathcal{L}(O_1)$ has rank 2 and basis $P, P^{\sigma\kappa}$.

Proof. — The first equality follows from a direct computation. The height $\langle P, P \rangle$ of P and the height $\langle P^{\sigma\kappa}, P^{\sigma\kappa} \rangle$ of $P^{\sigma\kappa}$ is computed with the formula described in Section 3.1.

To compute the height pairing matrix M we need only to check that the height of $P + P^{\sigma\kappa}$ is 2 and the equality $\langle P, P^{\sigma\kappa} \rangle = -1$ follows from bilinearity of the pairing. The determinant of M is non-zero, hence the points P and $P^{\sigma\kappa}$ are linearly independent over \mathbb{Z} . Finally, observe that $\mathcal{P}(O_1)$ has 6 elements which coincide with the elements of the set

$$\{\pm P, \pm P^{\sigma\kappa}, \pm P \pm P^{\sigma\kappa}\}. \quad \square$$

3.1.2. Orbit O_2

The orbit O_2 is defined by the following equations

$$\begin{aligned} a_4^2 &= B, & a^3 &= -A, \\ a_1 &= a_2 = a_3 = b = c = 0. \end{aligned}$$

Configuration of the curves in the orbit O_2 is very similar to Figure 3.1. Let K' denote the field $\mathbb{Q}(\sqrt{B}, \sqrt[3]{A}, \zeta_3)$ and let $\sigma_{K'} : \sqrt[3]{A} \mapsto \zeta_3 \sqrt[3]{A}$, which fixes the other generators of K' , denote a map which if extended to an automorphism of K' fixes the subfield $\mathbb{Q}(\sqrt{B}, \zeta_3)$. We consider a point $Q = (-\sqrt[3]{At^2}, \sqrt{B})$ that corresponds to a point on the orbit O_2 .

PROPOSITION 3.8. — *Let A, B be non-zero elements from \mathbb{Q} . Then the height pairing matrix of the points $Q, Q^{\sigma_{K'}}$ is M from Proposition 3.7. The following equality*

$$Q + Q^{\sigma_{K'}} + Q^{\sigma_{K'}^2} = 0$$

holds and $\mathcal{L}(O_2)$ is of rank 2 with basis $Q, Q^{\sigma_{K'}}$.

Proof. — We omit the proof since it is analogous to that of Proposition 3.7. \square

3.1.3. Equations of O_3

The orbit O_3 is defined by the following equation

$$\begin{aligned} a_1^2 &= A, & a_4^2 &= B, & 2a_1a_4 &= b^3, \\ a &= c = a_2 = a_3 = 0. \end{aligned}$$

Note that $b^6 - 4AB$ belongs to the ideal of O_3 . A configuration of the points in the orbit O_3 is depicted in the Figure 3.2 with extra data in Table 3.1.

Let L denote the field $\mathbb{Q}(\sqrt{A}, \sqrt{B}, \zeta_3, \sqrt[3]{4AB})$. Let σ_L be a map which maps $\sqrt[3]{4AB} \mapsto \zeta_3 \sqrt[3]{4AB}$ and fixes the other generators of L . If it extends to an automorphism of L , then it fixes the subfield $\mathbb{Q}(\sqrt{A}, \sqrt{B}, \zeta_3)$. Let τ_L denote a map such that $\tau_L(\sqrt{B}) = -\sqrt{B}$. If it extends to an automorphism of L , then it fixes the field $\mathbb{Q}(\sqrt{A}, \zeta_3, s)$.

Remark 3.9. — In the case when A and B are such that the corresponding automorphism does not exist we denote by T^r the point obtained from T by substitution of $-\sqrt{\alpha}$ in place of $\sqrt{\alpha}$.

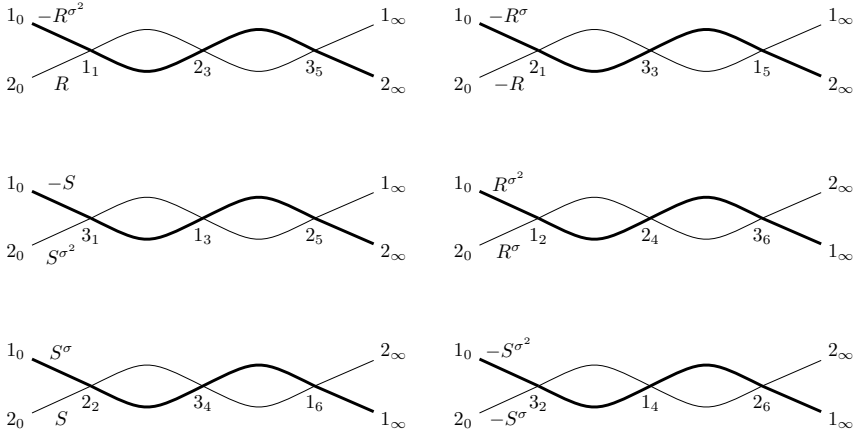


Figure 3.2. Configuration of the lines in $\mathcal{P}(O_3)$ on the surface.

We consider the points

$$R = \left(\frac{2\sqrt{A}\sqrt{B}}{\sqrt[3]{4AB}}t, \sqrt{At^3 + \sqrt{B}} \right),$$

$$S = \left(-\frac{2\sqrt{A}\sqrt{B}}{\sqrt[3]{4AB}}t, \sqrt{At^3 - \sqrt{B}} \right)$$

contained in $E_{A,B}(\overline{\mathbb{Q}}(t))$.

PROPOSITION 3.10. — Let A, B be non-zero elements from \mathbb{Q} . Points R and S have height 2 and they satisfy the following identities

$$R + R^{\sigma_L} + R^{\sigma_L^2} = 0$$

and

$$S + S^{\sigma_L} + S^{\sigma_L^2} = 0.$$

Table 3.1. Description of the labels in Figure 3.2

Point label	description
1_0	$(0, \sqrt{B})$ at $t = 0$
2_0	$(0, -\sqrt{B})$ at $t = 0$
1_∞	$(0, \sqrt{A})$ at $t = \infty$
2_∞	$(0, -\sqrt{A})$ at $t = \infty$
m_i where $0 < i < \infty$	$(\zeta_6^{2m-1}(2B)^{1/3}, 0)$ at $t = \zeta_6^{i-1}(\frac{A}{B})^{1/6}$

The Gram matrix of the pairs R, R^{σ_L} and S, S^{σ_L} is M from Proposition 3.7. The linear span $\mathcal{L}(O_3)$ has rank 4 and basis $R, R^{\sigma_L}, S, S^{\sigma_L}$.

Proof. — We omit the proof since it is analogous to that of Proposition 3.7. \square

PROPOSITION 3.11. — For A and B non-zero rational numbers a subgroup in $E(\overline{\mathbb{Q}}(t))$ spanned by the points $\{P, P^{\sigma_K}, Q, Q^{\sigma_{K'}}, R, R^{\sigma_L}, S, S^{\sigma_L}\}$ has rank 8 and the Gram matrix equal to the Kronecker product $I_4 \otimes M$ where I_4 is the 4 by 4 identity matrix.

Proof. — Let B_i denote the i -th element of the ordered tuple

$$(P, P^{\sigma_K}, Q, Q^{\sigma_{K'}}, R, R^{\sigma_L}, S, S^{\sigma_L}).$$

We need to show that $\langle B_i, B_j \rangle = 0$ for $i < j$ and $i+1 \neq j$, $i, j \in \{1, \dots, 8\}$. From the bilinearity of the height pairing this is equivalent to showing $\langle B_i + B_j, B_i + B_j \rangle = 4$ or equivalently $\overline{B_i + B_j} \cdot \overline{O} = 1$. To show that the curve $\overline{B_i + B_j}$ intersects the image of the zero section \overline{O} exactly once we look at the x -coordinate of $\overline{B_i + B_j}$. For $t = \infty$ there is no intersection with \overline{O} and for each pair of (i, j) defined above there is exactly one intersection if A, B are both non-zero. This last condition is verified in Magma code attached to this paper. \square

3.2. Further orbits

Although it is not strictly necessary for our arguments to compute the precise structure of the orbits O_i for $i \geq 4$ we include it for completeness. Some of those orbits could be used to provide an alternative proof of the theorem of Section 4. For each orbit O_i we compute the rank and a basis of the linear span $\mathcal{L}(O_i)$. We also use some of the points from orbits O_4, O_5, O_6 and O_7 to conveniently describe bases of points in $E_{A,B}(\mathbb{Q}(t))$, cf. Section 4.3.

3.2.1. Orbits of size 18

The orbit O_4 has size 18 and is defined by the following equations

$$\begin{aligned} a^3 &= -4A, \quad c^3 = -B, \quad a_3^2 = 3ac^2, \\ a_1 &= -\frac{1}{2B}a_3ac^2, \quad a_2 = a_4 = b = 0. \end{aligned}$$

Let $U_{j,k,m}$ denote a point

$$\left(-\zeta_3^j \left(\sqrt[3]{4At^2} + \sqrt[3]{B}\zeta_3^k \right), \frac{(-1)^{m+1} \sqrt[6]{A}\sqrt{-3} \left(\sqrt[3]{4At^2} + 2\sqrt[3]{B}\zeta_3^k \right) t}{2^{2/3}} \right)$$

where j, k belong to the set $\{0, 1, 2\}$ and m equals 1 or 2.

PROPOSITION 3.12. — *Let A, B be non-zero elements from \mathbb{Q} . It follows that*

$$\mathcal{P}(O_4) = \{U_{j,k,m} : j, k \in \{0, 1, 2\}, m \in \{1, 2\}\}.$$

The linear span $\mathcal{L}(O_4)$ has rank 4 and is generated by the points $U_{0,0,1}, U_{0,1,1}, U_{1,0,1}, U_{1,1,1}$. The lattice $(\mathcal{L}(O_4), \langle \cdot, \cdot \rangle)$ is isometric to the D_4 lattice.

Proof. — The points in the set $\mathcal{P}(O_4)$ satisfy the following relations

$$\begin{aligned} U_{j,k,1} &= -U_{j,k,2} && \text{for any } j, k, \\ U_{j,0,1} + U_{j,1,1} + U_{j,2,1} &= 0 && \text{for any } j, \\ U_{0,k,1} + U_{1,k,1} + U_{2,k,1} &= 0 && \text{for any } k. \end{aligned}$$

Since $\mathcal{P}(O_4)$ contains 18 points, the relations above imply that there are at most 4 points independent over \mathbb{Z} in $\mathcal{L}(O_4)$. We check by a direct computation that the points indicated in the proposition are linearly independent. The Gram matrix of their height pairing is conjugate to the Gram matrix of the lattice D_4 . \square

The orbit O_5 has size 18 and is defined by the equations

$$\begin{aligned} a^3 &= -A, \quad c^3 = -4B, \quad a_4^2 = -3B, \\ a_2 &= -\frac{1}{2B}a_4ac^2, \quad a_1 = a_3 = b = 0. \end{aligned}$$

Let $V_{j,k,m}$ denote a point

$$V_{j,k,m} = \left(-\zeta_3^j \left(\sqrt[3]{A}\zeta_3^k t^2 + \sqrt[3]{4B} \right), (-1)^{m+1} \sqrt[6]{B}\sqrt{-3} \left(\sqrt[3]{2A}\zeta_3^k t^2 + \sqrt[3]{B} \right) \right).$$

PROPOSITION 3.13. — *Let A, B be non-zero elements from \mathbb{Q} . It follows that*

$$\mathcal{P}(O_5) = \{V_{j,k,m} : j, k \in \{0, 1, 2\}, m \in \{1, 2\}\}.$$

The linear span $\mathcal{L}(O_4)$ has rank 4 and is generated by the points $V_{0,1,1}, V_{0,1,1}, V_{1,0,1}, V_{1,1,1}$. The lattice $(\mathcal{L}(O_5), \langle \cdot, \cdot \rangle)$ is isometric to the D_4 lattice.

Proof. — We omit the proof since it is analogous to that of Proposition 3.12. \square

3.2.2. Orbits of size 36

The orbit O_6 is of size 36 and is defined by

$$\begin{aligned} a_4^2 &= -3B, \quad b^6 = -108AB, \quad c^3 = -4B, \\ a &= -\frac{1}{6B}b^2c^2, \quad a_1 = -\frac{1}{6B}a_4b^3, \quad a_2 = -\frac{1}{3B}a_4b^2c, \quad a_3 = -\frac{1}{2B}a_4bc^2. \end{aligned}$$

Let $W_{j,k,m,n}$ denote a point

$$\begin{aligned} &\left(-2\sqrt[3]{A}(\zeta_3 + 1)\zeta_3^{2j+2k}t^2 + (\zeta_3 + 2)(-1)^m\sqrt[6]{4AB}\zeta_3^k t + \sqrt[3]{-4B}\zeta_3^j, \right. \\ &\quad 3\sqrt{A}(-1)^{mt^3} + 2\sqrt[3]{2A}\sqrt[6]{B}(\zeta_3 - 1)\zeta_3^{j+2k}t^2 \\ &\quad \left. - 3\sqrt[6]{A}\sqrt[3]{4B}(-1)^{mt}\zeta_3^{2j+k+1} + \sqrt{-3B} \right). \end{aligned}$$

PROPOSITION 3.14. — *Let A, B be non-zero elements from \mathbb{Q} . It follows that*

$$\mathcal{P}(O_6) = \{W_{j,k,m,n} : j, k \in \{0, 1, 2\}, m, n \in \{0, 1\}\}.$$

The linear span $\mathcal{L}(O_6)$ has rank 6 and is generated by the points $W_{0,0,0,0}$, $W_{0,1,0,0}$, $W_{0,0,1,0}$, $W_{0,1,1,0}$, $W_{1,0,0,0}$, $W_{1,1,0,0}$. The lattice $(\mathcal{L}(O_6), \langle \cdot, \cdot \rangle)$ is isometric to the E_6 lattice.

Proof. — We have the following relations among the points in the set $\mathcal{P}(O_6)$:

$$\begin{aligned} W_{j,k,m,0} + W_{j,k,m,1} &= 0 \quad \text{for any } j, k, m, \\ \sum_{j=0}^2 W_{j,j+s,m,n} &= 0 \quad \text{for any } m, n, s, \\ \sum_{k=0}^2 W_{j,k,m,n} &= 0 \quad \text{for any } j, m, n, \\ W_{1,1,1,0} &= W_{0,1,1,0} + W_{1,1,0,0} - W_{0,1,0,0}, \\ W_{1,0,1,0} &= W_{0,0,1,0} + W_{1,0,0,0} - W_{0,0,0,0}. \end{aligned}$$

From those relations it follows that there are at most 6 linearly independent points in $\mathcal{P}(O_6)$ and we check by a direct computation that they span an E_6 type lattice. \square

The orbit O_7 has size 18 and is defined by

$$\begin{aligned} b^6 &= -108AB, \quad c^3 = 8B, \quad a_4^2 = 9B \\ a &= \frac{1}{12B}b^2c^2, \quad a_1 = \frac{1}{18B}a_4b^3, \quad a_2 = \frac{1}{6B}a_4b^2c, \quad a_3 = \frac{1}{6B}a_4bc^2 \end{aligned}$$

Let $X_{j,k,m,n}$ denote a point where $j, k \in \{0, 1, 2\}$ and $m, n \in \{0, 1\}$. The x -coordinate of $X_{j,k,m,n}$ is

$$\left(\zeta_3^k \left(t^2 \left(\sqrt[3]{4A} (\zeta_3 + 1) \zeta_3^{2j}\right) + \left((\zeta_3 + 2) (-1)^n \sqrt[6]{4AB}\right) t + 2\sqrt[3]{B} \zeta_3^j\right)\right)$$

and the y -coordinate is

$$\begin{aligned} (-1)^m \left(\left(\sqrt{A} (2\zeta_3 + 1) (-1)^n \right) t^3 + \left(3\sqrt[3]{4A} \sqrt[6]{B} (\zeta_3 + 1) \zeta_3^j \right) t^2 \right. \\ \left. + \left(2\sqrt[6]{A} \sqrt[3]{2B} (\zeta_3 + 2) (-1)^n \zeta_3^{2j} \right) t + 3\sqrt{B} \right). \end{aligned}$$

PROPOSITION 3.15. — *Let A, B be non-zero elements from \mathbb{Q} . It follows that*

$$\mathcal{P}(O_7) = \{X_{j,k,m,n} : j, k \in \{0, 1, 2\}, m, n \in \{0, 1\}\}.$$

The linear span $\mathcal{L}(O_7)$ has rank 6 and is generated by the points

$$X_{0,0,0,0}, X_{0,1,0,0}, X_{0,0,0,1}, X_{0,1,0,1}, X_{1,0,0,0}, X_{1,1,0,0}.$$

The lattice $(\mathcal{L}(O_7), \langle \cdot, \cdot \rangle)$ is isometric to the E_6 lattice.

Proof. — We omit the proof since it is analogous to that of Proposition 3.14. \square

3.2.3. Orbit of size 108

The orbit O_8 is the longest one, of size 108, with the following defining polynomial equations

$$\begin{aligned} 0 &= 64B^3 + 48B^2c^3 + 228Bc^6 + c^9, \\ b^6 &= \frac{4A(7B^2 + 5Bc^3 + 25c^6)}{3B}, \\ a_4^2 &= B + c^3 \end{aligned}$$

and

$$\begin{aligned} a &= -\frac{b^2c^2(-11504B^2 + 1544Bc^3 + 7c^6)}{5184B^3}, \\ a_1 &= \frac{a_4b^3(2728B^2 + 4340Bc^3 + 19c^6)}{1296B^3}, \\ a_2 &= \frac{a_4b^2(4160B^2c + 2524Bc^4 + 11c^7)}{2592B^3}, \\ a_3 &= -\frac{a_4bc^2(-179B^2 + 227Bc^3 + c^6)}{162B^3} \end{aligned}$$

Let $p(x) = (x^3 + 6x^2 + 4)(x^6 - 6x^5 + 36x^4 + 8x^3 - 24x^2 + 16)$ be a polynomial. We observe that for $c = \alpha B^{1/3}$ the equation $64B^3 + 48B^2c^3 + 228Bc^6 + c^9 = 0$ is equivalent to $p(\alpha) = 0$. Let $c_1(o)$ denote the o -th root of the polynomial $p(x)$ defined by the formula

$$c_1(o) = -2^{2/3} \left(\sqrt[3]{2} \zeta_3^{2(\lfloor \frac{o-1}{3} \rfloor + o - 1)} + \zeta_3^{\lfloor \frac{o-1}{3} \rfloor} + 2^{2/3} \zeta_3^{o-1} \right)$$

for $o \in \{1, \dots, 9\}$.

Let $Y_{o,j,m,n}$ denote a point

$$Y_{o,j,m,n} = (at^2 + bt + c, a_1t^3 + a_2t^2 + a_3t + a_4)$$

for $m, n \in \{-1, 1\}$, $j \in \{0, 1, 2\}$ and $o = 1, \dots, 9$ and where $c = c(o) = c_1(o)B^{1/3}$, $a_4 = a_4(n, o) = (-1)^n B^{1/2}(1 + c_1(o))^{1/2}$ and $b = b(j, m, o) = (-1)^m (AB)^{1/6} (4/3(7 + 5c_1(o)^3 + 25c_1(o)^6))^{1/6} \zeta_3^j$. It is easy to check that the suitable roots of degree 2 and 6 in the expressions above belong to the field $\mathbb{Q}(\zeta_3, 2^{1/3})$.

PROPOSITION 3.16. — *Let A, B be non-zero elements from \mathbb{Q} . It follows that*

$$\mathcal{P}(O_8) = \{Y_{o,j,m,n} : j \in \{0, 1, 2\}, m, n \in \{0, 1\}, o \in \{1, \dots, 9\}\}.$$

The linear span $\mathcal{L}(O_8)$ has rank 8 and is generated by the points $Y_{1,0,0,0}$, $Y_{1,0,1,0}$, $Y_{1,1,0,0}$, $Y_{1,1,1,0}$, $Y_{1,2,0,0}$, $Y_{3,0,0,0}$, $Y_{3,0,1,0}$, $Y_{4,0,0,0}$. The lattice $\mathcal{L}(O_8)$ is isometric to the E_8 lattice.

Proof. — We have the following equalities

$$\begin{aligned} Y_{o,j,m,0} + Y_{o,j,m,1} &= 0, \\ Y_{1,j,m,0} + Y_{3,j,m,0} + Y_{2,j,m+1,0} &= 0, \\ Y_{4,j,m,0} + Y_{5,j,m,0} + Y_{6,j,m+1,0} &= 0, \\ Y_{8,j,m,0} + Y_{9,j,m,0} + Y_{7,j,m+1,0} &= 0, \end{aligned}$$

for any choice of o, j, m . We also have the following relation

$$\sum_{j,m} Y_{o,j,m,0} = 0$$

for any $o \in \{1, 3, 4, 5, 8, 9\}$. Relations above allow us to reduce the spanning set for $\mathcal{L}(O_8)$ to 30 points among which we find pairs which add up to the same points. This generates another 21 relations and we compute the height pairing matrix for the remaining 9 points. The height matrix has rank 8 and its kernel provides the final relation. Finally we check that the lattice of rank 8 that we have obtained has discriminant 1, thus it must

be isomorphic to E_8 since the whole Mordell–Weil lattice $E_{A,B}(\overline{\mathbb{Q}}(t))$ is isomorphic to the latter by [18]. \square

Remark 3.17. — We computed the relation between the roots of the Mordell–Weil lattice in terms of orbits. Let $R(G)$ denote the subset of elements in $G \subset E_{A,B}(\overline{\mathbb{Q}}(t))$ of height 2. The following equalities hold

$$\begin{aligned} R(\mathcal{L}(O_1)) &= \mathcal{P}(O_1) \\ R(\mathcal{L}(O_2)) &= \mathcal{P}(O_2) \\ R(\mathcal{L}(O_3)) &= \mathcal{P}(O_3) \\ R(\mathcal{L}(O_4)) &= \mathcal{P}(O_1) \cup \mathcal{P}(O_4) \\ R(\mathcal{L}(O_5)) &= \mathcal{P}(O_2) \cup \mathcal{P}(O_5) \\ R(\mathcal{L}(O_6)) &= \mathcal{P}(O_2) \cup \mathcal{P}(O_3) \cup \mathcal{P}(O_5) \cup \mathcal{P}(O_6) \\ R(\mathcal{L}(O_7)) &= \mathcal{P}(O_1) \cup \mathcal{P}(O_3) \cup \mathcal{P}(O_4) \cup \mathcal{P}(O_7) \\ R(\mathcal{L}(O_8)) &= \bigcup_{i=1}^8 \mathcal{P}(O_i) \end{aligned}$$

4. Proof of the main theorem

4.1. Structure of the Galois modules

Let A, B be non-zero rational numbers. In this section we compute in detail the Galois action of the group $G = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the module $M = E_{A,B}(\overline{\mathbb{Q}}(t))$ and the \mathbb{Q} -vector space $V = M \otimes \mathbb{Q}$. It follows from the discussion in Section 3.1 that V is a vector space of dimension 8 over \mathbb{Q} . We define four subspaces $V_i \subset V$, $i = 1, 2, 3, 4$ by their \mathbb{Q} -generators

$$\begin{aligned} V_1 &= \text{span}_{\mathbb{Q}}\langle P, P^{\sigma_K} \rangle, \\ V_2 &= \text{span}_{\mathbb{Q}}\langle Q, Q^{\sigma_{K'}} \rangle, \\ V_3 &= \text{span}_{\mathbb{Q}}\langle R + S, R^{\sigma_L} + S^{\sigma_L} \rangle, \\ V_4 &= \text{span}_{\mathbb{Q}}\langle R - S, R^{\sigma_L} - S^{\sigma_L} \rangle. \end{aligned}$$

PROPOSITION 4.1. — *Let A, B be non-zero rational numbers. The subspaces V_i are $\mathbb{Q}[G]$ -submodules of $V = E_{A,B}(\overline{\mathbb{Q}}(t)) \otimes \mathbb{Q}$. The $\mathbb{Q}[G]$ -module V is a direct sum $V_1 \oplus V_2 \oplus V_3 \oplus V_4$ as $\mathbb{Q}[G]$ -modules. and each subspace V_i is of dimension 2 over \mathbb{Q} .*

Proof. — Proposition 3.7 implies that the submodule V_1 is stable under the action of the group G . Proposition 3.8 implies that the submodule V_2 is G -stable. Proposition 3.10 implies that V_3 and V_4 are G -stable.

To prove that each V_i has dimension 2 over \mathbb{Q} we observe that the chosen spanning sets have the Gram matrix M with respect to the height pairing (defined in Proposition 3.7). Hence, the assumption that there exists two non-zero $x, y \in \mathbb{Q}$ such that $xg_1 + yg_2 = 0$ for g_1, g_2 - spanning elements of V_i , would imply that $M \cdot (x, y)^T = (0, 0)^T$ and since $\det M = 3$, $(x, y) = (0, 0)$.

Next, we show that V is a direct sum of V_i submodules. Equivalently, we show that the intersections $V_i \cap V_j$ are zero. The equality $V_i \cap V_j = 0$ for $i = 1, 2$ and $j \neq i$ follows directly from the structure of the Gram matrix for the set $\{P, P^{\sigma_K}, Q, Q^{\sigma_{K'}}, R, R^{\sigma_L}, S, S^{\sigma_L}\}$ described in Proposition 3.11. To verify $V_3 \cap V_4 = 0$ we check that $\langle R + S, R - S \rangle = 0$ and $\langle R + S, R^{\sigma_L} - S^{\sigma_L} \rangle = 0$ and we do a similar calculation for $R - S$. \square

Since the elliptic surface $\mathcal{E}_{A,B}$ has no torsion sections (Proposition 3.1) it follows that $V^G = E_{A,B}(\mathbb{Q}(t)) \otimes \mathbb{Q}$ and also $E_{A,B}(\mathbb{Q}(t)) = E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V^G$. We denote by V_i^G the G -invariants of a submodule V_i .

PROPOSITION 4.2. — *Let A, B be non-zero rational numbers and $E = E_{A,B}$. The following conditions hold:*

- *If $V_1^G \neq \{0\}$, then B is a cube.*
- *If $V_2^G \neq \{0\}$, then A is a cube.*
- *If $V_3^G \neq \{0\}$, then $4AB$ is a cube.*
- *If $V_4^G \neq \{0\}$, then $4AB$ is a cube.*

Proof. — Let X denote B, A or $4AB$. If X is not a cube in \mathbb{Q} , then there exists an automorphism in $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which restricts to respectively $\sigma_K, \sigma_{K'}$ or σ_L . In the \mathbb{Q} -basis of V_i the matrix of σ is

$$M := \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$$

which has characteristic polynomial $1 + x + x^2$, hence there are no fixed vectors in the representation attached to V_i , so $V_i \cap E(\mathbb{Q}(t)) = \{0\}$. \square

Let r_i denote the dimension of the \mathbb{Q} -space V_i^G . Note that r_i is also the \mathbb{Z} -rank of the module $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_i^G$. Let $x = x' \cdot \square$ denote a number x which is a product of x' with a square in \mathbb{Q}^\times .

PROPOSITION 4.3 (Analyse representation V_1). — *Assume B is a cube. Then one of the following conditions is true.*

- (i) *If $A \neq -3 \times \square$, then $r_1 = 0$.*

- (ii) If $A = \square$, then $r_1 = 1$ and $V_1^G = \langle P \rangle$.
- (iii) If $A = -3 \times \square$, then $r_1 = 1$ and $V_1^G = \langle P + 2P^{\sigma\kappa} \rangle$.

Proof.

(i). — The assumptions imply that there exists an automorphism θ in $\text{Gal}(\mathbb{Q}(\sqrt{A}, \zeta_3)/\mathbb{Q})$ which satisfies $\theta(\sqrt{A}) = \sqrt{A}$ and $\theta(\zeta_3) = -\zeta_3$. Hence, in the given basis of V_1 it has matrix $\begin{pmatrix} 1 & \\ 0 & -1 \end{pmatrix}$ and an eigenvector $P \otimes 1$ with eigenvalue 1. This vector is not fixed under the automorphism that sends \sqrt{A} to $-\sqrt{A}$ and fixes ζ_3 . Hence $r_1 = 0$.

(ii). — In this case the automorphism θ again fixes only a 1-dimensional subspace spanned by $P \otimes 1$ which belongs to $E(\mathbb{Q}(t)) \otimes \mathbb{Q}$, hence $r_1 = 1$.

(iii). — In this case the action of θ in the basis of V_1 provides a matrix $\begin{pmatrix} -1 & \\ 0 & 1 \end{pmatrix}$, hence it fixes the space spanned by the vector $(P + 2P^{\sigma\kappa}) \otimes 1$ which is rational, hence $r_1 = 1$. □

Propositions 4.2 and 4.3 completely characterize the structure of the subspace V_i^G .

Table 4.1. Points on the elliptic surface $\mathcal{E} : y^2 = x^3 + At^6 + B$.

Point	Formula	Height	Orbit
P	$(-\sqrt[3]{B}, \sqrt{At^3})$	2	O_1
Q	$(-\sqrt[3]{At^2}, \sqrt{B})$	2	O_2
R	$(\frac{2\sqrt{A}\sqrt{B}}{s}t, \sqrt{At^3 + \sqrt{B}})$	2	O_3
S	$(-\frac{2\sqrt{A}\sqrt{B}}{s}t, \sqrt{At^3 - \sqrt{B}})$	2	O_3

PROPOSITION 4.4 (Analyse representation V_2). — Assume A is a cube.

- (i) If $B \neq -3 \times \square$, then $r_2 = 0$.
- (ii) If $B = \square$, then $r_2 = 1$ and $V_2^G = \langle Q \rangle$.
- (iii) If $B = -3 \times \square$, then $r_2 = 1$ and $V_2^G = \langle Q + 2Q^{\sigma\kappa'} \rangle$.

Proof. — We omit the proof since it is analogous to that of Proposition 4.3. □

PROPOSITION 4.5 (Analyse representation V_3). — Assume $4AB$ is a cube.

- (i) If $A \neq -3 \times \square$, then $r_3 = 0$.
- (ii) If $A = \square$, then $r_3 = 1$ and $V_1^G = \langle R + S \rangle$.
- (iii) If $A = -3 \times \square$, then $r_3 = 1$ and

$$V_3^G = \langle R + S + 2(R^{\sigma L} + S^{\sigma L}) \rangle.$$

Proof. — We omit the proof since it is analogous to that of Proposition 4.3. \square

PROPOSITION 4.6 (Analyse representation V_4). — Assume $4AB$ is a cube.

- (i) If $B \neq -3 \times \square$, then $r_4 = 0$.
- (ii) If $B = \square$, then $r_4 = 1$ and $V_4^G = \langle R - S \rangle$.
- (iii) If $B = -3 \times \square$, then $r_4 = 1$ and $V_4^G = \langle R - S + 2(R^{\sigma_L} - S^{\sigma_L}) \rangle$.

Proof. — We omit the proof since it is analogous to that of Proposition 4.3. \square

4.2. Decision diagrams

The results of Section 4.1 are sufficient to conclude the value of the rank $r_{\mathcal{E}}$ of $E_{A,B}(\mathbb{Q}(t))$ based on the execution of the procedure which on input takes a pair of non-zero rational numbers A, B and prints on the output the value $r = r_{\mathcal{E}}$ (indicated by a red rectangular box in the diagrams).

The starting point for the procedure is the diagram on Figure 4.1. Each diamond box is a query with possible yes or no answer. Blue circles with numbers 1, 2, 3 denote the starting point of a subroutine explained on Figures 4.2, 4.3 and 4.4.

4.3. Rational basis

We compute below the set of generators of the group $E_{A,B}(\mathbb{Q}(t))$ for each choice of non-zero rational numbers A, B . We follow the structure of the diagrams from Section 4.2. We denote each paragraph with the label that corresponds to yes/no decisions made in the decision diagram (abbreviated as Y/N respectively) in order to reach the specific basis.

We use the following facts for the proofs below:

- (\dagger) Height function is quadratic and the minimal height of the non-zero point in $E_{A,B}(\overline{\mathbb{Q}}(t))$ is 2. There are no points of height 3 in the group $E_{A,B}(\overline{\mathbb{Q}}(t))$. In particular there are no such points in the group $E_{A,B}(\mathbb{Q}(t))$.
- The span of points $\{e_i\}$ is not m -saturated in $E_{A,B}(\overline{\mathbb{Q}}(t))$ if and only if one can find a linear combination $\sum_i m_i e_i$ with $m_i \in \{0, \dots, m-1\}$ which is m -divisible and non-zero.
- Let G denote the Gram matrix of the span S of points $\{e_i\}_{i=1}^m$ for some positive integer m . If $\det G \neq 0$, then it is an integer. If S is not m -saturated, then m^2 divides $\det G$.

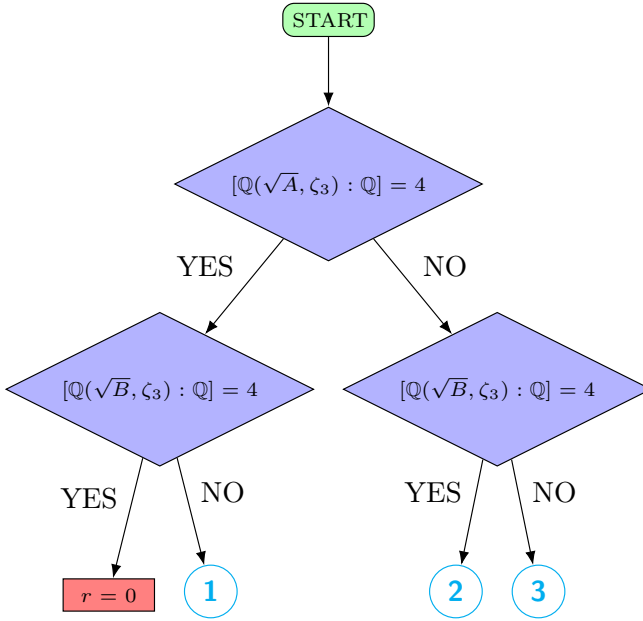


Figure 4.1. Initial point of the procedure

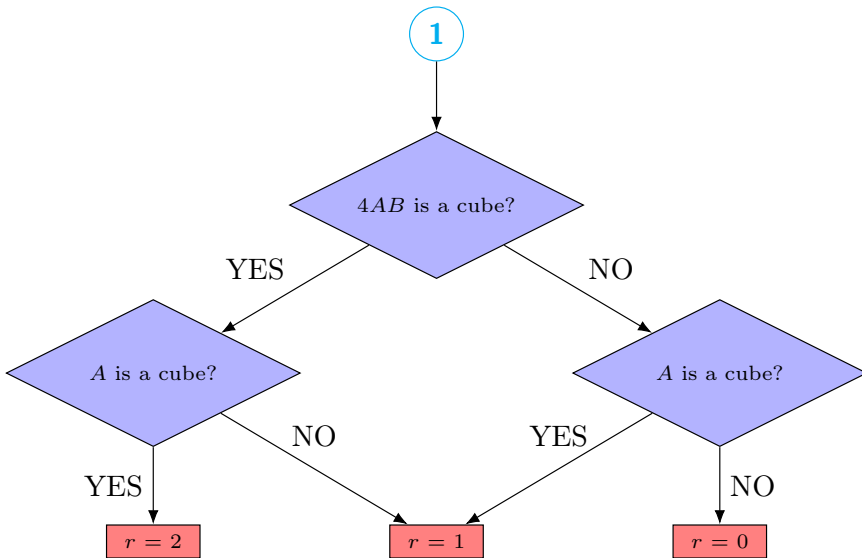


Figure 4.2. Subroutine 1

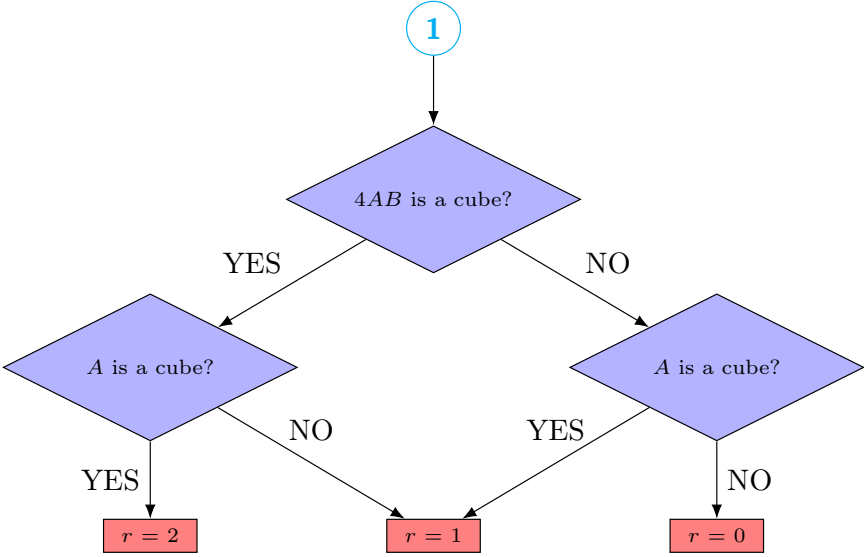


Figure 4.3. Subroutine 2

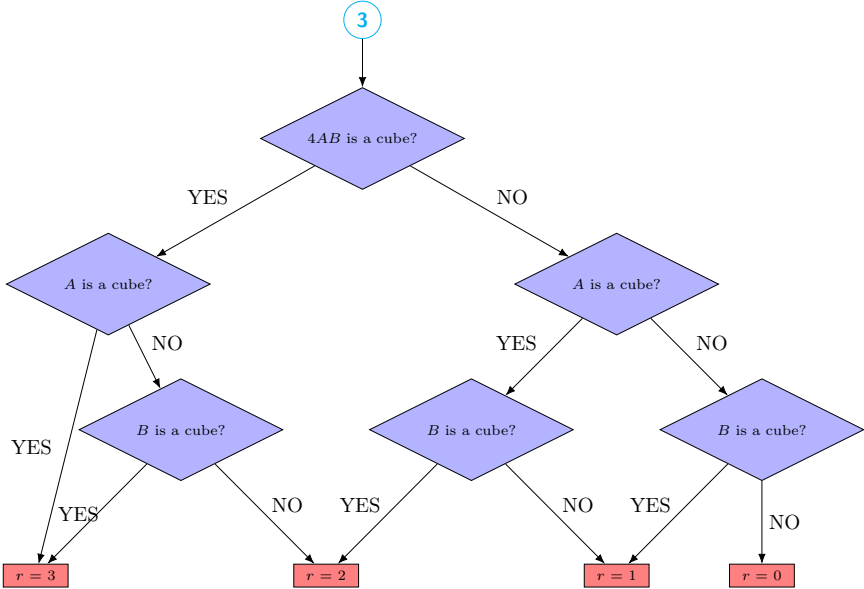


Figure 4.4. Subroutine 3

Table 4.2. Points on the elliptic curve $E_{A,B} : y^2 = x^3 + At^6 + B$.

Point	Formula	Height
$R + S$	$\left(\frac{1}{t^2} \frac{B}{\sqrt[3]{4AB}}, \frac{1}{t^3} \left(-\sqrt{At^6} - \frac{B}{2\sqrt{A}} \right) \right)$	4
$R - S$	$\left(t^4 \frac{A}{\sqrt[3]{4AB}}, -\frac{A}{2\sqrt{B}} t^6 - \sqrt{B} \right)$	4
$P + 2P^\sigma$	$\left(\frac{4A}{-3\sqrt[3]{B}} t^6 - \sqrt[3]{B}, \frac{8A\sqrt{-3A}}{-3^2 B} t^9 - 3\sqrt{-3At^3} \right)$	6
$Q + 2Q^\sigma$	$\left(\frac{4B}{-3\sqrt[3]{At^4}} - \sqrt[3]{At^2}, \frac{8B\sqrt{-3B}}{-3^2 At^6} - 3\sqrt{-3B} \right)$	6
$R + S + 2(R^\sigma + S^\sigma)$	$\left(-\frac{16A^2 t^{12} + 16ABt^6 + B^2}{3B \sqrt[3]{4ABt^2}}, -\frac{(2At^6 + B)(-32A^2 t^{12} - 32ABt^6 + B^2)}{6B^2 \sqrt{-3At^3}} \right)$	12
$R - S + 2(R^\sigma - S^\sigma)$	$\left(-\frac{A^2 t^{12} + 16ABt^6 + 16B^2}{3A \sqrt[3]{4ABt^8}}, -\frac{(At^6 + 2B)(A^2 t^{12} - 32ABt^6 - 32B^2)}{6A^2 \sqrt{-3Bt^{12}}} \right)$	12

4.3.1. When $r_{\mathcal{E}} = 1$

In the following cases, the rank of $E_{A,B}(\mathbb{Q}(t))$ is 1 and the union of the bases of the submodules $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_i^G$ gives the full basis of the Mordell–Weil lattice simply by the property (†). We give two choices for the basis, but in each case it can easily be determined: it is P or $R + S$ (resp. Q or $R - S$) if A (resp. B) is a square, and $P + 2P^\sigma$ or $R + S + 2(R + S)^\sigma$ (resp. $Q + 2Q^\sigma$ or $R - S + 2(R - S)^\sigma$) if A (resp. B) is -3 times a square.

YNYN

$$[\mathbb{Q}(\sqrt{A}, \zeta_3) : \mathbb{Q}] = 4 \wedge [\mathbb{Q}(\sqrt{B}, \zeta_3) : \mathbb{Q}] = 2 \wedge 4AB = \eta^3 \wedge A \neq \eta^3$$

- $r_1 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_1^G$ basis: empty
- $r_2 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_2^G$ basis: empty
- $r_3 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_3^G$ basis: empty
- $r_4 = 1$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_4^G$ basis: $R - S$ or $R - S + 2(R - S)^\sigma$.

YNNY

$$[\mathbb{Q}(\sqrt{A}, \zeta_3) : \mathbb{Q}] = 4 \wedge [\mathbb{Q}(\sqrt{B}, \zeta_3) : \mathbb{Q}] = 2 \wedge 4AB \neq \eta^3 \wedge A = \eta^3$$

- $r_1 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_1^G$ basis: empty
- $r_2 = 1$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_2^G$ basis: Q or $Q + 2Q^\sigma$
- $r_3 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_3^G$ basis: empty
- $r_4 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_4^G$ basis: empty.

NYNY

$$[\mathbb{Q}(\sqrt{A}, \zeta_3) : \mathbb{Q}] = 2 \wedge [\mathbb{Q}(\sqrt{B}, \zeta_3) : \mathbb{Q}] = 4 \wedge 4AB \neq \eta^3 \wedge B = \eta^3$$

- $r_1 = 1$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_1^G$ basis: P or $P + 2P^\sigma$
- $r_2 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_2^G$ basis: empty
- $r_3 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_3^G$ basis: empty
- $r_4 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_4^G$ basis: empty.

NYYN

$$[\mathbb{Q}(\sqrt{A}, \zeta_3) : \mathbb{Q}] = 2 \wedge [\mathbb{Q}(\sqrt{B}, \zeta_3) : \mathbb{Q}] = 4 \wedge 4AB = \eta^3 \wedge B \neq \eta^3$$

- $r_1 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_1^G$ basis: empty
- $r_2 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_2^G$ basis: empty
- $r_3 = 1$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_3^G$ basis: $R + S$ or $R + S + 2(R + S)^\sigma$
- $r_4 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_4^G$ basis: empty.

NNNYN

$$[\mathbb{Q}(\sqrt{A}, \zeta_3) : \mathbb{Q}] = 2 \wedge [\mathbb{Q}(\sqrt{B}, \zeta_3) : \mathbb{Q}] = 2 \wedge 4AB \neq \eta^3 \wedge A = \eta^3 \wedge B \neq \eta^3$$

- $r_1 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_1^G$ basis: empty
- $r_2 = 1$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_2^G$ basis: Q or $Q + 2Q^\sigma$
- $r_3 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_3^G$ basis: empty
- $r_4 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_4^G$ basis: empty.

NNNNY

$$[\mathbb{Q}(\sqrt{A}, \zeta_3) : \mathbb{Q}] = 2 \wedge [\mathbb{Q}(\sqrt{B}, \zeta_3) : \mathbb{Q}] = 2 \wedge 4AB \neq \eta^3 \wedge A \neq \eta^3 \wedge B = \eta^3$$

- $r_1 = 1$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_1^G$ basis: P or $P + 2P^\sigma$
- $r_2 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_2^G$ basis: empty
- $r_3 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_3^G$ basis: empty
- $r_4 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_4^G$ basis: empty.

 4.3.2. When $r_{\mathcal{E}} = 2$

In each case we have to verify whether the union of the bases of the submodules $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_i^G$ are saturated in $E_{A,B}(\mathbb{Q}(t))$. We compute for every such choice a basis of points with least heights and a lattice type corresponding to that basis. We denote by $\langle n \rangle$ a rank 1 lattice with the height pairing $b(\cdot, \cdot)$ such that the generator e of the lattice satisfies $b(e, e) = n$. We denote by $A_2(2)$ a lattice of rank 2 such that the Gram matrix of the height pairing has the form

$$\begin{pmatrix} 4 & -2 \\ -2 & 4 \end{pmatrix}.$$

We denote by $\Lambda_1 \oplus \Lambda_2$ the orthogonal sum of lattices Λ_1, Λ_2 . We denote by $\text{diag}(a_1, \dots, a_n)$ an n by n diagonal matrix with entries a_i on the diagonal, ordered from the top-left to the bottom-right.

YNYY

$$[\mathbb{Q}(\sqrt{A}, \zeta_3) : \mathbb{Q}] = 4 \wedge [\mathbb{Q}(\sqrt{B}, \zeta_3) : \mathbb{Q}] = 2 \wedge 4AB = \eta^3 \wedge A = \eta^3$$

- $r_1 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_1^G$ basis: empty
- $r_2 = 1$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_2^G$ basis: Q or $Q + 2Q^\sigma$
- $r_3 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_3^G$ basis: empty
- $r_4 = 1$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_4^G$ basis: $R - S$ or $R - S + 2(R - S)^\sigma$.

— $B = \square$: Points Q and $R - S$ form a basis of the full Mordell–Weil group, since the lattice has discriminant 8 and each non-zero point $\alpha Q + \beta(R - S)$ for $\alpha, \beta \in \{0, 1\}$ has height in the set $\{2, 4, 6\}$.

Minimal height basis. — $Q, R - S$

Lattice type. — $\langle 2 \rangle \oplus \langle 4 \rangle$

— $B = -3 \times \square$: Point $Q + 2Q^\sigma + (R - S) + 2(R - S)^\sigma$ has height 18 and is divisible by 3, namely

$$Q + 2Q^\sigma + (R - S) + 2(R - S)^\sigma = -3V_{0,0,1}.$$

The Gram matrix of the pair $Q + 2Q^\sigma, V_{0,0,1}$ is

$$\begin{pmatrix} 6 & -2 \\ -2 & 2 \end{pmatrix}$$

Let $e_1 = Q + 2Q^\sigma$ and $e_2 = V_{0,0,1}$. The height of the non-zero $\alpha_1 e_1 + \alpha_2 e_2$ where $\alpha_i \in \{0, 1\}$ belongs to the set $\{2, 4, 6\}$. Hence, no non-zero point of this form is 2-divisible. Because the Gram matrix has determinant 8 it follows that $\{e_1, e_2\}$ is a basis of rational points $E_{A,B}(\mathbb{Q}(t))$.

Minimal height basis. — $V_{0,0,1}, Q + 2Q^\sigma + V_{0,0,1}$

Lattice type. — $\langle 2 \rangle \oplus \langle 4 \rangle$

NYYY

$$[\mathbb{Q}(\sqrt{A}, \zeta_3) : \mathbb{Q}] = 2 \wedge [\mathbb{Q}(\sqrt{B}, \zeta_3) : \mathbb{Q}] = 4 \wedge 4AB = \eta^3 \wedge B = \eta^3$$

- $r_1 = 1, E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_1^G$ basis: P or $P + 2P^\sigma$
- $r_2 = 0, E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_2^G$ basis: empty
- $r_3 = 1, E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_3^G$ basis: $R + S$ or $R + S + 2(R + S)^\sigma$
- $r_4 = 0, E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_4^G$ basis: empty.

— $A = \square$: the basis of rational points consists of P and $R + S$ since the basis is 2 saturated and the Gram matrix is the diagonal matrix $\text{diag}(2, 4)$.

Minimal height basis. — $P, R + S$

Lattice type. — $\langle 2 \rangle \oplus \langle 4 \rangle$

— $A = -3 \times \square$: the points $P + 2P^\sigma$ and $R + S + 2(R + S)^\sigma$ form a lattice of index dividing 9 in the full Mordell–Weil lattice $E_{A,B}(\mathbb{Q}(t))$. We have

$$-3U_{0,0,1} = P + 2P^\sigma + R + S + 2(R + S)^\sigma$$

and the basis $e_1 = P + 2P^\sigma, e_2 = U_{0,0,1}$ has the Gram matrix

$$\begin{pmatrix} cc6 & -2 \\ -2 & 2 \end{pmatrix}.$$

The lattice spanned by e_1 and e_2 is 2-saturated.

Minimal height basis. — $U_{0,0,1}, P + 2P^\sigma + U_{0,0,1}$

Lattice type. — $\langle 2 \rangle \oplus \langle 4 \rangle$

NNYNN

$$[\mathbb{Q}(\sqrt{A}, \zeta_3) : \mathbb{Q}] = 2 \wedge [\mathbb{Q}(\sqrt{B}, \zeta_3) : \mathbb{Q}] = 2 \wedge 4AB = \eta^3 \wedge A \neq \eta^3 \wedge B \neq \eta^3$$

- $r_1 = 0, E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_1^G$ basis: empty
- $r_2 = 0, E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_2^G$ basis: empty
- $r_3 = 1, E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_3^G$ basis: $R + S$ or $R + S + 2(R + S)^\sigma$
- $r_4 = 1, E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_4^G$ basis: $R - S$ or $R - S + 2(R - S)^\sigma$.

— $A = \square, B = \square$: the lattice formed by $R + S$ and $R - S$ is not 2-saturated. Points R, S form the basis of $E_{A,B}(\mathbb{Q}(t))$.

Minimal height basis. — R, S

Lattice type. — $\langle 2 \rangle \oplus \langle 2 \rangle$

— $A = -3 \times \square, B = \square$: the basis is $R + R^\sigma + S^\sigma, R - S$ with the Gram matrix $\begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix}$ of determinant 12. To show this is a basis it is enough to check that the lattice is 2-saturated.

Minimal height basis. — $R + R^\sigma + S^\sigma, -(R - S)$

Lattice type. — $A_2(2)$

— $A = \square, B = -3 \times \square$: the basis is $R + R^\sigma - S^\sigma, R + S$ with the Gram matrix $\begin{pmatrix} 4 & 2 \\ 2 & 4 \end{pmatrix}$.

Minimal height basis. — $R + R^\sigma - S^\sigma, -(R + S)$

Lattice type. — $A_2(2)$

— $A = -3 \times \square, B = -3 \times \square$: sublattice of discriminant 144 spanned by the points $R - S + 2(R - S)^\sigma, R + S + 2(R + S)^\sigma$ has the Gram matrix $\text{diag}(12, 12)$. Points $R + 2R^\sigma, S + 2S^\sigma$ with the Gram matrix $\text{diag}(6, 6)$ are linearly independent and they form a 2 and 3 saturated lattice, so they form a basis of the group $E_{A,B}(\mathbb{Q}(t))$.

Minimal height basis. — $R + 2R^\sigma, S + 2S^\sigma$

Lattice type. — $\langle 6 \rangle \oplus \langle 6 \rangle$

NNYY

$$[\mathbb{Q}(\sqrt{A}, \zeta_3) : \mathbb{Q}] = 2 \wedge [\mathbb{Q}(\sqrt{B}, \zeta_3) : \mathbb{Q}] = 2 \wedge 4AB \neq \eta^3 \wedge A = \eta^3 \wedge B = \eta^3$$

- $r_1 = 1$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_1^G$ basis: P or $P + 2P^\sigma$
- $r_2 = 1$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_2^G$ basis: Q or $Q + 2Q^\sigma$
- $r_3 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_3^G$ basis: empty
- $r_4 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_4^G$ basis: empty.

— $A = \square$, $B = \square$: P, Q form a lattice with the Gram matrix $\text{diag}(2, 2)$, hence the lattice is saturated in the Mordell–Weil lattice $E_{A,B}(\mathbb{Q}(t))$.

Minimal height basis. — P, Q

Lattice type. — $\langle 2 \rangle \oplus \langle 2 \rangle$

— $A = \square$, $B = -3 \times \square$: $P, Q + 2Q^\sigma$ form a lattice with the Gram matrix $\text{diag}(2, 6)$, and this could a priori be not 2-saturated. That would be equivalent to $P + Q + 2Q^\sigma$ being 2-divisible, or equivalently $P + Q$ being two divisible, but this point has height 4, so cannot be 2-divisible.

Minimal height basis. — $P, Q + 2Q^\sigma$

Lattice type. — $\langle 2 \rangle \oplus \langle 6 \rangle$

— $A = -3 \times \square$, $B = \square$: the points $P + 2P^\sigma, Q$ form a basis of the full Mordell–Weil lattice by the previous argument.

Minimal height basis. — $Q, P + 2P^\sigma$

Lattice type. — $\langle 2 \rangle \oplus \langle 6 \rangle$

— $A = -3 \times \square$, $B = -3 \times \square$: the points $P + 2P^\sigma$ and $Q + 2Q^\sigma$ form a lattice with the Gram matrix $\text{diag}(6, 6)$, which is both 2 and 3 saturated.

Minimal height basis. — $P + 2P^\sigma, Q + 2Q^\sigma$

Lattice type. — $\langle 6 \rangle \oplus \langle 6 \rangle$

4.3.3. When $r_{\mathcal{E}} = 3$

NNYY

$$[\mathbb{Q}(\sqrt{A}, \zeta_3) : \mathbb{Q}] = 2 \wedge [\mathbb{Q}(\sqrt{B}, \zeta_3) : \mathbb{Q}] = 2 \wedge 4AB = \eta^3 \wedge A = \eta^3$$

- $r_1 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_1^G$ basis: empty
- $r_2 = 1$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_2^G$ basis: Q or $Q + 2Q^\sigma$
- $r_3 = 1$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_3^G$ basis: $R + S$ or $R + S + 2(R + S)^\sigma$

- $r_4 = 1$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_4^G$ basis: $R - S$ or $R - S + 2(R - S)^\sigma$.

— $A = \square$, $B = \square$: the Gram matrix for the triple Q , $R - S$, $R + S$ is $\text{diag}(2, 4, 4)$ and the points form a finite index subgroup in $E_{A,B}(\mathbb{Q}(t))$. The points Q, R, S have the Gram matrix $2I_3$ for the identity matrix I_3 of dimension 3. Hence the lattice they span is 2-saturated.

Minimal height basis. — Q, R, S .

Lattice type. — $\langle 2 \rangle \oplus \langle 2 \rangle \oplus \langle 2 \rangle$

— $A = -3 \times \square$, $B = \square$: the triple Q , $R + S + 2(R + S)^\sigma$, $R - S$ forms a finite index subgroup in $E_{A,B}(\mathbb{Q}(t))$. The Gram matrix of the triple equals $\text{diag}(2, 12, 4)$. We consider a 2-saturation of this lattice. The new lattice has basis $e_1 = Q$, $e_2 = R + (R + S)^\sigma$, $e_3 = -(R - S)$ with the Gram matrix

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & -2 \\ 0 & -2 & 4 \end{pmatrix}$$

with determinant 24. Any non-zero point of the form $\sum_{i=1}^3 \alpha_i e_i$ for $\alpha_i \in \{0, 1\}$ has a height in the set $\{2, 4, 6, 12, 14\}$, hence no non-zero point of this form is further 2-divisible in this lattice.

Minimal height basis. — $Q, R + (R + S)^\sigma, -(R - S)$.

Lattice type. — $\langle 2 \rangle \oplus A_2(2)$.

— $A = \square$, $B = -3 \times \square$: points $Q + 2Q^\sigma$, $R + S$, $R - S + 2(R - S)^\sigma$ span a finite index sublattice in $E_{A,B}(\mathbb{Q}(t))$ with the Gram matrix $\text{diag}(6, 4, 12)$. We have a relation

$$-3V_{0,0,1} = Q + 2Q^\sigma + R - S + 2(R - S)^\sigma$$

and the points $Q + 2Q^\sigma$, $R + S$, $V_{0,0,1}$ span a lattice of discriminant 32. This lattice is generated by $e_1 = V_{0,0,1}$, $e_2 = Q + 2Q^\sigma + V_{0,0,1}$ and $e_3 = R + S$ with the Gram matrix $\text{diag}(2, 4, 4)$. Finally, we check that $e_2 + e_3 = 2W_{0,2,0,1}$ and $Q + 2Q^\sigma - W_{0,2,0,1} + V_{0,0,1} = W_{0,2,1,1}$ and the points $W_{0,2,1,1}$, $W_{0,2,0,1}$ and $V_{0,0,1}$ form a lattice with the Gram matrix $2I_3$ where I_3 is the 3-dimensional identity matrix. Further 2-divisibility is not possible.

Minimal height basis. — $W_{0,2,1,1}, W_{0,2,0,1}, V_{0,0,1}$

Lattice type. — $\langle 2 \rangle \oplus \langle 2 \rangle \oplus \langle 2 \rangle$

— $A = -3 \times \square$, $B = -3 \times \square$: the points $Q + 2Q^\sigma, R + S + 2(R + S)^\sigma, R - S + 2(R - S)^\sigma$ span a finite index sublattice with the Gram matrix $\text{diag}(6, 12, 12)$. We find the following linear relations:

$$Q + 2Q^\sigma + (R - S + 2(R - S)^\sigma) = -3V_{0,0,1}$$

and

$$Q + 2Q^\sigma + R + S + 2(R + S)^\sigma + V_{0,0,1} = 2(W_{0,2,0,1} + W_{2,1,0,1} + W_{2,1,1,0}).$$

We check that the Gram matrix of the basis $e_1 = Q + 2Q^\sigma, e_2 = W_{0,2,0,1} + W_{2,1,0,1} + W_{2,1,1,0}, e_3 = V_{0,0,1}$ equals

$$\begin{pmatrix} 6 & 2 & -2 \\ 2 & 4 & 0 \\ -2 & 0 & 2 \end{pmatrix}.$$

The matrix defined above has determinant 24 and we check that non-zero points of the form $\sum_{i=1}^3 \alpha_i e_i$ such that $\alpha_i \in \{0, 1\}$ have heights in the set $\{2, 4, 6, 12, 14\}$. There are no points of height 3 in $E_{A,B}(\overline{\mathbb{Q}}(t))$, hence it follows that the basis $\{e_1, e_2, e_3\}$ is 2-saturated and thus spans the group $E_{A,B}(\mathbb{Q}(t))$.

Let $e'_1 = e_3, e'_2 = e_1 + e_3, e'_3 = -e_2$. This basis has the Gram matrix

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & -2 \\ 0 & -2 & 4 \end{pmatrix}.$$

Minimal heights basis. — $V_{0,0,1}, Q + 2Q^\sigma + V_{0,0,1}, -(W_{0,2,0,1} + W_{2,1,0,1} + W_{2,1,1,0})$

Lattice type. — $\langle 2 \rangle \oplus A_2(2)$.

NNYNY

$$[\mathbb{Q}(\sqrt{A}, \zeta_3) : \mathbb{Q}] = 2 \wedge [\mathbb{Q}(\sqrt{B}, \zeta_3) : \mathbb{Q}] = 2 \wedge 4AB = \eta^3 \wedge A \neq \eta^3 \wedge B = \eta^3$$

- $r_1 = 1$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_1^G$ basis: P or $P + 2P^\sigma$
- $r_2 = 0$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_2^G$ basis: empty
- $r_3 = 1$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_3^G$ basis: $R + S$ or $R + S + 2(R + S)^\sigma$
- $r_4 = 1$, $E_{A,B}(\overline{\mathbb{Q}}(t)) \cap V_4^G$ basis: $R - S$ or $R - S + 2(R - S)^\sigma$.

— $A = \square, B = \square$: finite index subgroup spanned by: $P, R + S, R - S$

Minimal height basis. — P, R, S .

Lattice type. — $\langle 2 \rangle \oplus \langle 2 \rangle \oplus \langle 2 \rangle$

— $A = \square$, $B = -3 \times \square$: finite index subgroup spanned by: P , $R + S$, $R - S + 2(R - S)^\sigma$

Minimal height basis. — $P, R + S, -(R + (R - S)^\sigma)$

Lattice type. — $\langle 2 \rangle \oplus A_2(2)$.

— $A = -3 \times \square$, $B = \square$: finite index subgroup spanned by: $P + 2P^\sigma$, $R + S + 2(R + S)^\sigma$, $R - S$ with diagonal the Gram matrix $\text{diag}(6, 12, 4)$. After 2 and 3-saturation we obtain a basis $P + 2P^\sigma, X_{1,2,0,1}, R - S$ with the Gram matrix

$$\begin{pmatrix} 6 & 2 & 0 \\ 2 & 2 & -2 \\ 0 & -2 & 4 \end{pmatrix}$$

Equivalent basis (points of height 2 only): $e_1 = P + 2P^\sigma - 2X_{1,2,0,1} - (R - S)$, $e_2 = X_{1,2,0,1}$, $e_3 = X_{1,2,0,1} + R - S$ with the Gram matrix $\text{diag}(2, 2, 2)$. In fact $e_1 = U_{0,0,2}$ and $e_3 = X_{1,2,1,0}$.

Minimal height basis. — $U_{0,0,2}, X_{1,2,0,1}, X_{1,2,1,0}$

Lattice type. — $\langle 2 \rangle \oplus \langle 2 \rangle \oplus \langle 2 \rangle$

— $A = -3 \times \square$, $B = -3 \times \square$: finite index subgroup spanned by: $P + 2P^\sigma, R + S + 2(R + S)^\sigma, R - S + 2(R - S)^\sigma$ which has the Gram matrix $\text{diag}(6, 12, 12)$. Points $P + 2P^\sigma, R + 2R^\sigma$ and $S + 2S^\sigma$ form an overlattice of the previous one with the Gram matrix $\text{diag}(6, 6, 6)$. Next we observe that

$$-3U_{0,0,1} = P + 2P^\sigma + R + 2R^\sigma + S + 2S^\sigma.$$

So, we find the following basis for the Mordell–Weil subgroup over $\mathbb{Q}(t)$:

$$U_{0,0,1}, -U_{0,0,1} - (S + 2S^\sigma), 2U_{0,0,1} + (R + 2R^\sigma) + (S + 2S^\sigma)$$

with the Gram matrix

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 4 & -2 \\ 0 & -2 & 4 \end{pmatrix}.$$

Minimal height basis. — $U_{0,0,1}, -U_{0,0,1} - (S + 2S^\sigma), 2U_{0,0,1} + (R + 2R^\sigma) + (S + 2S^\sigma)$

Lattice type. — $\langle 2 \rangle \oplus A_2(2)$.

5. Density on $\mathcal{E}_{A,B}$ with generic rank 0

As we have seen in Section 2, there are many elliptic surfaces $\mathcal{E}_{A,B}$ with the generic fibre of the form $E_t : y^2 = x^3 + At^6 + B$ such that the generic rank is $r_{\mathcal{E}} = 0$: for those there exists $a, b, c \in \mathbb{Z}$ such that a, b are coprime and such that $A = 3a^2c$, $B = cb^2$ and we do NOT have one of the following:

- if c or $-3c$ (resp. $3c$ or $-c$) is a square and $12(abc)^2$ and $3a^2c$ (resp. $12(abc)^2$ and b^2c) are cubes (else the generic rank $r_{\mathcal{E}}$ is 2);
- if c or $-3c$ (resp. $3c$ or $-c$) is a square and either $4AB$ or A (resp. $4AB$ or B) are cubes (else $r_{\mathcal{E}}$ is 1).

In the cases where we moreover have $W(E_t) = +1$ on every fibre, then the parity conjecture implies that the rank of the fibres are all even - possibly zero. Using [4, Lemma A.1. and A.2.] and the corresponding tables of values, one can easily determine if a particular elliptic surface $\mathcal{E}_{3ca^2, cb^2}$ has this property. Listing all the cases where we have $r_{\mathcal{E}} = 0$ and $W(\mathcal{E}_t) = +1$ is a tedious task, and we decided to omit it in this paper. This section will focus on giving an example of an alternate proof of the Zariski-density of the rational points that does not involve the generic rank nor the root number.

The following example could already be found in [27], based on [26, Sections 5, 6, 7]: the generic rank is $r_{\mathcal{E}} = 0$ and the root number is constant and equal to $+1$:

Example 5.1. — The elliptic surface $\mathcal{E}_{6,27,6}$ given by the equation $E_t : y^2 = x^3 + 6(27t^6 + 1)$ has as well the property that $W(E_t) = +1$ for all $t \in \mathbb{P}^1(\mathbb{Q})$. It follows from Theorem 1.1 that there are no non-zero $\mathbb{Q}(t)$ -rational points in $E_{6,27,6}(\mathbb{Q}(t))$. In this case, our theorem is not sufficient to prove the Zariski density of the rational points on $\mathcal{E}_{6,27,6}$.

It is possible to prove it in a totally different way. Note that the construction of the multisection in [3] fails to work, because of the difficulty of finding a torsion point on the fibres of the surface. However, Rosa Winter and the first author [7] construct the following multisection.

On the surface $\mathcal{E}_{6,27,6}$ we find the following algebraic curve:

$$C : x^3 - \frac{131769}{2704}x^2t^2 + \frac{936903}{1352}xt^4 - \frac{1089}{1352}xt - \frac{6223513}{2704}t^6 + \frac{7743}{1352}t^3 + \frac{16215}{2704} = 0.$$

This is a singular curve of genus 1, with a double singularity at the point $[x_0, y_0, t_0] = [22, 104, 1]$. The desingularisation \tilde{C} of the curve C has a non-singular point $[\frac{12793}{2704}, -\frac{2327053}{140608}, 1]$, thus \tilde{C} is an elliptic curve. We observe

that C is a multisection (passing through each fibre exactly 3 times), and that \tilde{C} has rank 3 (infinitely many rational points), and moreover that $\mathcal{E}_{6-27,6}$ is the blow-up of a del Pezzo surface of degree 1 (no torsion section). So we can apply [19, Theorem 6.4] to conclude the Zariski density of the rational points on $\mathcal{E}_{6-27,6}$.

BIBLIOGRAPHY

- [1] D. J. BERNSTEIN, “Detecting perfect powers in essentially linear time”, *Math. Comput.* **67** (1998), no. 223, p. 1253-1283.
- [2] N. BOURBAKI, *Lie groups and Lie algebras. Chapters 4–6*, Elements of Mathematics, Springer, 2002, translated from the 1968 French original by Andrew Pressley, xii+300 pages.
- [3] J. BULTHUIS, “Rational points on del Pezzo surfaces of degree one”, Msc thesis, Leiden University, 2018.
- [4] J. DESJARDINS, “On the density of rational points on rational elliptic surfaces”, *Acta Arith.* **189** (2019), no. 2, p. 109-146.
- [5] ———, “On the variation of the root number in families of elliptic curves”, *J. Lond. Math. Soc.* **99** (2019), no. 2, p. 295-331.
- [6] J. DESJARDINS & B. NASKRĘCKI, “Verification code in MAGMA of the calculations in the paper Geometry of the del Pezzo surface $y^2 = x^3 + Am^6 + Bn^6$ ”, <https://zenodo.org/records/10659434>, 2019.
- [7] J. DESJARDINS & R. WINTER, “Density of rational points on a family of del Pezzo surfaces of degree one (with an appendix by Jean-Louis Colliot-Thélène)”, *Adv. Math.* **405** (2022), article no. 108489 (20 pages).
- [8] T. DOKCHITSER & V. DOKCHITSER, “Root numbers and parity of ranks of elliptic curves”, *J. Reine Angew. Math.* **658** (2011), p. 39-64.
- [9] I. V. DOLGACHEV, *Classical algebraic geometry. A modern view*, Cambridge University Press, 2012, xii+639 pages.
- [10] H. A. HELFGOTT, “On the behavior of the root numbers in families of elliptic curves”, <https://arxiv.org/abs/math/0408141>, 2003.
- [11] V. A. ISKOVSKIĖ, “Minimal models of rational surfaces over arbitrary fields”, *Izv. Akad. Nauk SSSR, Ser. Mat.* **43** (1979), no. 1, p. 19-43, 237.
- [12] E. JABARA, “Rational points on some elliptic surfaces”, *Acta Arith.* **153** (2012), no. 1, p. 93-108.
- [13] J. KOLLÁR, *Rational curves on algebraic varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge, vol. 32, Springer, 1996, viii+320 pages.
- [14] J. KOLLÁR & M. MELLA, “Quadratic families of elliptic curves and unirationality of degree 1 conic bundles”, *Am. J. Math.* **139** (2017), no. 4, p. 915-936.
- [15] E. MANDUCHI, “Root numbers of fibers of elliptic surfaces”, *Compos. Math.* **99** (1995), no. 1, p. 33-58.
- [16] Y. I. MANIN, *Cubic forms: algebra, geometry, arithmetic*, North-Holland Mathematical Library, vol. 4, North-Holland; Elsevier, 1974, translated from the Russian by M. Hazewinkel, vii+292 pages.
- [17] R. MIRANDA, *The basic theory of elliptic surfaces*, Dottorato di Ricerca in Matematica, ETS Editrice, 1989, vi+108 pages.
- [18] K. OGUIISO & T. SHIODA, “The Mordell–Weil lattice of a rational elliptic surface”, *Comment. Math. Univ. St. Pauli* **40** (1991), no. 1, p. 83-99.

- [19] C. SALGADO & R. VAN LUIJK, “Density of rational points on del Pezzo surfaces of degree one”, *Adv. Math.* **261** (2014), p. 154-199.
- [20] C. SALGADO, D. TESTA & A. VÁRILLY-ALVARADO, “On the unirationality of del Pezzo surfaces of degree 2”, *J. Lond. Math. Soc.* **90** (2014), no. 1, p. 121-139.
- [21] T. SHIODA, “On the Mordell–Weil lattices”, *Comment. Math. Univ. St. Pauli* **39** (1990), no. 2, p. 211-240.
- [22] J. H. SILVERMAN, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer, 1994, xiv+525 pages.
- [23] J. TATE, “Algorithm for determining the type of a singular fiber in an elliptic pencil”, in *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Mathematics, vol. 476, 1975, p. 33-52.
- [24] M. ULAS, “Rational points on certain elliptic surfaces”, *Acta Arith.* **129** (2007), no. 2, p. 167-185.
- [25] ———, “Rational points on certain del Pezzo surfaces of degree one”, *Glasg. Math. J.* **50** (2008), no. 3, p. 557-564.
- [26] A. VÁRILLY-ALVARADO, “Weak approximation on del Pezzo surfaces of degree 1”, *Adv. Math.* **219** (2008), no. 6, p. 2123-2145.
- [27] ———, “Density of rational points on isotrivial rational elliptic surfaces”, *Algebra Number Theory* **5** (2011), no. 5, p. 659-690.

Manuscrit reçu le 25 novembre 2019,
révisé le 15 décembre 2021,
accepté le 15 mai 2023.

Julie DESJARDINS
Mathematical and Computational Sciences
University of Toronto Mississauga
Deerfield Hall
Mississauga, ON L5L 3E2 (Canada)
julie.desjardins@utoronto.ca

Bartosz NASKREŃCKI
Faculty of Mathematics and Computer Science
Adam Mickiewicz University in Poznań
ul. Uniwersytetu Poznańskiego 4
61-614, Poznań (Poland)
Mathematical Institute
Polish Academy of Sciences
ul. Śniadeckich 8
00-656, Warszawa (Poland)
bartosz.naskrecki@amu.edu.pl