DISTRIBUTION OF MORDELL–WEIL RANKS OF FAMILIES OF ELLIPTIC CURVES

BARTOSZ NASKRĘCKI

ABSTRACT. We discuss the distribution of Mordell–Weil ranks of the family of elliptic curves $y^2=(x+\alpha f^2)(x+\beta g^2)(x+\gamma h^2)$ where f,g,h are coprime polynomials that parametrize the projective smooth conic $a^2+b^2=c^2$ and α,β,γ are elements from $\overline{\mathbb{Q}}$. In our previous papers we discussed certain special cases of this problem and in this article we complete the picture by proving the general results.

1. INTRODUCTION

In our previous papers [11], [14] and thesis [12] we have studied in several aspects the following family of curves

$$y^2=x(x-f^2)(x-g^2) \tag{1}$$

where f,g are two elements from certain field. We considered the case where f,g are rational functions in one variable and satisfy the extra relation $f^2+g^2=h^2$ where h is also a rational function. The most general results were obtained in the case when $f,g,h\in\overline{\mathbb{Q}}[t]$ under the assumption that the polynomials are pairwise coprime. By a simple change of variables we can put this equation into a more symmetric form

$$y^2=(x+f^2)(x+g^2)(x+h^2)$$

Now we can either forget the relation $f^2+g^2=h^2$, but then the connection with previous equation is lost or we can generalize it in another direction. In this article we consider a general family of the form

$$y^2=(x+\alpha f^2)(x+\beta g^2)(x+\gamma h^2). \tag{2}$$

This curve contains an obvious point $(0,fgh)$ of infinite order and we would like to discuss how the rank of the Mordell-Weil group of curve (2) varies with α,β,γ.

We can offer the most complete description in the situation when

$$\max\{\deg f,\deg g,\deg h\}=2. \tag{3}$$

We will show that in such cases what we obtain is a Weierstrass model of a generic fiber of a K3 surface defined over some number field. We are interested in the computation of the Mordell–Weil group of the generic fiber over the rational function field with suitable coefficients. This will be related to the computation of the Néron-Severi group of the associated elliptic surface.

The main result of this paper will be proved in Sections 3 and 4.

Key words and phrases. elliptic curve, Mordell-Weil rank, elliptic surface.

Main Theorem 1.1. *Let* $(\alpha,\beta,\gamma)\in\overline{\mathbb{Q}}^3$ *be such that* $\alpha\beta\gamma\neq 0$. *Assume that* f,g,h *are coprime polynomials in* $\overline{\mathbb{Q}}[t]$ *that satisfy conditions* $f^2+g^2=h^2$ *and* (3). *Then the curve* (2) *is smooth and is an elliptic curve. The Mordell-Weil rank of elliptic curve* (2) *over* $\overline{\mathbb{Q}}(t)$ *varies between* 2 *and* 6 *and each case is explicitly described in Sections 3 and 4.*

After short preliminaries in Section 2 we analyse the rank variation in family 2 in Section 3. Then we focus on the special case of the family with constants $\alpha=\beta=\gamma=1$ in Section 4 that was previously discussed in [11], [12], [14]. We develop a certain mechanism that allows us to easily switch between triples f,g,h that parametrize a conic $a^2+b^2=c^2$. In fact, we prefer to perform certain computations in the most convenient way, by choosing the *standard* triple $f=t^2-1, g=2t, h=t^2+1$. Such a choice is arbitrary, and we can switch to any other such triple of polynomials. This implies in particular that geometrically the elliptic surface that corresponds to the curve (2) and the one that corresponds to the choice of standard polynomials is isomorphic (not as fibred surface). So we can analyse simply the family

$$E_{(\alpha,\beta,\gamma)}:\ y^2=(x+\alpha(t^2-1)^2)(x+\beta\cdot 4t^2)(x+\gamma(t^2+1)^2). \tag{4}$$

In paper [14] we have analyzed mostly the case $\alpha=\beta=\gamma=1$ with full description of the geometric Mordell-Weil group and certain results over number fields. We have also studied certain base changes of the family induced by a map $\phi:\mathbb{P}^1\to\mathbb{P}^1$, $\phi: t\mapsto\phi(t)$. Further we concentrate on the reduction modulo a prime of the model $\alpha=\beta=\gamma=1$ and develop the properties of the supersingular K3 surfaces that occur at certain primes.

The curves in family (2) appeared in [3] and were studied from another perspective in [13]. They might also have applications in the study of dynamics on supersingular K3 surfaces but this will be analysed elsewhere, cf. [5], [20].

2. Preliminaries

We formulate in this section the necessary definitions and theorems that will be used throughout the article. The reader can consult also [21], [22], [25].

Definition 2.1. Let k be an algebraically closed field. Let C be a smooth projective curve over k and S be a smooth projective surface over k. We call a triple (S,C,π) an elliptic surface when $\pi:S\to C$ is a surjective morphism such that

- there exists a non-empty set $B\subset C(k)$ such that for any $v\in C(k)\setminus B$ the fibre $\pi^{-1}(v)$ is a curve of genus 1,
- there exists a section $O:C\to S$ of the morphism π,
- no fibre $\pi^{-1}(v)$ for $v\in C(k)$ contains (-1)-curves.

To any elliptic curve over $F(t)$ we can attach the corresponding elliptic surface fibred over $\mathbb{P}^1_F$. We call it a Kodaira-Néron model of E over $F(t)$.

For an elliptic curve E over $K=\overline{\mathbb{Q}}(t)$ we denote by $\langle\cdot,\cdot\rangle_E$ the height pairing attached to E as in [21]. The group $E(K)/E(K)_{\text{tors}}$ with the induced pairing $\langle\cdot,\cdot\rangle_E$ is a positive definite lattice, cf. [21, Theorem 7.4]. To simplify the notation, we write $\langle\cdot,\cdot\rangle$ if the curve E is fixed. Explicitly, for two given points $P,Q\in E(K)$ their intersection pairing is given by

$$\langle P,Q\rangle=\chi(S)+\overline{P}.\overline{O}+\overline{Q}.\overline{O}-\overline{P}.\overline{Q}-\sum_{v\in B}c_v(P,Q). \tag{5}$$

For a point P in $E(K)$ we denote by $\overline{P}$ the curve which lies in S and is the image of a section determined by the point P, cf. [21, Lemma 5.2]. The curve $\overline{O}$ is the image of the zero section $O : \mathbb{P}^1_{\overline{\mathbb{Q}}} \to S$. In the case $P = Q$ the formula simplifies to

$$\langle P, P\rangle = 2\chi(S) + 2\overline{P}.\overline{O} - \sum_{v\in B} c_v(P, P). \tag{6}$$

The rational numbers $c_v(P, Q)$ depend only on the fibre type above $v \in B$ of bad reduction and on the indices of the components that intersect curves $\overline{P}$ and $\overline{Q}$, cf. [21, Theorem 8.6]. We usually denote $c_v(P, P)$ by $c_v(P)$. We denote by $\langle P, P\rangle$ the *height of point P*.

For an elliptic surface (S, C, π) we denote by $\mathrm{NS}(S)$ the Néron-Severi group of the surface S. It follows from [21, Cor. 3.2] that it is a finitely generated and torsion free abelian group. We denote its rank by $\rho(S)$ and call it the *Picard number*. Moreover, we can induce on $\mathrm{NS}(S)$ a structure of a lattice by using the intersection product of divisors. Let B denote the set of closed points v in C such that $\pi^{-1}(v)$ is singular. We denote by m_v the number of components of $\pi^{-1}(v)$. We denote by E the generic fiber of π treated as an elliptic curve over $k(C)$. The Mordell-Weil rank of the generic fiber $E(k(C))$ and the rank $\rho(S)$ are related by the so-called Shioda-Tate formula

Theorem 2.2 ([21, Cor. 5.3])**.** *Let (S, C, π) be an elliptic surface with generic fiber E. The following equality holds*

$$\rho(S) = 2 + \sum_{v\in B}(m_v - 1) + \operatorname{rank} E(k(C)). \tag{7}$$

It is standard to give upper bounds for Picard numbers in terms of the Euler characteristic $\chi(S) = \chi(S, \mathcal{O}_S)$ and the genus $g(C)$ of curve C. In characteristic zero they follow from Lefschetz (1,1)-classes theorem [8, Prop. 3.3.2].

$$\rho(S) \le 10\chi(S) + 2g(C). \tag{8}$$

In positive characteristic we have a weaker bound

$$\rho(S) \le 12\chi(S) - 2 + 4g(C). \tag{9}$$

The numbers $\chi(S)$ of elliptic surface S can be used to identify the type of algebraic surface represented by S. An elliptic surface S is a rational surface if and only if $\chi(S) = 1$, it is a K3 surface when $\chi(S) = 2$ and is of Kodaira dimension when $\chi(S) \ge 3$. We can compute the numbers $\chi(S)$ in terms of explicit numbers $e(F_v)$ which depend on the reduction types of bad fibers $\pi^{-1}(v)$.

Theorem 2.3 ([15, Thm. 1])**.** *Let (S, C, π) be an elliptic surface over the field k of characteristic* $\mathrm{char}(k) \neq 2, 3$*. The following equality holds*

$$12\chi(S) = \sum_{v\in B} e(F_v)$$

where the number $e(F_v)$ depend on the Kodaira type of fiber $\pi^{-1}(v)$ as follows

In general the bounds (8), (9) are not sharp and we need the approach that requires the use of ℓ-adic cohomology and good reduction to positive characteristic. The main ideas come from [6, Ex. 20.3.6]. The details of this approach are explained in [25, §6] and [9, §4]. We say that our elliptic surface (S, C, π) has a model over $\operatorname{Spec} A$ where A is a discrete valuation ring in some number field K, with maximal

Typ F_v	$I_n(n\geq 1)$	II	III	IV	$I_n^*(n\geq 0)$	II^*	III^*	IV^*
$e(F_v)$	n	2	3	4	$n+6$	10	9	8

Table 1. Euler numbers $e(F_v)$.

ideal $\mathfrak{p}$ with residue field $\mathbb{F}_q = A/\mathfrak{p}$ of characteristic p. We assume that S has *good reduction* modulo p which means that we have a smooth morphism $S \to \operatorname{Spec} A$. For any prime $\ell \neq p$ there are natural injective homomorphisms

$$\mathrm{NS}(S_{\overline{\mathbb{Q}}}) \otimes \mathbb{Q}_\ell \hookrightarrow \mathrm{NS}(S_{\overline{\mathbb{F}}_q}) \otimes \mathbb{Q}_\ell \hookrightarrow H^2_{\text{ét}}(S_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell(1)). \tag{10}$$

On the ℓ-adic cohomology group $H^2_{\text{ét}}(S_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell(1))$ there is an action of Frobenius automorphism Φ. Its characteristic polynomial $P(x) = \det(Ix - \Phi)$ has the property that it is defined over $\mathbb{Z}$ and all its roots are complex algebraic numbers of norm q. We denote the multiplicity of root α by $\lambda(\alpha, \Phi)$. We denote by R_Φ the sum of multiplicities $\lambda(\zeta q, \Phi)$ where ζ is some root of unity.

Corollary 2.4 ([25, Cor. 2.3])**.** *For the elliptic surface (S, C, π) with good reduction at p we have the inequalities*

$$\rho(S_{\overline{\mathbb{Q}}}) \leq \rho(S_{\overline{\mathbb{F}}_q}) \leq R_\Phi. \tag{11}$$

In practical terms we deal with the case where the base curve C is the projective line $\mathbb{P}^1$. The ℓ-adic cohomology group $H^2_{\text{ét}}(S_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell(1))$ is of dimension $12\chi(S_{\overline{\mathbb{F}}_q}) - 2$ in this case and the Frobenius automorphism acts on the Néron-Severi group in an explicit way. The action on the part coming from the components of bad fibers only permutes the components in each fiber. On the part that comes from sections (which are induced by points on the generic fiber) the Frobenius action can be determined by the $x \mapsto x^q$ Frobenius action on the coefficients of points on the generic fiber. To compute the characteristic polynomial of Φ we have to apply the Grothendieck-Lefschetz formula and count the points over finite fields, cf. [11]. When the image of specialization map of Néron-Severi groups

$$\mathrm{sp}_{\mathfrak{p}} : \mathrm{NS}(S_{\overline{\mathbb{Q}}}) \to \mathrm{NS}(S_{\overline{\mathbb{F}}_q})$$

is of finite index by the properties of lattices we have that the discriminant $\Delta(\mathrm{NS}(S_{\overline{\mathbb{Q}}}))$ equals $[\mathrm{NS}(S_{\overline{\mathbb{F}}_q}) : \mathrm{sp}_{\mathfrak{p}}(\mathrm{NS}(S_{\overline{\mathbb{Q}}}))]^2 \Delta(\mathrm{NS}(S_{\overline{\mathbb{F}}_q}))$. The discriminant $\Delta(\mathrm{NS}(S_{\overline{\mathbb{F}}_q})$ can be computed if we assume the Artin-Tate conjecture. This is unconditional in the case when S is a K3 surface, cf. [10, Thm. 6.1], [1, Thm. 5.2], [11, Thm. 5.2]. We will use it only in the form of the following corollary.

Corollary 2.5. *Let $(S, \mathbb{P}^1, \pi)$ be a K3 elliptic surface with good reduction at prime p. We assume that the Néron-Severi group is defined over $\mathbb{F}_q$. Then*

$$q^{\rho(S_{\mathbb{F}_q})-21} \cdot \frac{\lim\limits_{x\to q} P(x)}{(x-q)^{\rho(S_{\mathbb{F}_q})}} \equiv -\Delta(\mathrm{NS}(S_{\mathbb{F}_q}))\ (mod\ (\mathbb{Q}^\times)^2). \tag{12}$$

All over the paper we work with Weierstrass models of elliptic curves over $\overline{\mathbb{Q}}(t)$. We say that such a model is minimal at $t - a$ for $a \in \overline{\mathbb{Q}}$ if it is minimal in the usual sense, cf.[23, Chap. VII.1]. We say also that it is *minimal at infinity* or at $t = \infty$ if the change of coordinates $t \mapsto 1/s$ and $(x, y) \mapsto (xs^{2n}, ys^{3n})$ for some choice of n

provide us with a Weierstrass model which is minimal at $s = 0$ in the usual sense. If a model is minimal at every place we say it is globally minimal. In general we can check if a prime p is a prime of good reduction for an elliptic surface over $\mathbb{P}^1$ by analysing its globally minimal Weierstrass model. It is particularly simple for curves defined over $\mathbb{Q}(t)$. We denote by $\mathrm{rad}(h)$ the square free part of polynomial h.

Lemma 2.6 ([12, Tw. 2.2.12])**.** *Let E be an elliptic curve defined over $\mathbb{Q}(t)$ with globally minimal Weierstrass model*

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

where $a_i \in \mathbb{Z}[t]$. Let $\Delta \in \mathbb{Z}[t]$ be its discriminant and $j = f/g \in \mathbb{Q}(t)$ its j-invariant where f, g are coprime polynomials in $\mathbb{Z}[t]$. Let p be a prime number greater than 5 such that $p \nmid \mathrm{disc}(h)$ for every polynomial h in the list $\{\mathrm{rad}(a_i) : i = 1, 2, 3, 4, 6\} \cup \{\mathrm{rad}(f), \mathrm{rad}(g), \mathrm{rad}(\Delta)\}$. We denote by $\tilde{E}$ the reduction modulo p of the equation of E. If $\tilde{E}$ defines an elliptic curve over $\mathbb{F}_p(t)$ and the model is globally minimal and the reductions $\tilde{h}$ of polynomials $h \in \{\mathrm{rad}(f), \mathrm{rad}(g), \mathrm{rad}(\Delta)\}$ are separable, than the elliptic surface $\mathcal{E}$ with generic fiber E has good reduction at p.

3. General families with moderate ranks

In this section we consider the variation of the Mordell-Weil rank in family (4) for different choices of (α, β, γ). Our main tool in this section is the Shioda-Tate formula and theorems on good reduction of Néron-Severi groups. Theorem 4.2 and a similar reasoning to Corollary 4.4 allow us to reduce the computations on (2) to a fixed triple of coprime polynomials that establish a rational parametrization of the conic $a^2 + b^2 = c^2$. We choose the parametrizing polynomials $f = t^2 - 1$, $g = 4t^2$ and $h = t^2 + 1$. We work over the field $\overline{\mathbb{Q}}(t)$ and a change of coordinates between two Weierstrass models (4) for two different pairs (α, β, γ) and $(\alpha', \beta', \gamma')$ determines an equivalence relation between pairs: $(\alpha, \beta, \gamma) \sim (\alpha', \beta', \gamma')$ if and only if there exists an element $\lambda \in \overline{\mathbb{Q}}^{\times}$ such that $(\alpha, \beta, \gamma) = (\lambda\alpha', \lambda\beta', \lambda\gamma')$. This is equivalent to saying that the triples (α, β, γ), $(\alpha', \beta', \gamma')$ determine the same point in $\mathbb{P}^2(\overline{\mathbb{Q}})$. We can restrict to the affine part $\mathbb{A}^2(\overline{\mathbb{Q}})$ where $\gamma \neq 0$ because the curve (4) becomes singular when $\alpha\beta\gamma = 0$. This proves the following statement.

Proposition 3.1. *Let $(\alpha, \beta, \gamma) \in \{(x, y, z) : xyz \neq 0\} \subset \mathbb{P}^2(\overline{\mathbb{Q}})$ be a closed point. The curve $E_{(\alpha,\beta,\gamma)}$ is smooth and is isomorphic to $E_{(\alpha/\gamma,\beta/\gamma,1)}$. We also have the group isomorphism*

$$E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t)) \cong E_{(\alpha/\gamma,\beta/\gamma,1)}(\overline{\mathbb{Q}}(t))$$

The discriminant of the Weierstrass equation (4) is defined by

$$\Delta_{(\alpha,\beta,\gamma)} = \Delta(E_{(\alpha,\beta,\gamma)})(t) = 16 \cdot \Delta_1^2 \cdot \Delta_2^2 \cdot \Delta_3^2 \tag{13}$$

where

$$\Delta_1 = \alpha - 2\alpha t^2 - 4\beta t^2 + \alpha t^4$$
$$\Delta_2 = \alpha - \gamma - 2\alpha t^2 - 2\gamma t^2 + \alpha t^4 - \gamma t^4$$
$$\Delta_3 = \gamma - 4\beta t^2 + 2\gamma t^2 + \gamma t^4$$

The j-invariant of the family is equal to

$$j_{(\alpha,\beta,\gamma)} = j(E_{(\alpha,\beta,\gamma)})(t) = \frac{j_{\mathrm{num}}}{\Delta_1^2 \cdot \Delta_2^2 \cdot \Delta_3^2} \tag{14}$$

where

$$\begin{aligned} j_{\text{num}} = 2^8 \Big(& 16\beta^2 t^4 - 4\beta\gamma \left(t^3+t\right)^2 + \alpha^2 \left(t^2-1\right)^4 - \\ & -\alpha \left(t^2-1\right)^2 \left(4\beta t^2 + \gamma \left(t^2+1\right)^2\right) + \gamma^2 \left(t^2+1\right)^4 \Big)^3 \end{aligned}$$

We observe that $\Delta_{(\alpha,\beta,\gamma)}(t)$ is a square of certain polynomial $\delta(t)$ in $\overline{\mathbb{Q}}[t]$. This polynomial $\delta(t)$ is separable in $\overline{\mathbb{Q}}[t]$ if and only if

$$\alpha\beta\gamma(\alpha+\beta)(\alpha-\gamma)(\beta-\gamma)(\alpha\beta-\alpha\gamma-\beta\gamma) \neq 0 \tag{15}$$

Proposition 3.2. *Under the assumption* (15) *the curve $E_{(\alpha,\beta,\gamma)}$ is a globally minimal Weierstrass model of an elliptic curve. Its associated elliptic surface is an elliptic K3 surface and has bad fibers of type I_2 for t such that $\Delta_{(\alpha,\beta,\gamma)}(t) = 0$. It is smooth for $t = \infty$.*

Proof. We deduce that equation (4) is minimal at every finite place and has good reduction at infinity ([23, VII, Remark 1.1]). The reduction types are I_2 for $t \neq \infty$ and such that $\Delta_{(\alpha,\beta,\gamma)}(t) = 0$. Let S be the elliptic surface for which $E_{(\alpha,\beta,\gamma)}$ is the generic fiber. By the results of Oguiso [15, Theorem 1] and Shioda [21, Theorem 2.8] the Euler characteristic $\chi(S) = \chi(S, \mathcal{O}_S)$ is equal to 2. This implies that our surface S is a K3 surface. □

If the condition (15) is violated, then our curve $E_{(\alpha,\beta,\gamma)}$ will be either singular (only for $\alpha\beta\gamma = 0$) or will have a different configuration of singular fibers of the associated elliptic surface. The Zariski closed set

$$V((\alpha+\beta)(\alpha-\gamma)(\beta-\gamma)(\alpha\beta-\alpha\gamma-\beta\gamma)) \subset \mathbb{P}^2$$

is the sum of irreducible components

$$\begin{aligned} V_{1,1,0} &= V(\alpha+\beta) \\ V_{1,0,-1} &= V(\alpha-\gamma) \\ V_{0,1,-1} &= V(\beta-\gamma) \\ V_q &= V(\alpha\beta-\alpha\gamma-\beta\gamma) \end{aligned}$$

Let us denote by U the open set $\mathbb{P}^2 \setminus V(\alpha\beta\gamma)$. We say that a triple $(\alpha,\beta,\gamma) \in U$ is *generic* if (α,β,γ) does not belong to any of the closed sets $V_{1,1,0}, V_{1,0,-1}, V_{0,1,-1}, V_q$. The set of such triples is again Zariski open. We denote it by $\mathcal{U}_{\text{gen}}$.

3.1. **Generic triple (α,β,γ).**

In the generic case an elliptic surface $\mathcal{E}_{(\alpha,\beta,\gamma)}$ attached to $E_{(\alpha,\beta,\gamma)}$ will be a K3 surface hence its Picard rank satisfies the inequality $\rho(\mathcal{E}_{(\alpha,\beta,\gamma)}) \leq 20$. Application of Shioda-Tate formula shows that the rank of $E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t))$ is at most 6 in this case. Let us consider 6 points on this curve. To simplify the notation assume for now that $A = (t^2-1)^2$, $B = 4t^2$ and $q(\alpha,\beta,\gamma) =$

$\alpha\beta-\alpha\gamma-\beta\gamma$.

$$\begin{aligned}
P_1:\ x(P_1)=0,\quad & y^2(P_1)=\alpha\beta\gamma AB(A+B)\\
P_2:\ x(P_2)=-\alpha A+(q(\alpha,\beta,\gamma)/\gamma)B,\quad & y^2(P_2)=\frac{\alpha B(\gamma-\alpha)q(\alpha,\beta,\gamma)(A\gamma-\beta B+B\gamma)^2}{\gamma^3}\\
P_3:\ x(P_3)=\beta\gamma/(-\beta+\gamma)A,\quad & y^2(P_3)=\frac{A\beta\gamma q(\alpha,\beta,\gamma)(A\gamma-\beta B+B\gamma)^2}{(\beta-\gamma)^3}\\
P_4:\ x(P_4)=-(\alpha\beta)/(\alpha+\beta)(A+B),\quad & y^2(P_4)=\frac{\alpha\beta(A+B)q(\alpha,\beta,\gamma)(\alpha A-\beta B)^2}{(\alpha+\beta)^3}\\
P_5:\ x(P_5)=-\alpha(A+B),\quad & y^2(P_5)=-\alpha B(\alpha-\gamma)(A+B)(\alpha A+\alpha B-\beta B)\\
P_6:\ x(P_6)=\beta A,\quad & y^2(P_6)=A\beta(\alpha+\beta)(A+B)(A\beta+A\gamma+B\gamma)
\end{aligned}$$

Without further assumptions the points P_1,P_2,P_3 and P_4 all belong to $E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t))$. Point P_5 with such a choice of x-coordinate exists if and only if $\alpha=\beta$. The point P_6 is well-defined on $E_{(\alpha,\beta,\gamma)}$ only when $\beta=-\gamma$. We denote by $\mathcal{G}$ the set of generic triples (α,β,γ) such that $\alpha\neq\beta$ and $\beta\neq-\gamma$.

Lemma 3.3. *Let $(\alpha,\beta,\gamma)\in\mathcal{G}$ be a generic triple. The set $\{P_1,P_2,P_3,P_4\}$ spans a rank 4 subgroup of $E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t))$. Their height pairing matrix $(\langle P_i,P_j\rangle)_{1\leq i,j\leq 4}$ looks as follows*

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

Proof. We denote by S the Kodaira-Néron model of $E_{(\alpha,\beta,\gamma)}$. It has bad fibers over points $t_0\in\overline{\mathbb{Q}}$ such that $(\alpha A-\beta B)(t_0)=0$ or $(\alpha A-\gamma(A+B))(t_0)=0$ or $(\beta B-\gamma(A+B))(t_0)=0$. All bad fibers are of type I_2 and the image $\overline{P_i}$ of the section $P_i:\mathbb{P}^1\to S$ over the point t_0 lies in the component which does not intersect the component of the zero section $O:\mathbb{P}^1\to S$ if and only if $y^2(P_i)(t_0)=0$ and the first coordinate reduces to the first coordinate of the appropriate two-torsion point which happens to be singular at that fiber. The height pairing is symmetric so we have to compute only the values $\langle P_i,P_j\rangle$ for $i\leq j$.

From the equation of $E_{(\alpha,\beta,\gamma)}$ it follows that $\pi:S\to\mathbb{P}^1$ is a K3 surface, hence $\chi(S)=2$. Moreover, we check that for $i=1,2,3,4$ we have $\overline{P_i}.\overline{O}=0$. This is easy to see for all $t\neq\infty$. For $t=\infty$ we make a change of coordinates $t=1/s$ and $(x,y)\mapsto(xs^4,ys^6)$ and look at the fiber at $s=0$. Now observe that the correcting terms $c_v(P_1)$ for P_1 are all zero, hence $\langle P_1,P_1\rangle=4$. For $\langle P_1,P_2\rangle$ we have that $c_v(P_1,P_2)=0$ for all points v and we check that $\overline{P_1}.\overline{P_2}=2$. This is true because we have a system of equations

$$\begin{aligned} x(P_1) &= x(P_2)\\ y^2(P_1) &= y^2(P_2)\end{aligned}\tag{16}$$

and the number of its solutions equals the intersection number $(\overline{P_1}+\overline{-P_1}).(\overline{P_2}+\overline{-P_2})$. The elements t_0 that satisfy the system (16) are the one that satisfy

$$(-\alpha\beta B+\alpha\gamma A+\alpha\gamma B+\beta\gamma B)(t_0)=0.$$

Defining polynomial is separable for $(\alpha,\beta,\gamma)\in\mathcal{G}$ and we can easily check that $\pi^{-1}(t_0)$ is never a singular fiber. For $t_0=\infty$ by a change of coordinates we easily check that there is no solution for $s = 0$. Hence

$$(\overline{P_1} + \overline{-P_1}).(\overline{P_2} + \overline{-P_2}) = 4$$

The involution $\iota : P \mapsto -P$ on the generic fiber $E_{(\alpha,\beta,\gamma)}$ extends to an isomorphism on S and it preserves the intersection numbers. The divisor $\overline{P_2} + \overline{-P_2}$ is invariant under ι and $\iota(\overline{P_1}) = \overline{-P_1}$. This implies that

$$\overline{P_1}.(\overline{P_2} + \overline{-P_2}) = 2.$$

Now we observe that $\overline{P_1}$ cannot intersect both $\overline{P_2}$ and $\overline{-P_2}$ for our choice of t_0. Without loss of generality we can choose square roots in such a way that $\overline{P_1}.\overline{P_2} = 2$. This implies that $\langle P_1, P_2\rangle = 0$.

A similar computation shows that $\langle P_1, P_3\rangle = 0$. In this case what we have to use is the fact that A is not separable and both solutions $t = \pm 1$ count twice. The same way we obtain $\langle P_1, P_4\rangle = 0$.

We claim that $\langle P_2, P_2\rangle = 2$. This is easily checked because for t_0 such that $(\gamma(A + B) - \beta B)(t_0) = 0$ the point $P_2(t_0)$ is singular on the fiber above t_0 and in the blow-up it is moved to the other component of the I_2 fiber above t_0, so the correcting terms for $v = t_0$ are $c_v(P_2) = 1/2$. Polynomial $(\gamma(A + B) - \beta B)(t)$ is separable, hence the claim follows by height formula (6).

Now we prove that $\langle P_2, P_3\rangle = 0$. The common intersection would appear for t_0 such that $(\gamma(A + B) - \beta B)(t_0)$, hence in the fibers of bad reduction. This implies already that $c_v(P_2, P_3) = 1/2$ for $v = t_0$. To prove that $\overline{P_2}.\overline{P_3} = 0$ is equivalent to proving that $\overline{P_2 - P_3}.\overline{O} = 0$. To check this we use the addition formula and $x(P_2 + P_3)$ is a degree 4 polynomial in t with nonzero free coefficient

$$-\frac{\alpha\gamma^2}{-\alpha\beta + \alpha\gamma + \beta\gamma},$$

hence the divisor $\overline{P_2 - P_3}$ never intersects the divisor $\overline{O}$ at any place.

We claim that $\langle P_2, P_4\rangle = 0$. The solutions of the system $x(P_2) = x(P_4),\ y^2(P_2) = y^2(P_4)$ in t lead to t_0 that satisfy $(\alpha^2 A\gamma + \alpha^2\beta(-B) + \alpha^2 B\gamma - \alpha\beta^2 B + \alpha\beta B\gamma + \beta^2 B\gamma)(t_0) = 0$. These points t_0 do not coincide with the places of bad reduction because of the assumptions on (α, β, γ), hence $\overline{P_2}.\overline{P_4} = 2$. Now the correcting terms $c_v(P_2, P_4)$ are always zero because the points never meet the same component at the fibers of bad reduction. This proves the claim.

To prove $\langle P_3, P_3\rangle = 2$ we proceed as in the case of point P_2. Next we show that $\langle P_3, P_4\rangle = 0$. The solutions t_0 to the system $x(P_3) = x(P_4),\ y^2(P_1) = y^2(P_2)$ satisfy $(\alpha A\beta - 2\alpha A\gamma - A\beta\gamma + \alpha\beta B - \alpha B\gamma)(t_0) = 0$ and again they never meet the points for which we have bad reduction, hence $\overline{P_2}.\overline{P_4} = 2$ and the correcting terms $c_v(P_3, P_4)$ are zero for all v.

Now to finish the proof we show that $\langle P_4, P_4\rangle = 2$ but this is proved the same way as for P_2 and P_3. We conlude by saying that the height pairing matrix of points P_i, $i = 1, 2, 3, 4$ has nonzero determinant, so the points are linearly independent. □

Proposition 3.4. *There exists a triple $(\alpha, \beta, \gamma) \in \mathcal{G}$ such that*

$$\textit{rank } E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t)) = 4.$$

Proof. We put $\alpha = 3, \beta = 5$ and $\gamma = 1$. We have to show that $\rho(\mathcal{E}_{(\alpha,\beta,\gamma)}) \leq 18$. The elliptic surface $\mathcal{E}_{(3,5,1)}$ associated with $E_{(3,5,1)}$ has good reduction at $p = 1009$ by Lemma 2.6 and the Néron-Severi group is defined over $\mathbb{F}_p$. We compute the characteristic polynomial of Frobenius automorphism Φ for any prime $\ell \neq p$. It follows that

$$P(x) = (x-1009)^{18}(x^4 + 412x^3 - 801146x^2 + 419449372x + 1009^4).$$

The last factor is irreducible over $\mathbb{Z}[t]$ and is not a cyclotomic polynomial, hence $R_\Phi = 18$. Corollary 2.4 implies that $\rho(\mathcal{E}_{(3,5,1)}) \leq 18$. Now application of Shioda-Tate formula finishes the proof. □

Lemma 3.5. *Let $(\alpha,\beta,\gamma) \in \mathcal{U}_{gen}$ be a generic triple such that $\beta = -\gamma$ and $\alpha \neq \beta$. The set $\{P_1, P_2, P_3, P_4, P_6\}$ spans a rank 5 subgroup of $E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t))$. Its height pairing matrix looks as follows*

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

Proof. By Lemma 3.3 we already know that the points P_1, P_2, P_3 and P_4 span a rank 4 subgroup of the full Mordell-Weil group. We have to compute now the intersections $\langle P_i, P_6\rangle$ for $i = 1,2,3,4$ and $\langle P_6, P_6\rangle$.

To show that $\langle P_6, P_6\rangle = 4$ we check that $\overline{P_6}.\overline{O} = 0$ and that $c_v(P_6) = 0$ for all v. Now observe that $\langle P_i, P_6\rangle = 2 - \overline{P_i}.\overline{P_6}$ for $i = 1,2,3,4$. We will prove that $\overline{P_i}.\overline{P_6} = 2$. This is equivalent to prove that the system $x(P_i) = x(P_6)$, $y^2(P_i) = y^2(P_6)$ has exactly four solutions (some of them possibly multiple). For $i = 1,3$ the solutions come from the equation $A(t) = 0$. For $i = 2$, we obtain the solutions from $(\alpha A - A\gamma + 2\alpha B - B\gamma)(t) = 0$. For $i = 4$ we get $(-2\alpha A + A\gamma - \alpha B)(t) = 0$. □

Proposition 3.6. *There exists a triple $(\alpha,\beta,\gamma) \in \mathcal{U}_{gen}$ such that $\beta = -\gamma$ and $\alpha \neq \beta$ and*

$$\textit{rank}\ E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t)) = 5.$$

Proof. We put $\alpha = 3, \beta = -1$ and $\gamma = 1$. We check that the surface $S = \mathcal{E}_{(3,-1,1)}$ has good reduction at primes $p = 241, 409$ with the full Néron-Severi group of $S_{\overline{\mathbb{F}}_p}$ defined over $\mathbb{F}_p$. We compute the characteristic polynomials P_p of Φ_p for a fixed $\ell \neq p$

$$P_{241}(x) = (x-241)^{20}(x^2 + 478x + 241^2)$$
$$P_{409}(x) = (x-409)^{20}(x^2 - 626x + 409^2)$$

Now by Corollary 2.5 we obtain

$$\Delta(\mathrm{NS}(S_{\overline{\mathbb{F}}_{241}})) \equiv -3 \cdot 5 \bmod (\mathbb{Q}^\times)^2,$$
$$\Delta(\mathrm{NS}(S_{\overline{\mathbb{F}}_{409}})) \equiv -3 \bmod (\mathbb{Q}^\times)^2.$$

Suppose that the rank $E_{(-3,-1,1)}(\overline{\mathbb{Q}}(t))$ would be equal to 6. Then by Shioda-Tate formula this will imply that $N = \rho(S_{\overline{\mathbb{Q}}}) = 20$. The image $\mathrm{sp}_p(N)$ would be a finite index subgroup in the codomain. So this will imply that the discriminants $\Delta(\mathrm{NS}(S_{\overline{\mathbb{F}}_{409}}))$ and $\Delta(\mathrm{NS}(S_{\overline{\mathbb{F}}_{241}}))$ should be equal modulo squares. But they are not, hence a contradiction. This implies that $\rho(N) \leq 19$ and by Shioda-Tate formula again we obtain the statement of the proposition. □

Lemma 3.7. *Let $(\alpha,\beta,\gamma)\in\mathcal{U}_{gen}$ be a generic triple such that $\alpha=\beta$ and $\beta\neq-\gamma$. The set $\{P_1,P_2,P_3,P_4,P_5\}$ spans a rank 5 subgroup of $E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t))$. Their height pairing matrix looks as follows*

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

Proof. The proof is similar to the proof of Lemma 3.5. □

Proposition 3.8. *There exists a triple $(\alpha,\beta,\gamma)\in\mathcal{U}_{gen}$ such that $\alpha=\beta$ and $\beta\neq-\gamma$ and*

$$\textit{rank}\ E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t))=5.$$

Proof. We put $\alpha=3,\beta=3$ and $\gamma=1$ and consider $S=\mathcal{E}_{(3,3,1)}$. We check that S has good reduction at primes $p=73,97$. Like in the proof of Proposition 3.6 we compute the discriminant of the reduction of Néron-Severi groups. The characteristic polynomials of Frobenius are as follows

$$P_{73}(x)=(x-73)^{20}(x^2+142x+73^2)$$
$$P_{97}(x)=(x-97)^{20}(x^2-2x+97^2)$$

We obtain $\Delta(\mathrm{NS}(S_{\overline{\mathbb{F}}_{73}}))\equiv-2 \pmod{(\mathbb{Q}^\times)^2}$ and $\Delta(\mathrm{NS}(S_{\overline{\mathbb{F}}_{97}}))\equiv-3 \pmod{(\mathbb{Q}^\times)^2}$. This leads to the conclusion that $\rho(S)\leq 19$ which implies the statement of the proposition. □

3.2. **Type** $(\alpha,\beta,\gamma)=(-1,-1,1)$**.** Now we consider a very special generic triple (α,β,γ). It satisfies two extra conditions $\alpha=\beta$ and $\beta=-\gamma$. By the projective equivalence of tuples we can state the results for $\alpha=\beta=-\gamma=-1$. The Kodaira types of singular fibers that appear in this case are:

(17)

point	fiber type
$t^2+2t-1=0$	I_2
$t^4+1=0$	I_2
$t^2-2t-1=0$	I_2
$t^4+6t^2+1=0$	I_2

There are six linearly independent points on the curve:

$$R_1=(0,fgh)$$
$$R_2=(h^2,\sqrt{2}fgh)$$
$$R_3=(1/2h^2,\sqrt{-6}(h^2-2g^2)h)$$
$$R_4=(-f^2,\sqrt{2}fgh)$$
$$R_5=(-1/2g^2,\sqrt{6}g(2h^2-g^2))$$
$$R_6=(-1/2f^2,\sqrt{6}f(2h^2-f^2))$$

With respect to the height pairing $\langle\cdot,\cdot\rangle$ the determinant of Gram matrix equals 384

$$\begin{pmatrix} 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & -2 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & -2 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix} \tag{18}$$

By the Shioda-Tate formula this proves that we have found sufficiently many independent points to obtain at least a finite index subgroup in the full Mordell-Weil group. In fact we can easily determine the full Mordell-Weil group using a full descent computation like in [11, Lemma 6.2]. We denote by T_1 and T_2 the generators of the torsion subgroup. By the fibers configuration it is easy to prove (cf. [22, Cor. 7.5]) that the full torsion subgroup is isomorphic to $\mathbb{Z}/2\oplus\mathbb{Z}/2$. We put $T_1=(4t^2,0)$ and $T_2=(-t^4-2t^2-1,0)$. We consider 6 points Q_1,Q_2,Q_3,Q_4,Q_5,Q_6 with coefficients in the field $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{-3})(t)$ defined as follows

$$2Q_1 = R_1-R_2-R_4-R_5+R_6-T_2, \tag{19}$$
$$2Q_2 = R_1-R_2-R_5+R_6-T_2, \tag{20}$$
$$2Q_3 = R_1-R_4-R_5+R_6-T_2, \tag{21}$$
$$2Q_4 = R_1-R_2+R_3-R_4-R_5+T_1-T_2, \tag{22}$$
$$2Q_5 = R_1-R_2-R_3-R_4-R_5+T_1-T_2, \tag{23}$$
$$2Q_6 = R_1-R_2+R_3-R_4+R_6+T_1. \tag{24}$$

The height pairing matrix for the points Q_i has the form

$$\begin{pmatrix} 3 & 5/2 & 5/2 & 5/2 & 5/2 & 5/2 \\ 5/2 & 3 & 3/2 & 2 & 2 & 2 \\ 5/2 & 3/2 & 3 & 2 & 2 & 2 \\ 5/2 & 2 & 2 & 3 & 2 & 5/2 \\ 5/2 & 2 & 2 & 2 & 3 & 3/2 \\ 5/2 & 2 & 2 & 5/2 & 3/2 & 3 \end{pmatrix} \tag{25}$$

and determinant equal to 3/8. Now we follow the approach in proof of [11, Lemma 6.2] and prove that the points Q_i and torsion generators T_1 and T_2 span the whole Mordell-Weil group over $\overline{\mathbb{Q}}(t)$. We omit tedious computations which can be easily done by a computer package. This allows us to deduce that the discriminant of the Néron-Severi group in this case will be $-2^5\cdot 3$. This can be used to deduce the supersingular primes p that allow in positive characteristic to get rank 8 over $\mathbb{F}_{p^2}$, cf. Section 5.

The number field $F=\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{-3})$ is normal and its Galois group is isomorphic to $(\mathbb{Z}/2)^3$. Generators τ_1,τ_2,τ_3 are determined easily

$$\begin{aligned} \tau_1(\sqrt{2})&=\sqrt{2}, & \tau_1(\sqrt{3})&=\sqrt{3}, & \tau_1(\sqrt{-3})&=-\sqrt{-3} \\ \tau_2(\sqrt{2})&=-\sqrt{2}, & \tau_2(\sqrt{3})&=-\sqrt{3}, & \tau_2(\sqrt{-3})&=\sqrt{-3} \\ \tau_3(\sqrt{2})&=-\sqrt{2}, & \tau_3(\sqrt{3})&=\sqrt{3}, & \tau_3(\sqrt{-3})&=-\sqrt{-3} \end{aligned}$$

Group $\mathrm{Gal}(F/\mathbb{Q})$ acts naturally on the group $G=E_{(-1,-1,1)}(\overline{\mathbb{Q}}(t))=E_{(-1,-1,1)}(F(t))$ (cf. [12, Wn. 2.5.18]) and we obtain a Galois action on the free module G/G_{tors}

which determines a representation

$$\rho : \mathrm{Gal}(F/\mathbb{Q}) \to \mathrm{GL}_6(\mathbb{Z}).$$

We represent the matrices in the basis $\{Q_i + G_{\mathrm{tors}}\}$ of G/G_{tors}

$$\rho(\tau_1) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\rho(\tau_2) = \begin{pmatrix} -3 & -2 & -2 & -4 & -4 & -4 \\ 2 & 1 & 2 & 2 & 2 & 2 \\ 2 & 2 & 1 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\rho(\tau_3) = \begin{pmatrix} -7 & -6 & -6 & -6 & -6 & -6 \\ 2 & 1 & 2 & 2 & 2 & 2 \\ 2 & 2 & 1 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & -1 & 1 \\ 2 & 2 & 2 & 1 & 2 & 1 \\ 2 & 2 & 2 & 2 & 2 & 1 \end{pmatrix}$$

The tuples $v \in \mathbb{Z}^6$ such that $\rho(\sigma)v = v$ for all $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ represent the points P in $E_{(-1,-1,1)}(F(t))$ such that $\sigma(P) - P \in E[2](F(t))$ for all σ. We easily find that the submodule $\{v : \rho(\tau_1\tau_3)v = v\}$ is one-dimensional and is generated by the vector $(3, -1, -1, 0, -1, -1)^T$. This combination represents a point $Q = 3Q_1 - Q_2 - Q_3 - Q_5 - Q_6$ which satisfies $\tau_i(Q) = Q + T_2$ for $i = 1, 2, 3$. This implies that the free part of $E_{(-1,-1,1)}(\mathbb{Q}(t))$ is spanned by $2Q = P_1$, hence

$$E_{(-1,-1,1)}(\mathbb{Q}(t)) \cong \mathbb{Z} \oplus \mathbb{Z}/2 \oplus \mathbb{Z}/2.$$

3.3. **Triples** $(\alpha, \beta, \gamma) \in U$ **with** $\alpha = \gamma$**.** Let us denote the set of triples $(\alpha, \beta, \gamma) \in U$ with $\alpha = \gamma$ and $\alpha \neq -\beta$ and $\beta \neq \gamma$ by $\mathcal{S}_1$. In this situation the equation $E_{(\alpha,\beta,\gamma)}$ defines an elliptic curve which is a generic fiber of elliptic surface $\mathcal{E}_{(\alpha,\beta,\gamma)}$ with bad fibers of types I_2 and I_4. The discriminant of the Weierstrass equation of $E_{(\alpha,\beta,\gamma)}$ has the form

$$256\alpha^2 t^4 \left(\alpha + \alpha t^4 - 2\alpha t^2 - 4\beta t^2\right)^2 \left(\alpha + \alpha t^4 + 2\alpha t^2 - 4\beta t^2\right)^2$$

For $t = 0$ and $t = \infty$ we have the I_4 fibers and for t that are roots of

$$\left(\alpha + \alpha t^4 - 2\alpha t^2 - 4\beta t^2\right)\left(\alpha + \alpha t^4 + 2\alpha t^2 - 4\beta t^2\right) = 0$$

we have I_2 fibers. Shioda-Tate formula implies that we have the bound

$$\operatorname{rank} E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t)) \leq 4.$$

Lemma 3.9. *Let $(\alpha, \beta, \gamma) \in \mathcal{S}_1$. The set of points $\{P_1, P_3, P_4\}$ spans a rank 3 subgroup of $E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t))$. Their height pairing matrix looks as follows*

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

Proof. We observe first that the points P_1, P_3 and P_4 are the only well-defined point from the list in §3.1 that are not two-torsion. Essentially we reprove part of Lemma 3.3 with the extra assumption $\alpha = \gamma$. Observe that the assumption does not change the fiber types of bad reduction crucial for our computation. □

Proposition 3.10. *There exists a triple $(\alpha, \beta, \gamma) \in \mathcal{S}_1$ and*

$$\textit{rank}\ E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t)) = 3.$$

Proof. We put $\alpha = 1$, $\beta = 4$ and $\gamma = 1$ and we consider $S = \mathcal{E}_{(1,4,1)}$. The surface S has good reduction at primes $p = 61$ and $p = 181$ with its Néron-Severi group defined already over $\mathbb{F}_p$. The characteristic polynomials of Frobenius are as follows

$$P_{61}(x) = (x-61)^{20}(x^2+118x+61^2)$$
$$P_{181}(x) = (x-181)^{20}(x^2+166x+181^2)$$

We obtain $\Delta(\mathrm{NS}(S_{\overline{\mathbb{F}}_{61}})) \equiv -3{\cdot}5 \pmod{(\mathbb{Q}^\times)^2}$ and $\Delta(\mathrm{NS}(S_{\overline{\mathbb{F}}_{97}})) \equiv -3{\cdot}11 \pmod{(\mathbb{Q}^\times)^2}$. This leads to the conclusion that $\rho(S) \leq 19$ which implies the statement of the proposition. □

3.4. **Triples** $(\alpha, \beta, \gamma) \in U$ **with** $\alpha = -\beta$**.** Let us denote the set of triples $(\alpha, \beta, \gamma) \in U$ with $\alpha = -\beta$ and $\alpha \neq \gamma$ and $\beta \neq \gamma$ by $\mathcal{S}_2$. In this situation the equation $E_{(\alpha,\beta,\gamma)}$ defines an elliptic curve which is a generic fiber of elliptic surface $\mathcal{E}_{(\alpha,\beta,\gamma)}$ with bad fibers of types I_2 and I_4. The discriminant of the Weierstrass equation of E has the form

$$16\alpha^2\left(t^2+1\right)^4\left(\alpha-\gamma+\alpha t^4-\gamma t^4-2\alpha t^2-2\gamma t^2\right)^2\left(\gamma+\gamma t^4+4\alpha t^2+2\gamma t^2\right)^2$$

For each root of t^2+1 we have an I_4 fiber and for t that are roots of the remaining factors of the discriminant we have I_2 fibers. Shioda-Tate formula implies that we have the bound

$$\operatorname{rank} E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t)) \leq 4.$$

Lemma 3.11. *Let $(\alpha, \beta, \gamma) \in \mathcal{S}_2$. The set of points $\{P_1, P_2, P_3\}$ spans a rank 3 subgroup of $E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t))$. Their height pairing matrix looks as follows*

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

Proof. We mimic the proof of Lemma 3.9. □

Proposition 3.12. *There exists a triple $(\alpha, \beta, \gamma) \in \mathcal{S}_2$ and*

$$\textit{rank}\ E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t)) = 3.$$

Proof. We put $\alpha = 5$, $\beta = -5$ and $\gamma = 1$ and we consider $S = \mathcal{E}_{(5,-5,1)}$. The surface S has good reduction at primes $p = 29$ and $p = 101$ with its Néron-Severi group defined already over $\mathbb{F}_p$. The characteristic polynomials of Frobenius are as follows

$$P_{29}(x) = (x-29)^{20}(x^2+54x+29^2)$$
$$P_{101}(x) = (x-101)^{20}(x^2-122x+101^2)$$

We obtain $\Delta(\mathrm{NS}(S_{\overline{\mathbb{F}}_{29}})) \equiv -7 \pmod{(\mathbb{Q}^{\times})^2}$ and $\Delta(\mathrm{NS}(S_{\overline{\mathbb{F}}_{97}})) \equiv -5 \pmod{(\mathbb{Q}^{\times})^2}$. This leads to the conclusion that $\rho(S) \leq 19$ which implies the statement of the proposition. □

3.5. **Case $\beta = \gamma$.** In this section let us denote the set of triples $(\alpha, \beta, \gamma) \in U$ with $\beta = \gamma$ and $\alpha \neq \gamma$ and $\alpha \neq -\beta$ by $\mathcal{S}_3$. In this situation the equation $E_{(\alpha,\beta,\gamma)}$ defines an elliptic curve which is a generic fiber of elliptic surface $\mathcal{E}_{(\alpha,\beta,\gamma)}$ with bad fibers of types I_2 and I_4. The discriminant of the Weierstrass equation of E has the form

$$16\beta^2(t-1)^4(t+1)^4\left(\alpha+\alpha t^4-2\alpha t^2-4\beta t^2\right)^2\left(\alpha-\beta+\alpha t^4-\beta t^4-2\alpha t^2-2\beta t^2\right)^2$$

For $t = 1$ and $t = -1$ we have an I_4 fiber and for t that are roots of the remaining factors of the discriminant we have I_2 fibers. Shioda-Tate formula implies that we have the bound

$$\operatorname{rank} E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t)) \leq 4.$$

Lemma 3.13. *Let $(\alpha, \beta, \gamma) \in \mathcal{S}_3$. The set of points $\{P_1, P_2, P_4\}$ spans a rank 3 subgroup of $E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t))$. Their height pairing matrix looks as follows*

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

Proof. We mimic the proof of Lemma 3.9. □

Proposition 3.14. *There exists a triple $(\alpha, \beta, \gamma) \in \mathcal{S}_3$ and*

$$\textit{rank } E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t)) = 3.$$

Proof. We put $\alpha = 5$, $\beta = 1$ and $\gamma = 1$ and we consider $S = \mathcal{E}_{(5,1,1)}$. The surface S has good reduction at primes $p = 29$ and $p = 101$ with its Néron-Severi group defined already over $\mathbb{F}_p$. The characteristic polynomials of Frobenius are as follows

$$\begin{aligned} P_{29}(x) &= (x-29)^{20}(x^2+22x+29^2) \\ P_{101}(x) &= (x-101)^{20}(x^2+106x+101^2) \end{aligned}$$

We obtain $\Delta(\mathrm{NS}(S_{\overline{\mathbb{F}}_{29}})) \equiv -5 \pmod{(\mathbb{Q}^{\times})^2}$ and $\Delta(\mathrm{NS}(S_{\overline{\mathbb{F}}_{97}})) \equiv -23 \pmod{(\mathbb{Q}^{\times})^2}$. This leads to the conclusion that $\rho(S) \leq 19$ which implies the statement of the proposition. □

3.6. **Further degeneration.** In this paragraph we list the remaining two special cases which are determined by triples (α, β, γ) in the intersections of $U \cap V_{1,0,-1} \cap V_{1,1,0}$ and $U \cap V_{0,1,-1} \cap V_{1,1,0}$.

Type $(1, -1, -1)$. The Kodaira types of singular fibers that appear in this case are:

(26)

point	fiber type
$t^4+1=0$	I_2
$t=1$	I_4
$t^2+1=0$	I_4
$t=-1$	I_4

We can easily find two linearly independent points:

$$\begin{aligned} P_1 &= (0, fgh) \\ P_2 &= (-f^2 + g^2, \sqrt{2}f^2 g) \end{aligned}$$

with height pairing matrix

$$\begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix} \tag{27}$$

and they span a rank 2 subgroup which is of finite index in the full Mordell-Weil group.

Type $(1, -1, 1)$.The Kodaira types of singular fibers that appear in this case are:

(28)

point	fiber type
$t = \infty$	I_4
$t = 0$	I_4
$t^2 + 1 = 0$	I_4
$t^4 + 6t^2 + 1 = 0$	I_2

We find two points:

$$\begin{aligned} P_1 &= (0, \sqrt{-1}fgh) \\ P_3 &= (-1/2f^2, 1/(2\sqrt{-2})f(g^2 + h^2)) \end{aligned}$$

with height pairing matrix

$$\begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix} \tag{29}$$

The points P_1 and P_3 are linearly independent.

3.7. **Case** $\alpha\beta - \alpha\gamma - \beta\gamma = 0$**.** The equation $\alpha\beta - \alpha\gamma - \beta\gamma = 0$ is homogeneous and we can parametrize it as a quadric in $\mathbb{P}^2$. We consider the triples $(\alpha, \beta, \gamma) \in U$ that are parametrized by $r \neq 0$ as follows

$$\alpha = r(r-1), \beta = r, \gamma = r - 1. \tag{30}$$

The curve $E_{(\alpha,\beta,\gamma)}$ in this case has the Weierstrass equation

$$y^2 = (x + r(r-1)(t^2-1)^2)(x + r(4t^2))(x + (r-1)(t^2+1)^2) \tag{31}$$

with discriminant $\Delta = 16r^2(r-1)^2\delta^6$, where $\delta = -1 + r - 2t^2 - 2rt^2 - t^4 + rt^4$. It can be easily transformed into another form

$$(-1)\delta(y')^2 = x'(x'-1)(x'-r)$$

where $x + r(4t^2) = x'(-1)\delta$ and $y = y'\delta^2$. The curve $(y')^2 = x'(x'-1)(x'-r)$ determines a constant fibration so every fiber is of type I_0 and the twist by $-\delta$ introduces four I_0^* fibers over the points t_0 such that $\delta(t_0) = 0$. The curve (31) is hence a globally minimal Weierstrass model. Application of Shioda-Tate formula allows us to compute the bound $\operatorname{rank} E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t)) \leq 2$.

We observe that the equation $-\delta = s^2$ with respect to variables t and s defines a quartic model of elliptic curve $(y')^2 = x'(x'-1)(x'-r)$. This means that the isotrivial elliptic surface attached to (31) is a Kummer fibration $\mathcal{E}$ related to two elliptic curves $E_1 : -\delta = s^2$ and $E_2 : (y')^2 = x'(x'-1)(x'-r)$. They are isomorphic over $\overline{\mathbb{Q}}$ and by [22, §12.6] it follows that $\rho(\mathcal{E}) = 18 + \operatorname{rank} Hom(E_1, E_2)$. This implies

K	R_K	ω	$j(E)$
$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Z}[\sqrt{-1}]$	$1+\sqrt{-1}$	1728
$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Z}[\sqrt{-2}]$	$\sqrt{-2}$	8000
$\mathbb{Q}(\sqrt{-7})$	$\mathbb{Z}[\sqrt{-7}]$	$\frac{1+\sqrt{-7}}{2}$	-3375

FIGURE 1. Three elliptic curves E with j-invariant $j(E)$ and endomorphism ring isomorphic to R_K

that we have precisely rank 2 if E_1 has complex multiplication, and otherwise rank 1. We have the usual point of infinite order in any case on the curve (31).

$$P_1 = (0, 2(r-1)rt\left(t^4-1\right))$$

The other linearly independent point in the CM case can be obtained as follows. We consider a quadratic twist of E_2 by $-\delta$. We denote this curve by $E_2^{(-\delta)}$. Let σ denote the automorphism of the field $\overline{\mathbb{Q}}(t)(\sqrt{-\delta})$ determined by $\sigma(\sqrt{-\delta}) = -\sqrt{-\delta}$. There is a natural isomorphism ϕ between the group of points $\tilde{H} = \{P : E_2(\overline{\mathbb{Q}}(t)(\sqrt{-\delta})) : \sigma(P) = -P\}$ and the group $E_2^{(-\delta)}(\overline{\mathbb{Q}}(t))$. For a point $P \in \tilde{H}$ we have $P = (\alpha, \beta\sqrt{-\delta})$ for $\alpha, \beta \in \overline{\mathbb{Q}}(t)$. Then $\phi(P) = (\alpha(-\delta), \beta(-\delta)^2)$. Since E_1 and E_2 are isomorphic, we assume for now that $E_1 = E_2$ to simplify the notation. Since E_2 is a CM curve, then $\mathrm{End}(E_2)$ is isomorphic to an order R_K in some quadratic imaginary extension K of $\mathbb{Q}$. We pick an element ω of R_K that is not in $\mathbb{Z}$. It induces an endomorphism $[\omega] \in \mathrm{End}(E_2)$. On the curve E_2 our point P_1 from (31) induces a point

$$P_1' = \left(\frac{4rt^2}{-\delta}, \frac{2r(r-1)t(t^2-1)(1+t^2)}{\delta\sqrt{-\delta}}\right).$$

It maps via ϕ to $P_1^{(-\delta)}$ on $E_2^{(-\delta)}$. We observe that for any point $Q \in E_2(\overline{\mathbb{Q}}(t)(\sqrt{-\delta}))$ the endomorphism $[\omega]$ is equivariant with respect to σ: $[\omega](\sigma(Q)) = \sigma([\omega](Q))$. In particular $[\omega](\sigma(P_1')) = \sigma([\omega](P_1'))$ and this implies $[\omega](P_1') \in \tilde{H}$, and via ϕ it corresponds to a point in $E_2^{(-\delta)}(\overline{\mathbb{Q}}(t))$ which we denote by abuse of notation by $[\omega](P_1^{(-\delta)})$. The points $P_1^{(-\delta)}$ and $[\omega](P_1^{(-\delta)})$ cannot be linearly dependent because of the choice of $[\omega]$, so they span a rank two subgroup in $E_2^{(-\delta)}(\overline{\mathbb{Q}}(t))$. We denote for now the curve E_2 by E_r. We have proved the following lemma.

Lemma 3.15. *Let $(\alpha, \beta, \gamma) \in U$ be such that $\alpha\beta - \alpha\gamma - \beta\gamma = 0$. Choose parameter r like in* (30). *Then the following holds*

$$\operatorname{rank} E_{(\alpha,\beta,\gamma)}(\overline{\mathbb{Q}}(t)) = \begin{cases} 1 & \textit{if } E_r \textit{ does not have complex multiplication,} \\ 2 & \textit{otherwise.} \end{cases}$$

Example 3.16. In several simple cases of complex multiplication on E_2 we can actually compute explicitly the point $[\omega](P_1^{(-\delta)})$ for some particular choice of ω. We freely adopt the results of [24, II, Prop. 2.3.1]

For a fixed parameter r we choose an isomorphism between E_r and curve E from Figure 2. This induces via the chain of morphisms $E_r \xrightarrow{\text{iso}} E \xrightarrow{[\omega]} E \xrightarrow{\text{iso}^{-1}} E_r$ the endomorphism $[\omega]$ on E_r. We skip the simple but tedious algebraic manipulations and offer the final results

- $E : y^2 = x^3 + x, \quad j = 1728, \quad \omega = 1 + \sqrt{-1}$
$$[\omega](x,y) = \big(\omega^{-2}(x + 1/x), \omega^{-3}y(1 - 1/x^2)\big)$$
- $E : y^2 = x^3 + 4x^2 + 2x, \quad j = 8000, \quad \omega = \sqrt{-2}$
$$[\omega](x,y) = (\omega^{-2}(x + 4 + 2/x), \omega^{-3}y(1 - 2/x^2))$$
- $E : y^2 = x^3 - 35x + 98, \quad j = -3375, \quad \omega = (1 + \sqrt{-7})/2$
$$[\omega](x,y) = (\alpha^{-2}(x - 7(1-\omega)^4/(x + \omega^2 - 2)), \omega^{-3}y(1 + 7(1-\omega)^4)/(x + \omega^2 - 2)^2)$$

Figure 2. Certain endomorphisms of degree 2 in End(E)

- $f = 2$, $j = 1728$, $\eta = \sqrt{8\sqrt{-1}}$
$$P_2^{(-\delta)} = \left(\frac{(1 - (2 - 4\sqrt{-1})t^2 + t^4)^2}{(1+t^2)^2(1 - 6t^2 + t^4)}, \frac{\eta t(-1 + 5t^2 - 26t^4 + 26t^6 - 5t^8 + t^{10})}{(1+t^2)^3(1 - 6t^2 + t^4)^2}\right)$$
Height pairing matrix of $(P_1^{(-\delta)}, P_2^{(-\delta)})$
$$\begin{pmatrix} 4 & 4 \\ 4 & 8 \end{pmatrix}$$
- $f = 3 + 2\sqrt{2}$, $j = 8000$, $\eta = \sqrt{-3 - 2\sqrt{2}}$
$$P_2^{(-\delta)} = \left(\frac{(\sqrt{2} + 2)\left(t^4 - 1\right)^2}{4t^2\left(\sqrt{2}t^4 + \sqrt{2} - 4t^2\right)}, \frac{\eta\left(4\sqrt{2}t^{10} - 4\sqrt{2}t^2 - t^{12} - 5t^8 + 5t^4 + 1\right)}{8\sqrt{2}t^3\left(-2\sqrt{2}t^2 + t^4 + 1\right)^2}\right)$$
Height pairing matrix of $(P_1^{(-\delta)}, P_2^{(-\delta)})$
$$\begin{pmatrix} 4 & 0 \\ 0 & 8 \end{pmatrix}$$
- $f = 1/2(1 + 3\sqrt{-7})$, $j = -3375$
$$x(P_2^{(-\delta)}) = \frac{(3\sqrt{-7} - 1)\left((-\sqrt{-7} - 3)t^2 + 4t^4 + 4\right)^2}{64t^2\left((3 - \sqrt{-7})t^4 - 3(1 - \sqrt{-7})t^2 - \sqrt{-7} + 3\right)}$$
$$y(P_2^{(-\delta)}) = \frac{(\sqrt{-7} + 1)\left(t^4 - 1\right)\left(3(\sqrt{-7} - 5)t^6 + 3(\sqrt{-7} - 5)t^2 + 4t^8 + 24t^4 + 4\right)}{t^3\left(3(\sqrt{-7} - 5)t^2 + 8t^4 + 8\right)^2}$$
Height pairing matrix of $(P_1^{(-\delta)}, P_2^{(-\delta)})$
$$\begin{pmatrix} 4 & 2 \\ 2 & 8 \end{pmatrix}$$

4. Case $\alpha = \beta = \gamma = 1$

The remaining case of triple $(\alpha, \beta, \gamma) = (1, 1, 1)$ was studied extensively in [12] and [14]. In this section we offer an alternative proof of [14, Lem. 5.8]. We apply theorems from [18] to avoid elaborate height computations performed in [14]. Moreover, the techniques applied in this section justify our previous restriction of family (2) to the case where $(f, g, h) = (t^2 - 1, 2t, t^2 + 1)$. We conclude in this section that over $\overline{\mathbb{Q}}(t)$ the classification of the curves with parameters (α, β, γ) do not essentially depend on the choice of fixed parametrizing triple.

Let K be a field of characteristic 0 and assume that

$$E : y^2 = x^3 + Ax^2 + Bx$$

is a Weierstrass model of an elliptic curve such that $A, B \in K$. Let $\sigma : K \to K$ be an automorphism of field K. The curve

$$E^\sigma : y^2 = x^3 + \sigma(A)x^2 + \sigma(B)x$$

is a Weierstrass model of another elliptic curve over K. The map

$$\begin{gathered} E(K) \to E^\sigma(K) \\ (x, y) \mapsto (\sigma(x), \sigma(y)) \\ O \mapsto O \end{gathered} \tag{32}$$

establishes an isomorphism of the Mordell-Weil groups $E(K)$ and $E^\sigma(K)$.

Now we will recall certain results about rational curves and their parameterizations from [18, Chap. 4]. Let F be any algebraically closed field of characteristic zero. The function $f(t) \in F(t)$ is in *reduced form* when the numerator and denominator of f are coprime.

Definition 4.1. Let $f \in F(t)$ be a rational function in reduced form. If f is non-zero, the degree of f is the maximum of the degrees of the numerator and denominator of f. When f is zero, we define its degree to be -1. We denote the degree of f by $\deg(f)$.

Rational functions of degree 1 are called *linear*. When f is linear, it is of the form $f(t) = (at + b)/(ct + d)$, where $ad - bc \neq 0$ and $a, b, c, d \in F$. We write shortly $f(t) = \gamma t$ where γ is the corresponding matrix

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(F).$$

By a theorem of Clebsch, every irreducible curve of genus 0 has a parametrization, cf. [18, Chap. 4.1]. In particular, every smooth conic $C : \alpha a^2 + \beta b^2 = \gamma c^2$ has a parametrization. Let $F_C(x, y) = 0$ be the affine equation of C. We always assume that F_C is an irreducible and nonconstant polynomial in $F[x, y]$. The parametrization is a non-constant rational map

$$\mathcal{P} : t \mapsto (\chi_1(t), \chi_2(t))$$

such that $F_C(\chi_1(t), \chi_2(t)) = 0$. We define the degree of a parametrization $\mathcal{P}$ as follows

$$\deg \mathcal{P} = \max\{\deg \chi_1, \deg \chi_2\}.$$

We say that a parametrization $\mathcal{P}$ of curve C is *proper*, when the rational map $\mathcal{P}$ is birational. Two parametrizations of the same curve C are related to each other.

Theorem 4.2 ([18, Chap. 4, Lemma 4.17])**.** *Let P be any affine parametrization of the rational curve C. Let $\mathcal{P}'$ be any other parametrization of C.*

- *There exists a nonconstant rational function $f \in F(t)$ such that $\mathcal{P}'(t) = \mathcal{P}(f(t))$.*
- *Parametrization $\mathcal{P}'$ is proper if and only if there exists a linear function $f \in F(t)$ such that $\mathcal{P}'(t) = \mathcal{P}(f(t))$.*

Now it is important for us to establish a relation between the degree of the defining polynomial $F_C(x, y)$ of our rational curve and the degree of any proper parametrization $\mathcal{P}$.

Theorem 4.3. *Let C be an affine rational curve defined over F with defining polynomial $F_C(x, y) \in F[x, y]$ and let $\mathcal{P} = (\chi_1, \chi_2)$ be a parametrization of C. Then $\mathcal{P}$ is proper if and only if*

$$\deg \mathcal{P} = \max\{\deg_x(F_C), \deg_y(F_C)\}.$$

Furthermore if $\mathcal{P}$ is proper and χ_1 is nonzero, then $\deg \chi_1 = \deg_y(F_C)$; similarly if χ_2 is nonzero then $\deg \chi_2 = \deg_x(F_C)$.

This theorem easily implies that every proper parametrization $\mathcal{P}_C$ of a smooth conic C is of degree 2 and the other way around every triple of coprime polynomials $f, g, h \in F[t]$ and such that $f^2 + g^2 = h^2$, $\max\{\deg f, \deg g, \deg h\} = 2$ determines a proper parametrization of the curve $a^2 + b^2 = c^2$. We denote such a parametrization by $\mathcal{P}_{f,g,h}$. Its equation in variable t is given by

$$\mathcal{P}_{f,g,h}(t) = (f(t)/h(t), g(t)/h(t)).$$

Any two such parametrizations $\mathcal{P}_{f,g,h}$ and $\mathcal{P}_{f',g',h'}$ are related by a linear change of variable $\mathcal{P}_{f',g',h'}(t) = \mathcal{P}_{f,g,h}(\gamma t)$ for a $\gamma \in \mathrm{GL}_2(F)$. We denote by $E_{f,g,h}$ the curve in the form 2 with $\alpha = \beta = \gamma$.

Corollary 4.4. *Let (f, g, h) and (f', g', h') be two triples of polynomials in variable t that parametrize the conic $a^2 + b^2 = c^2$ in a proper way. There exists a linear function γt, $\gamma \in GL_2(F)$ such that the automorphism $\sigma : t \mapsto \gamma t \in Aut(F(t))$ induces an isomorphism of the Mordell-Weil groups*

$$E_{f,g,h}(F(t)) \cong E_{f',g',h'}(F(t))$$

where $E_{f',g',h'}$ is $F(t)$-isomorphic to the curve $E^{\sigma}_{f,g,h}$. In particular, we obtain the equality

$$\textit{rank } E_{f,g,h}(F(t)) = 2.$$

Proof. The curve $E_{f,g,h}$ is isomorphic over $F(t)$ to the curve $y^2 = x(x-1)(x-(f/g)^2)$. Next we apply Theorem 4.3 to compare parametrizations $\mathcal{P}_{f,g,h}$ and $\mathcal{P}_{f',g',h'}$. By the theorem there exists an element $\gamma \in \mathrm{GL}_2(F)$ such that

$$f/h(\gamma t) = f'/h'(t), \quad g/h(\gamma t) = g'/h'(t).$$

This easily implies that $f/g(\gamma t) = f'/g'(t)$. We apply the automorphism σ to the curve $E_{f,g,h}$ and we get a curve $E^{\sigma}_{f,g,h}$ which is $F(t)$-isomorphic to $E_{f',g',h'}$. Finally this implies $E_{f,g,h}(F(t))$ is isomorphic to $E^{\sigma}_{f,g,h}(F(t))$ and to $E_{f',g',h'}(F(t))$. The last statement of the theorem follows for example from the fact that

$$\text{rank } E_{t^2-1,2t,t^2+1}(F(t)) = 2$$

cf. [11, Lemma 3.8]. □

Remark 4.5. We stress the fact that in general the curves $E_{f,g,h}$ and $E_{f',g',h'}$ for different parametrizations are not $F(t)$-isomorphic. This can be easily seen by comparing the j-invariants for both curves as a function of variable t.

We can keep track of the field of definition for the curve $E_{f,g,h}$. Suppose we let F be a number field and assume f, g, h all lie in $F[t]$ and that they determine a proper parametrization $\mathcal{P}_{f,g,h}$ of the conic $a^2 + b^2 = c^2$. We assume that the polynomials are coprime. We call a parametrization determined by polynomials $(t^2 - 1, 2t, t^2 + 1)$ a *standard parametrization.* It is easy to see that for any pair of coordinates $(x_0, y_0) \in F^2$ where $y_0 \neq 0$ we put $t = \frac{x_0+1}{y_0}$ to recover the point. For the point $(-1, 0)$ we put $t = 0$ and for $(1, 0)$ we put $t = 1/s$ to change the coordinate chart and in the projective coordinates we take $s = 0$. So every point of $\mathbb{P}^1(F)$ can be reached by this parametrization. We can assume without loss of generality that $\deg f = 2$. If not, then $\deg g = 2$ or otherwise this will imply $\deg h = 1$ and the triple (f, g, h) would not determine a proper parametrization of the conic.

Then from the equation $f^2 = h^2 - g^2$ we can deduce that $h - g = s_1^2$ and $h + g = s_2^2$ where f factors as $s_1 s_2$. We must have $\deg s_1 = \deg s_2 = 1$, otherwise the parametrization could not be proper. Assume $s_1 = c(t - \alpha)$ and $s_2 = d(t - \beta)$ for some $c, d, \alpha, \beta \in \bar{F}$. From the assumptions about f, g, h we get that $cd \in F$. Because $h = (s_1^2 + s_2^2)/2 \in F[t]$, $g = (s_2^2 - s_1^2)/2 \in F[t]$, then $c^2, d^2 \in F$ and $\alpha, \beta \in F$. We will show now that the parametrization $\mathcal{P}_{f,g,h}$ is related to the standard parametrization $\mathcal{P}_{t^2-1,2t,t^2+1}$ via a linear rational function with coefficients in F. This will imply that the groups $E_{f,g,h}(F(t))$ and $E_{t^2-1,2t,t^2+1}(F(t))$ are $F(t)$-isomorphic.

We have the equalities

$$\frac{f}{h} = \frac{2s_1s_2}{s_1^2 + s_2^2} = \frac{2(\gamma t)}{1 + (\gamma t)^2},$$

$$\frac{g}{h} = \frac{s_2^2 - s_1^2}{s_1^2 + s_2^2} = \frac{(\gamma t)^2 - 1}{1 + (\gamma t)^2}$$

where γ is a matrix from $\mathrm{GL}_2(F)$

$$\gamma = \begin{pmatrix} d/c & -(d/c)\beta \\ 1 & -\alpha \end{pmatrix}.$$

So the automorphism $t \mapsto \gamma t$ of $F(t)$ induces the isomorphism of the Mordell-Weil groups. The group $E_{t^2-1,2t,t^2+1}(F(t))$ can have rank 1 or 2 by [14, Thm. 3.1], and the result follows for any curve $E_{f,g,h}$ over $F(t)$ where $f^2 + g^2 = h^2$ determines a proper parametrization.

Remark 4.6. This way of reasoning can be generalized to any conic $\alpha a^2 + \beta b^2 = \gamma c^2$ defined over F. We have to fix one parametrization of this conic over F and then relate other $F(t)$-parametrizations to the fixed one. So in general we would also get a choice between rank 1 or 2.

Remark 4.7. It is not always true that the equality $2 \deg f = \deg(f^2 - g^2)$ holds as the standard parametrization $(t^2 - 1, 2t, t^2 + 1)$ might suggest. In fact we can have $\deg(f^2 - g^2) < 2 \deg f$ and in the situation of our previous lemma this can only happen when $\deg f = \deg g = 2$ (then we can only have $\deg(f^2 - g^2) = 3$).

Consider the following example:

$$\begin{aligned} f &= \frac{t^2}{\sqrt{2}} - \frac{t}{\sqrt{2}} + i\left(\frac{t}{\sqrt{2}} - \frac{1}{2\sqrt{2}}\right) + \frac{1}{2\sqrt{2}} \\ g &= \frac{t^2}{\sqrt{2}} - \frac{t}{\sqrt{2}} + i\left(\frac{1}{2\sqrt{2}} - \frac{t}{\sqrt{2}}\right) + \frac{1}{2\sqrt{2}} \\ h &= t^2 - t \\ f^2 - g^2 &= i\left(2t^3 - 3t^2 + 2t - \frac{1}{2}\right) \end{aligned}$$

Remark 4.8. We can always pull back an elliptic surface $(S, \mathbb{P}^1, \pi)$ along a morphism $f : \mathbb{P}^1 \to \mathbb{P}^1$ to obtain a new elliptic surface $(S', \mathbb{P}^1, \pi')$. Surface S' is birational to the fiber product $S \times_\phi \mathbb{P}^1$. When we apply this construction to an automorphism $f \in \mathrm{Aut}(\mathbb{P}^1)$, surfaces S and S' are isomorphic. This implies that for different parametrizations (f, g, h) and (f', g', h') that both determine a proper parametrization of the Pythagorean conic, the surfaces attached to $E_{f,g,h}$ and $E_{f',g',h'}$ are in fact isomorphic. This isomorphism do not respect the elliptic fibrations. Nonetheless, the Néron-Severi lattice is the same for both.

Remark 4.9. From [22, Prop. 11.14] or [21, Thm. 8.12] we obtain the invariance of the height pairing under the automorphism $\sigma \in \mathrm{Aut}(F(t))$. More precisely, for any $P, Q \in E(F(t))$ the intersection pairing $\langle P, Q\rangle_E$ equals $\langle P^\sigma, Q^\sigma\rangle_{E^\sigma}$. In particular, this implies that the Mordell-Weil lattices on both curves are the same.

For polynomials f, g, h that properly parametrize the conic $a^2 + b^2 = c^2$ the attached K3 surfaces corresponding to $E_{f,g,h}$ are isomorphic over $\overline{\mathbb{Q}}$ but not for any parametrization of $a^2 + b^2 = c^2$. In fact, we can easily produce an improper parametrization $(\frac{t^{2k}-1}{2}, t^k, \frac{t^{2k}+1}{2})$ for any $k \geq 2$. The elliptic surface attached to such a curve E_k will have Euler characteristic equal to $2k$, so for different values of k we will certainly obtain non-isomorphic elliptic surfaces. A quick computation reveals that the two linearly independent points in $E_k(\overline{\mathbb{Q}}(t))$ that we are able to produce might not give a complete list of free generators of the Mordell-Weil group. A numerical computation using the Nagao statistics, cf. [16] suggests that at least over $\mathbb{Q}(t)$ the Mordell-Weil rank should be again equal to 1.

Question 4.10. *Is it possible to determine the Mordell-Weil rank of the group $E_k(\mathbb{Q}(t))$ or $E_k(\overline{\mathbb{Q}}(t))$ when k varies?*

5. Supersingular reduction

An elliptic curve of the form $E_{f,g,h} : y^2 = x(x - f^2)(x - g^2)$ such that f, g, h determine a proper parametrization $\mathcal{P}_{f,g,h}$ of the conic $a^2 + b^2 = c^2$ is a generic fiber of a K3-surface of a very special type.

Lemma 5.1. *Let $f, g, h \in \overline{\mathbb{Q}}[t]$ be polynomials that determine a proper parametrization of the conic $a^2 + b^2 = c^2$. Let $(\mathcal{E}, \mathbb{P}^1, \pi)$ be the Kodaira-Néron model of the curve $E_{f,g,h}$. Then the triple $(\mathcal{E}, \mathbb{P}^1, \pi)$ is a singular elliptic K3-surface, i.e. its Picard number equals* 20.

Proof. We have an explicit description of the Kodaira types corresponding to the singular fibers of π. Corollary 4.4 implies that the rank of the Mordell-Weil group $E_{f,g,h}(\bar{\mathbb{Q}}(t))$ is two and the upper bound for the Picard number equal to 20. Application of the Shioda-Tate formula allows us to conclude the statement. □

Assume that X is a K3 surface in characteristic 0. We consider the situation when the rank of $NS(X)$ is maximal possible, equal to 20. We denote by $d(X)$ the discriminant of the Néron-Severi lattice. For elliptic K3 surfaces it can be computed if we have the information about the structure of the Mordell-Weil group of the generic fiber and about the fibration, cf. [21]. We have an explicit formula, cf. [22, §11.9]

$$d(X) = (-1)^{\mathrm{rank}(E_{\mathrm{gen}}(K))}\mathrm{disc}(\mathrm{Triv}(X)) \cdot \mathrm{disc}(MWL(X))/(\#(E_{\mathrm{gen}}(K))_{\mathrm{tors}})^2$$

Field K is the function field of $\mathbb{P}^1$ and E_{gen} is the generic fiber of X. The lattice $\mathrm{Triv}(X)$ is generated by the general smooth fiber F, image of the zero section $\overline{O}$ and the components of bad fibers that form root sublattices of standard types A_n, D_n and E_n with appropriate Dynkin diagrams. The lattice $MWL(X) = E_{gen}(K)/(E_{gen}(K))_{\mathrm{tors}}$ with intersection pairing induced from the height pairing on E_{gen}.

The Neron-Severi group $NS(X)$ embeds as a lattice into $H^2(X,\mathbb{Z})$ with its lattice structure inherited from the cup-product. The orthogonal complement of $NS(X)$ is called the transcendental lattice of X and is denoted by $T(X)$. For K3 surfaces the second Betti number equals 22, so for X singular, this means that rank $T(X) = 2$. It can be proved that $T(X)$ is an even lattice of discrminant $-d(X)$, cf. [19]. Every singular K3-surface can be defined over a number field F and we would like to consider the situation when X can be reduced modulo a prime p. More precisely, we consider a non-empty open subset U of Spec $\mathbb{Z}_F$, where $\mathbb{Z}_F$ is the ring of algebraic integers in F, and a smooth proper morphism $\mathcal{X} \to U$ with generic fiber isomorphic to X. We denote by π_F the canonical morphism $\mathrm{Spec}\,\mathbb{Z}_F \to \mathrm{Spec}\,\mathbb{Z}$. For a closed point $\mathfrak{p}$ in U we denote by $X_{\mathfrak{p}}$ the fiber above $\mathfrak{p}$, which is a K3 surface defined over the residue field of $\mathfrak{p}$. In characteristic p the rank of Néron-Severi group can achieve rank 22. Such a K3 surface is called *supersingular.* We analyze the set $S_p(\mathcal{X})$ that contains primes $\mathfrak{p}$ above p such that $X_{\mathfrak{p}}$ is supersingular. By the work of Shimada [19] we can now say when the reduction of the K3 surface would be supersingular. Let $\chi_p(x)$ denote the Legendre symbol (x/p) for p an odd prime. We have the following theorem

Theorem 5.2 ([19, Thm. 1])**.** *Let p be a prime such that $p \nmid 2d(X)$. Then*

- *if $\chi_p(x) = 1$, then $S_p(\mathcal{X}) = \emptyset$,*
- *if $\mathfrak{p} \in S_p(\mathcal{X})$, then $d(X_{\mathfrak{p}}) = p^2$, i.e. the surface $X_{\mathfrak{p}}$ is of Artin invariant* 1.

Moreover, there exists a finite set N of primes in $\mathbb{Z}$ that contains the prime divisors of $2d(X)$ such that for any $p \notin N$

$$S_p(\mathcal{X}) = \begin{cases} \emptyset & \text{if } \chi_p(d(X)) = 1 \\ \pi^{-1}(p) & \text{if } \chi_p(d(X)) = -1 \end{cases} \tag{33}$$

This theorem allows us to easily detect for which primes we can expect to have the supersingular reduction of the surface $S_{f,g,h}$ attached to the curve $E_{f,g,h}$. We need to compute the discriminant.

Lemma 5.3. *Let (f,g,h) be a triple of polynomials which parametrizes the conic $a^2+b^2=c^2$ in a proper way. The discriminant of the elliptic surface $S_{f,g,h}$ with generic fibre $E_{f,g,h}$ is equal to -32.*

Proof. Let X denote the elliptic surface $S_{f,g,h}$. From the assumptions the polynomials f, g and f^2-g^2 are separable. The trivial lattice in $\mathrm{NS}(X)$ contains

$\deg f + \deg g$ copies of the root lattice A_3, $\deg(f^2-g^2)$ copies of the lattice A_1 and possibly a copy of A_{n-1} lattice that corresponds to the fiber above ∞, where $n = 8\deg f - 4\deg g - 2\deg(f^2-g^2)$. If $\deg g = \deg f = 2$ and $\deg(f^2-g^2) = 2\deg f$ there is no such lattice, namely $n = 0$. In the situation $\deg g = 1$ we have $n = 4$ and for $\deg g = 2$ and $\deg(f^2-g^2) = 3$ we get $n = 2$. In each case we obtain that the trivial lattice is a sum $U + 4A_3 + 4A_1$ where $U = \text{span }(F, \overline{O})$.

Torsion subgroup $E_{f,g,h}(\bar{\mathbb{Q}}(t))$ was computed in [12] and is of order 8. The remaining part is the Mordell-Weil lattice. It is of rank two with generators

$$\begin{aligned} Q_1 =& (-(1+\sqrt{2})g(g-h), \sqrt{-1}(1+\sqrt{2})g(g-h)(\sqrt{2}g-h)),\\ Q_2 =& ((f-h)(g-h), (f+g)(f-h)(g-h)) \end{aligned}$$

and height pairing matrix

$$\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix} \tag{34}$$

The root lattices corresponding to different bad fibers are orthogonal to each other in $\text{NS}(X)$ and we have the standard formula $\text{disc}(A_n) = (-1)^n(n+1)$. The image of the zero section and the general fiber span a lattice U in $\text{NS}(X)$ which is of discriminant -1. Hence we get $d(X) = -32$. □

For a model of $S_{f,g,h}$ with good reduction at a prime above p it easy is to check whether the reduction will be supersingular. We assume that $p \neq 2$, because this is exactly the condition $p \nmid 2d(X)$ from Theorem 5.2.

$$\chi_p(x) = -1 \Leftrightarrow \left(\frac{-32}{p}\right) = -1 \Leftrightarrow p \equiv 5, 7, 13, 15 (\text{mod } 16).$$

It is now convenient to switch to the standard parametrization $(t^2-1, 2t, t^2+1)$ and its associated elliptic surface which is defined over $\mathbb{Q}$. The Weierstrass equation for this model has the form

$$y^2 = x(x-(t^2-1)^2)(x-4t^2).$$

It is a globally minimal model and is defined over $\mathbb{Z}[t]$. This has the advantage that we can perform the Tate algorithm both in characteristic zero and in positive characteristic (at least equal to 5). We can do the blow-ups simultaneously at least if the reduced equation behaves in a similar way as the equation in characteristic 0, cf. [12, Tw. 2.2.12].

Proposition 5.4. *The surface $S_{t^2-1,2t,t^2+1}$ has good reduction for primes $p \geq 5$.*

Proof. We check that after modulo p reduction the radicals of polynomials $a_i(t)$ and of discriminant of the Weierstrass equation, and the numerator and denominator of j-invariant remain separable (and that they do not have a common root modulo p). We also check this for the model at infinity. The support of the discriminants of all computed polynomials is contained in the set $\{2, 3\}$. So we can perform the Tate algorithm in characteristic p and in characteristic zero, and we will get the same reduction types, which implies that in fact we have a good reduction modulo p. □

The results lead to the following corollary.

Corollary 5.5. *The surface $S_{t^2-1,2t,t^2+1}$ has good supersingular reduction at primes $p \geq 5$ such that $p \equiv 5, 7, 13, 15(mod\ 16)$. The discriminant of the Néron-Severi* *group is equal to p^2. Generic fiber is an elliptic curve over $\mathbb{F}_p(t)$ with geometric Mordell-Weil rank 4.*

Proof. By [4, Thm.3,4] we can identify the action of Frobenius automorphism acting on the transcendental lattice $T(X)$. We find that in our situation we have the CM-form corresponding to level 8 in [17, Tab.1]. This implies the equality $N = \{2, 3\}$ where N is the set from Theorem 5.2. Now we prove the last statement. Because of the good reduction situation we obtain exactly the same fiber types of bad reduction. For the supersingular case the Picard number equals 22, so the application of Shioda-Tate formula leads to the conclusion that the Mordell-Weil rank of $E_{t^2-1,2t,t^2+1}(\overline{\mathbb{F}}_p(t))$ equals 4. □

Remark 5.6. Supersingular K3 surface of Artin invariant 1 is unique up to isomorphism and very special in another way that the generators of the Néron-Severi group are defined over $\mathbb{F}_{p^2}$. So we can even say that $E_{t^2-1,2t,t^2+1}(\overline{\mathbb{F}}_p(t)) = E_{t^2-1,2t,t^2+1}(\mathbb{F}_{p^2}(t))$.

Example 5.7. We can produce explicit basis of the Mordell-Weil group for a few small primes. In fact, the theorem implies that the height of the extra points that add rank two to the Mordell-Weil group will grow unbounded and this means that the computations for sufficiently large primes require sieving over many rational functions with both denominator and numerator of very high degree. This computations become quickly infeasible for a typical computer.

In our computations we have exploited the fact that $E_{t^2-1,2t,t^2+1}[2]$ is contained in the $\mathbb{F}_p(t)$-rational points subgroup. Under this assumption we can apply a full 2-descent described in [23, Chap. 10]. The torsion subgroup of $E_{t^2-1,2t,t^2+1}(\mathbb{F}_{p^2}(t))$ is always isomorphic to $\mathbb{Z}/2 \oplus \mathbb{Z}/4$. This is a consequence of [14, Cor. 5.4] applied in positive characteristic. The crucial step is to prove that not all two-torsion points are divisible by 2. It suffices to prove that the polynomial $f^2 - g^2 = t^4 - 6t^2 + 1$ is separable over $\mathbb{F}_{p^2}[t]$, which is always the case for primes $p \geq 3$.

The free part of the Mordell-Weil group will always contain the reductions of points Q_1 and Q_2, so below we only present the other two generators and compute the height pairing matrix. The trivial lattice $\mathrm{Triv}(S_{t^2-1,2t,t^2+1})$ has discriminant 2^{12} and the torsion subgroup has order 8. This implies that if we provide two points Q_3, Q_4 such that the height pairing matrix of the tuple (Q_1, Q_2, Q_3, Q_4) has determinant $p^2/2^6$, then the points generate the free part of the Mordell-Weil group.

Case $p = 5$**:** We realize $\mathbb{F}_{5^2}$ as $\mathbb{F}_5[s]/(s^2 + 4s + 2)$.

$$Q_3 = (s^3 t(t+1)(t+s^{22}), s^{10} t(t+1)(t+s^3)(t+s^{14})(t+s^{16})(t+s^{22}))$$

$$Q_4 = (t^4 + 4t^2, t^5 + 4t^3)$$

Height pairing matrix with determinant $5^2/2^6$.

$$\begin{pmatrix} 1/2 & 0 & 1/4 & 0 \\ 0 & 1 & 0 & 1/2 \\ 1/4 & 0 & 2 & -5/4 \\ 0 & 1/2 & -5/4 & 3/2 \end{pmatrix}$$

Case $p = 7$**:** Let us assume that $\mathbb{F}_{7^2} = \mathbb{F}_7[s]/(s^2 - 3)$.

$$Q_3 = (t^2 + t, st(1+t)(2+t)^2)$$

$$Q_4 = (1, 2t(3+t)(4+t))$$

Height pairing matrix with determinant $7^2/2^6$.

$$\begin{pmatrix} 1/2 & 0 & -1/4 & 0 \\ 0 & 1 & 0 & 1/2 \\ -1/4 & 0 & 1 & 0 \\ 0 & 1/2 & 0 & 2 \end{pmatrix}$$

Case $p = 13$**:** We realize $\mathbb{F}_{13^2}$ as $\mathbb{F}_{13}[s]/(s^2+12s+2)$.

$$Q_3 = (s^5(t+s^{82})^2(t+12), s^{47}(t+s^4)(t+s^{18})(t+s^{82})(t+12)(t+s^{115}))$$

$$Q_4 = \left(\frac{11t(t+2)^2(t+6)^2}{(t+5)^2}, \frac{3t(t+2)(t+6)(t+7)(t+8)(t+11)\left(t^2+2t+12\right)}{(t+5)^3}\right)$$

Height pairing matrix with determinant $13^2/2^6$.

$$\begin{pmatrix} 1/2 & 0 & 1/4 & 0 \\ 0 & 1 & 1/2 & 1/2 \\ 1/4 & 1/2 & 2 & 1/4 \\ 0 & 1/2 & 1/4 & 7/2 \end{pmatrix}$$

Example 5.8. The curve $y^2 = (x-(t^2-1)^2)(x-4t^2)(x+(t^2+1)^2)$ that we considered before also determines a singular K3 surface. By the discriminant computation we checked that it is equal to $-2^5 \cdot 3$, hence we obtain supersingular reduction at primes p such that $\left(\frac{-2^5\cdot 3}{p}\right) = -1$, so $p = 13, 17, 19, 23, 37, 41, 43, 47, 61, 67, 71, \ldots$. We check that the attached CM-form attached to the transcendental lattice by [4] is of level $N = 24$, cf [17, Tab. 1]. For each supersingular prime we will obtain rank 8 over $\mathbb{F}_{p^2}$.

6. Remarks

Below we discuss several aspects of the general family (1) that were not discussed elsewhere. We deal mainly with the family of type $\alpha = \beta = \gamma = 1$ and for the other cases we can perform a similar study.

6.1. **Lower bounds over Q.**

We proved in [14] what are the lower bounds for the Mordell-Weil rank of specialization in our family. This theorem relies on the Silverman's specialization result, cf. [24, III §11, Thm. 11.4]. Silverman's theorem allows us only to say that for all but finitely many elements in the number field F over which the curve (1) is defined, the specialization homomorphism will be injective. We will discuss below an approach to this problem, for number fields with class number one, that allows us to produce an infinite and explicit set of specialization for which the specialization homomorphism is injective.

To simplify the exposition we will discuss only the specialization of curves $E_{f,g,h}$ for $f, g, h \in \mathbb{Q}[t]$ which parametrize the conic $a^2+b^2=c^2$. The tool we want to use is the theorem from [7].

Theorem 6.1 ([7, Thm. 1.1])**.** *Let E be a nonconstant elliptic curve over $\mathbb{Q}(t)$ given by the equation*

$$E = E(t) : y^2 = (x-e_1)(x-e_2)(x-e_3) \quad (e_1, e_2, e_3 \in \mathbb{Z}[t]).$$

Assume that $t_0 \in \mathbb{Q}$ satisfies the following condition.

(*) For every nonconstant square-free divisor h in $\mathbb{Z}[t]$ of $(e_1-e_2)(e_1-e_3)$ or $(e_2-e_1)(e_2-e_3)$ or $(e_3-e_1)(e_3-e_1)$, the rational number $h(t_0)$ is not a square in $\mathbb{Q}$.

Then the specialization homomorphism $sp_{t_0} : E(\mathbb{Q}(t)) \to E(t_0)(\mathbb{Q})$ is injective.

In our situation, let $e_1 = 0, e_2 = (t^2-1)^2$ and $e_3 = 4t^2$. It is easy to compute the set of rational numbers that satisfies property $(*)$. We obtain the set that contains 35 polynomials of degree at most 6. Quick computation reveals that for all rational numbers t_0 with naive height smaller than 500 (there are 304463 such rational numbers) about 97.5% of this numbers satisfy condition $(*)$. The set of elements of $\mathbb{Q}$ of naive height at most equal to 10 that satisfy condition (*) is

$$\{-6,-10/3,-8/3,-7/4,-8/5,-10/7,-7/5,-7/6,-6/7,-5/7,-7/10,$$
$$-5/8,-4/7,-3/8,-3/10,-1/6,1/6,3/10,3/8,4/7,5/8,7/10,5/7,6/7,$$
$$7/6,7/5,10/7,8/5,7/4,8/3,10/3,6\}.$$

Elements of $\mathbb{Q}$ that do not satisfy condition $(*)$ can still produce an injective specialization homomorphism or at least preserve the rank bound. In this case the rank of $E_{t^2-1,2t,t^2+1}(\mathbb{Q}(t))$ equals one and by a direct computation we have checked that for all t_0 for which the specialized curve is nonsingular, the rank was at least one for all t_0 with naive height at most 400.

6.2. **Polynomial solutions.** For any curve

$$E_{\alpha,\beta,\gamma} : y^2 = x(x-\alpha a^2)(x-\beta b^2), \quad \alpha a^2 + \beta b^2 = \gamma c^2$$

and a fixed conic $C : q(a,b,c) = 0$ we can ask for the description of the $K(C)$-points of $E_{\alpha,\beta,\gamma}$. In fact, the curve $E_{\alpha,\beta,\gamma}$ is not well-defined over $K(C)$, so we slightly change the model to

$$y^2 = x(x-1)(x-\beta b^2/(\alpha a^2)).$$

By abuse of notation we will denote this curve again by $E_{\alpha,\beta,\gamma}$. The curve written this way is an elliptic curve defined over $K(C)$. We ask now for the description of $K(C)$ points on this curve, written explicitly in terms of homogeneous variables a, b, c. We will carefully analyze only the simplest case when $q(a,b,c) = a^2+b^2-c^2$ is the equation that defines Pythagorean triples. Function field $K(C)$ is isomorphic to $K(\mathbb{P}^1) = \bar{\mathbb{Q}}(t)$, where t is a variable. We rewrite the equation

$$y^2 = x(x-1)(x-\frac{b^2}{a^2}) \tag{35}$$

in the form

$$y^2 = x(x-1)(x-\left(2t/(t^2-1)\right)^2).$$

We use the field isomorphism $\phi : K(C) \to K(\mathbb{P}^1)$, which satisfies $\phi(a/c) = (t^2-1)/(t^2+1)$, $\phi(b/c) = 2t/(t^2+1)$. This can be deduced from the standard parametrization of the circle by lines. The inverse to this map ϕ^{-1} satisfies $\phi^{-1}(t) = b/(c-a)$.

Proposition 6.2. *Every $K(C)$-point (x,y) on $E_{1,1,1}$ is represented by three polynomials $k, l, m \in \bar{\mathbb{Q}}[a,b,c]$ that satisfy $x = k/l^2$, $y = m/l^3$ and $\deg k = 2 + 2\deg l$, $\deg m = 3 + 3\deg l$.*

Proof. The proof follows from the definition of ϕ. We observe that each $K(C)$-point on $E_{1,1,1}$ is obtained from the point on (35) by a linear change of variables $(x,y) \mapsto (xa^2, ya^3)$. □

6.3. **Two isogeny.** We observe that the curve

$$E_{f,g} : y^2 = x(x - f^2)(x - g^2)$$

admits two–isogenies defined over the field K of definition of elements f, g. The isogenous curve $E_{f,g}/\langle T\rangle$ for $T \in E_{f,g}[2]$ is not always of the form above if the kernel contains only $(f^2, 0)$ or by symmetry $(g^2, 0)$. We analyze the isogeny with kernel $\{O, (0, 0)\}$. It is easy to determine it explicitly by Velu formulas [26] and an explicit computation in MAGMA. Consider the curve

$$E_{i(f-g),i(f+g)} : y^2 = x(x + (f - g)^2)(x + (f + g)^2)$$

which is isomorphic to $E_{f,g}/\langle(0, 0)\rangle$ over K with isomorphism $(x, y) \mapsto (x+f^2+g^2, y)$. The two-isogeny $\tau : E_{f,g} \to E_{f,g}/\langle(0, 0)\rangle$ is given by the formula

$$\tau(x, y) = ((x^2 + f^2g^2)/x, (x^2y - f^2g^2y)/x^2).$$

If we allow the relation $f^2 + g^2 = h^2$, then $-(f - g)^2 - (f + g)^2 = -2h^2$. Both conics $a^2 + b^2 = c^2$ and $-a^2 - b^2 = -2c^2$ can be easily parametrized properly with polynomials in $\mathbb{Q}(t)$, however the curves are not $\mathbb{Q}$-isomorphic. The existence of $\mathbb{Q}(t)$-isogeny implies that we have exactly the same rank of Mordell-Weil groups over $\mathbb{Q}(t)$ for both curves associated with those conics.

Acknowledgements

The author would like to express his gratitude to the organisers of the ALANT 2014 conference for allowing him to speak about his results and stimulating atmosphere of the conference. He also thanks Remke Kloosterman for his suggestion of proof in §6.2. The author was supported by the National Science Centre Poland research grant 2012/05/N/ST1/02871 and by the DFG grant Sto299/11-1 within the framework of the Priority Programme SPP 1489.

References

[1] Michael Artin and Peter Swinnerton-Dyer, *The Shafarevich-Tate conjecture for pencils of elliptic curves on K3 surfaces*, Invent. Math. **20** (1973), 249–266.

[2] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language.*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[3] Andrew Bremner and Maciej Ulas, *Points at rational distances from the vertices of certain geometric objects*, ArXiv e-prints (2015), 1–23, 1502.07312.

[4] Noam D. Elkies and Matthias Schütt, *Modular forms and K3 surfaces*, Adv. Math. **240** (2013), 106–131.

[5] Hélène Esnault, Keiji Oguiso, and Xun Yu, *Automorphisms of elliptic K3 surfaces and Salem numbers of maximal degree*, ArXiv e-prints (2014), 1–12, 1411.0769.

[6] William Fulton, *Intersection theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 2, Springer-Verlag, Berlin, 1984.

[7] Ivica Gusić and Petra Tadić, *Injectivity of the specialization homomorphism of elliptic curves*, J. Number Theory **148** (2015), 137–152.

[8] Daniel Huybrechts, *Complex geometry*, Universitext, Springer-Verlag, Berlin, 2005.

[9] Remke Kloosterman, *Elliptic K3 surfaces with geometric Mordell-Weil rank 15*, Canad. Math. Bull. **50** (2007), no. 2, 215–226.

[10] James Milne, *On a conjecture of Artin and Tate*, Ann. of Math. (2) **102** (1975), no. 3, 517–533.

[11] Bartosz Naskręcki, *Mordell-Weil ranks of families of elliptic curves associated to Pythagorean triples*, Acta Arithmetica **160** (2013), no. 2, 159–183.

[12] ———, *Ranks in families of elliptic curves and modular forms*, Adam Mickiewicz University (2014), Ph.D. thesis.

[13] ______, *Divisibility sequences of polynomials and heights estimates*, to appear in New York Journal of Mathematics (2016), 1–32.

[14] ______, *Mordell-Weil ranks of families of elliptic curves parametrized by binary quadratic forms*, preprint (2016), 1–21.

[15] Keiji Oguiso, *An elementary proof of the topological Euler characteristic formula for an elliptic surface*, Comment. Math. Univ. St. Paul. **39** (1990), no. 1, 81–86.

[16] Michael Rosen and Joseph H. Silverman, *On the rank of an elliptic surface*, Invent. Math. **133** (1998), no. 1, 43–67.

[17] Matthias Schütt, *CM newforms with rational coefficients*, Ramanujan J. **19** (2009), no. 2, 187–205.

[18] J. Rafael Sendra, Franz Winkler, and Sonia Pérez-Díaz, *Rational algebraic curves*, Algorithms and Computation in Mathematics, vol. 22, Springer, Berlin, 2008, A computer algebra approach.

[19] Ichiro Shimada, *Transcendental lattices and supersingular reduction lattices of a singular K3 surface*, Trans. Amer. Math. Soc. **361** (2009), no. 2, 909–949.

[20] Ichiro Shimada, *Automorphisms of supersingular K3 surfaces and Salem polynomials*, ArXiv e-prints (2015), 1–16, 1503.04517.

[21] Tetsuji Shioda, *On the Mordell-Weil lattices*, Comment. Math. Univ. St. Paul. **39** (1990), no. 2, 211–240.

[22] Tetsuji Shioda and Matthias Schütt, *Elliptic surfaces*, ArXiv e-prints (2010), arXiv:0907.0298v3.

[23] Joseph Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986.

[24] ______, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[25] Ronald van Luijk, *An elliptic K3 surface associated to Heron triangles*, J. Number Theory **123** (2007), no. 1, 92–119.

[26] Jacques Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241.

Faculty of Mathematics and Computer Science, Adam Mickiewicz University, Umultowska 87, 61-614 Poznań, Poland, and School of Mathematics, University of Bristol, University Walk, Bristol BS8 1TW, UK, E-mail: nasqret@gmail.com