An elliptic K3 surface associated to Heron triangles

Ronald van Luijk
Department of Mathematics 3840
970 Evans Hall
University of California
Berkeley, CA 94720-3840
rmluijk@math.berkeley.edu

Abstract:

A rational triangle is a triangle with rational sides and rational area. A Heron triangle is a triangle with integral sides and integral area. In this article we will show that there exist infinitely many rational parametrizations, in terms of s, of rational triangles with perimeter $2s(s+1)$ and area $s(s^2-1)$. As a corollary, there exist arbitrarily many Heron triangles with all the same area and the same perimeter. The proof uses an elliptic K3 surface Y. Its Picard number is computed to be 18 after we prove that the Néron-Severi group of Y injects naturally into the Néron-Severi group of the reduction of Y at a prime of good reduction. We also give some constructions of elliptic surfaces and prove that under mild conditions a cubic surface in $\mathbb{P}^3$ can be given the structure of an elliptic surface by cutting it with the family of hyperplanes through a given line L. Some of these constructions were already known, but appear to have lacked proof in the literature until now.

Keywords:

Heron triangles, elliptic surfaces, K3 surfaces, Néron-Severi group, Tate conjecture, Diophantine equations, arithmetic geometry, algebraic geometry, number theory

Table of contents:

1 Introduction

A *rational triangle* is a triangle with rational sides and area. A *Heron triangle* is a triangle with integral sides and area. Let $\mathbb{Q}(s)$ denote the field of rational functions in s with coefficients in $\mathbb{Q}$. The main theorem of this article states the following.

Theorem 1.1 *There exists a sequence $\{(a_n, b_n, c_n)\}_{n\geq 1}$ of triples of elements in $\mathbb{Q}(s)$ such that*

(1) *for all $n \geq 1$ and all $\sigma \in \mathbb{R}$ with $\sigma > 1$, there exists a triangle $\Delta_n(\sigma)$ with sides $a_n(\sigma)$, $b_n(\sigma)$, and $c_n(\sigma)$, inradius $\sigma - 1$, perimeter $2\sigma(\sigma + 1)$, and area $\sigma(\sigma^2 - 1)$, and*

(2) *for all $m, n \geq 1$ and $\sigma_0, \sigma_1 \in \mathbb{Q}$ with $\sigma_0, \sigma_1 > 1$, the rational triangles $\Delta_m(\sigma_0)$ and $\Delta_n(\sigma_1)$ are similar if and only if $m = n$ and $\sigma_0 = \sigma_1$.*

Remark 1.2 The triples of the sequence mentioned in Theorem 1.1 can be computed explicitly. We will see that we can take the first four to be

$$(a_n, b_n, c_n) = \left(\frac{s(s+1)(y_n + z_n)}{x_n + y_n + z_n}, \frac{s(s+1)(x_n + z_n)}{x_n + y_n + z_n}, \frac{s(s+1)(x_n + y_n)}{x_n + y_n + z_n}\right), \quad (1)$$

with

$$\begin{aligned}
(x_1, y_1, z_1) =& \big(1 + s, -1 + s, (-1 + s)s\big),\\
x_2 =&(-1 + s)(1 + 6s - 2s^2 - 2s^3 + s^4)^3,\\
y_2 =&(-1 + s)(-1 + 4s + 4s^2 - 4s^3 + s^4)^3,\\
z_2 =&s(1 + s)(3 + 4s^2 - 4s^3 + s^4)^3,\\
x_3 =&(-1 + s)(1 + 2s + 2s^2 - 2s^3 + s^4)^3\\
&(-1 - 22s + 66s^2 + 14s^3 - 72s^4 + 30s^5 + 6s^6 - 6s^7 + s^8)^3,\\
y_3 =&(1 + s)(-1 + 20s + 68s^2 - 84s^3 + 139s^4 + 32s^5 - 224s^6+\\
&64s^7 + 149s^8 - 148s^9 + 60s^{10} - 12s^{11} + s^{12})^3,\\
z_3 =&(-1 + s)s(5 + 10s + 126s^2 + 62s^3 - 225s^4 + 52s^5 + 28s^6+\\
&12s^7 + 27s^8 - 62s^9 + 38s^{10} - 10s^{11} + s^{12})^3,\\
x_4 =&(1 + s)(-1 - 62s + 198s^2 + 1698s^3 + 7764s^4 - 8298s^5 - 10830s^6 + 43622s^7 - 15685s^8\\
&-45356s^9 - 1348s^{10} + 75284s^{11} - 13088s^{12} - 93076s^{13} + 85220s^{14} + 12s^{15} - 49467s^{16}\\
&+40842s^{17} - 16034s^{18} + 2282s^{19} + 844s^{20} - 546s^{21} + 138s^{22} - 18s^{23} + s^{24})^3,\\
y_4 =&(-1 + s)(-1 + 54s + 550s^2 - 10s^3 + 5092s^4 + 16674s^5 + 98s^6 - 51662s^7 + 22875s^8+\\
&41916s^9 - 63076s^{10} + 45628s^{11} + 13088s^{12} - 63644s^{13} + 38884s^{14} + 17668s^{15}-\\
&31195s^{16} + 8302s^{17} + 8990s^{18} - 9554s^{19} + 4476s^{20} - 1254s^{21} + 218s^{22} - 22s^{23} + s^{24})^3,\\
z_4 =&(-1 + s)s(-7 - 28s - 1168s^2 - 2588s^3 + 5170s^4 + 6940s^5 + 20176s^6 - 10628s^7-\\
&70305s^8 + 46664s^9 + 85440s^{10} - 107832s^{11} + 380s^{12} + 66840s^{13} - 46848s^{14} + 13656s^{15}-\\
&1465s^{16} - 2796s^{17} + 5712s^{18} - 5228s^{19} + 2738s^{20} - 884s^{21} + 176s^{22} - 20s^{23} + s^{24})^3.
\end{aligned}$$

Multiplying these four triples by a common denominator and substituting only integral σ, we obtain an infinite parametrized family of quadruples of pairwise nonsimilar Heron triangles, all with the same area and the same perimeter. For any positive integer N we can do the same to N triples of the sequence. We find that Theorem 1.1 implies the following corollary.

Corollary 1.3 *For every positive integer N there exists an infinite family, parametrized by s, of N-tuples of pairwise nonsimilar Heron triangles, all N with the same area $A(s)$ and the same perimeter $p(s)$, such that for any two different $\sigma, \sigma' \in \mathbb{Z}_{>1}$ the corresponding ratios $A(\sigma)/p(\sigma)^2$ and $A(\sigma')/p(\sigma')^2$ are different.*

This corollary generalizes a theorem of Mohammed Aassila [Aa], and Alpar-Vajk Kramer and Florian Luca [KL]. Their papers give identical parametrizations to prove the existence of an infinite parametrized family of *pairs* of Heron triangles with the same area and perimeter. The corollary also answers the question, posed by Alpar-Vajk Kramer and Florian Luca and later by Richard Guy, whether triples of Heron triangles with the same area and perimeter exist, or even N-tuples with $N > 3$. Shortly after Richard Guy had posed this question, Randall Rathbun found with a computer search a set of 8 Heron triangles with the same area and perimeter. Later he found the smallest 9-tuple. Using our methods, we can find an N-tuple for any given positive integer N. For example, Table 1 shows 20 values of a, b, and c such that the triangle with sides a, b, and c has perimeter p and area A as given.

We will exhibit a bijection between the set of triples (a, b, c) of sides of (rational) triangles up to scaling and a subset of the set of (rational) points on a certain algebraic surface X described in section 2. We will prove Theorem 1.1 by finding infinitely many suitable curves on X. In section 3 we introduce the notion of elliptic surface and state some of their properties. Two constructions of elliptic surfaces are described in section 4. These constructions were already known, but the proof that they actually yield elliptic surfaces appears to lack in the literature. Section 4 therefore contains detailed proofs of these technical facts. One of these constructions is used to give some blow-up $\widetilde{X}$ of X the structure of an elliptic surface over $\mathbb{P}^1$ in section 5. In that same section we prove Theorem 1.1 by examening an elliptic K3 surface $Y \to C$, obtained from $\widetilde{X} \to \mathbb{P}^1$ by a base change $C \to \mathbb{P}^1$.

The relation between the geometry and the arithmetic of K3 surfaces in general is not clear at all, see [BT]. The last two sections are therefore dedicated to a deeper analysis of the geometry of the K3 surface Y. They are not needed for the proof of the main theorem and serve their own interest. Section 6 describes the behavior of the Néron-Severi group of a surface under good reduction. This again was already known, but until now lacked proof in the literature. It is used in section 7 to determine the full Néron-Severi group of Y and the Mordell-Weil group of the generic fiber of $Y \to C$.

Our theorem has been incorporated in Guy's book on unsolved problems in number theory in the sections about Heron triangles, see [Guy], D21 and D22.

a	b	c
115439787835070058360 0	232446631613602606200 0	263265398501698232640 0
109693916042374263600 0	248535072633150831528 0	252922829274845802072 0
135330122225622444120 0	204400760237766172080 0	271420935486982281000 0
132688262921705346240 0	207629339763603958200 0	270834215265061592760 0
117529195759686711000 0	228790167745523464080 0	264832454445160722120 0
139206802977584482140 0	199799632791467408700 0	272145382181319006360 0
166471797486156041880 0	170388527676114435187 5	274291492788100420132 5
115962139816224221520 0	231496900738776855000 0	263692777395369820680 0
158288681552560158600 0	178791865172932035024 0	274071271224878703576 0
136333867081236584760 0	203194920668969469240 0	271623030200164843200 0
162973818120098905920 0	173943209724336332280 0	274234790105935659000 0
195881992932811185000 0	142602090855086542680 0	272667734162473169520 0
225605920352614041240 0	119506941485433451950 0	266038956112323404010 0
222794475440101765200 0	121359776954817240840 0	266997565555451891160 0
200558259600261441278 4	138559086520953319821 6	272034471829156136100 0
246216910565063217780 0	110047231042889679000 0	254887676342418000420 0
219820893128953260760 0	123416019674281248200 0	267914905147136388240 0
244079551410116942520 0	110548673829717439680 0	256523592710536515000 0
246961685150522837040 0	109910702437714924200 0	254279430362133135960 0
262305576736327457833 5	114381747226434391704 0	234464493987609047662 5
$p = a + b + c = 6111518179503708972000$		
$A = 1340792724147847711994993266314426038400000$		

Table 1: 20 triangles with the same area and the same perimeter

The author would like to thank Bjorn Poonen, Robin Hartshorne, Arthur Ogus, Tom Graber, Bas Edixhoven, Jasper Scholten, Jan Stienstra, Igor Dolgachev, and especially Hendrik Lenstra for very helpful discussions.

2 A surface associated to Heron triangles

For a triangle with sides a, b, and c, let r, p, and A denote its inradius, perimeter, and area respectively. The line segments from the vertices of the triangle to the midpoint of the incircle divide the triangle in three smaller triangles of areas $ar/2$, $br/2$, and $cr/2$. Adding these we find $A = rp/2$. Set $x = p/2 - a$, $y = p/2-b$, and $z = p/2-c$. Then we get $p = 2(x+y+z)$, so $A = r(x+y+z)$. Heron's formula $A^2 = (x + y + z)xyz$ then yields $r^2(x + y + z) = xyz$. Therefore, the point $[r : x : y : z] \in \mathbb{P}^3$ lies on the surface $X \subset \mathbb{P}^3_{\mathbb{Q}}$ given by $r^2(x+y+z) = xyz$. Conversely, if $[1 : x : y : z]$ lies on X, with $x, y, z > 0$, then the triangle with sides $a = y + z$, $b = x + z$, and $c = x + y$ has inradius 1. Thus we get a bijection between the set of triples (a, b, c) of sides of triangles up to scaling and the set of real points $[r : x : y : z]$ on X with positive ratios x/r, y/r, and z/r. Let $G \subset \operatorname{Aut} X$ denote the group of automorphisms of X induced by the permutations of the coordinates x, y, and z. Let $f \colon X \dashrightarrow \mathbb{P}^1$ be the rational map given by $f \colon [r : x : y : z] \mapsto [r : x+y+z]$. Note that if we let G act trivially on $\mathbb{P}^1$, then f commutes with the action of G.

Lemma 2.1 *For $i = 1, 2$, let Δ_i denote a triangle, let a_i, b_i, and c_i denote the sides of Δ_i, and let P_i be the point on X corresponding to the equivalence class (under scaling) of the triple (a_i, b_i, c_i). Then Δ_1 and Δ_2 are similar if and only if P_1 and P_2 are in the same orbit under G. Up to scaling, Δ_1 and Δ_2 have the same inradius and perimeter if and only if P_1 and P_2 map to the same point under f.*

Proof. This is obvious. □

To set our strategy for proving Theorem 1.1, note that it asserts that for fixed σ, the infinitely many pairwise nonsimilar triangles $\Delta_n(\sigma)$, with $n \geq 1$, all have the same perimeter $2\sigma(\sigma + 1)$ and inradius $\sigma - 1$. By Lemma 2.1 this is equivalent to the statement that the infinitely many points corresponding to the triples $(a_n(\sigma), b_n(\sigma), c_n(\sigma))$ all map under f to $[\sigma - 1 : \sigma(\sigma + 1)]$, and that they are all in different orbits under G. To prove Theorem 1.1, we will find a suitable infinite collection of curves on X, mapping surjectively to $\mathbb{P}^1$ under f. Those maps will not be surjective on rational points, but for rational σ each of these curves will intersect $f^{-1}([\sigma - 1 : \sigma(\sigma + 1)])$ in a rational point.

Remark 2.2 Since the equation $r^2(x + y + z) = xyz$ is linear in x, we find that X is rational. A parametrization is given by the birational equivalence $\mathbb{P}^2 \dashrightarrow X$, given by

$$\begin{aligned}[r : x : y : z] &= [vw(u - v) : v(uv + w^2) : w^2(u - v) : uv(u - v)], \quad \text{or} \\ [u : v : w] &= [yz : r^2 : yr] = [z(x + y + z) : xz : r(x + y + z)] \\ &= [r(x + y + z) : xr : xy].\end{aligned}$$

3 Elliptic surfaces

In this section we will describe part of the theory of elliptic surfaces. Most of these results can also be found in Shioda's paper [Shi]. During this section, k will denote an algebraically closed field. All varieties, unless stated otherwise, are k-varieties. A variety V over a field l is called smooth if the morphism $V \to \operatorname{Spec} l$ is smooth. We will start with the definition of a lattice. Note that for any abelian groups A and G, a symmetric bilinear map $A \times A \to G$ is called nondegenerate if the induced homomorphism $A \to \operatorname{Hom}(A, G)$ is injective. We do not require a lattice to be definite, only nondegenerate.

Definition 3.1 *A* lattice *is a free $\mathbb{Z}$-module L of finite rank, endowed with a symmetric, bilinear, nondegenerate map $\langle \_\,, \_ \rangle \colon L \times L \to \mathbb{Q}$, called the* pairing *of the lattice. An* integral lattice *is a lattice whose pairing is $\mathbb{Z}$-valued. A lattice L is called* even *if $\langle x, x \rangle \in 2\mathbb{Z}$ for every $x \in L$. A* sublattice *of L is a submodule L' of L, such that the induced bilinear map on L' is nondegenerate. A sublattice L' of L is called* primitive *if L/L' is torsion-free. The positive or negative definiteness* *or signature of a lattice is defined to be that of the vector space $L_{\mathbb{Q}}$ together with the induced pairing.*

Definition 3.2 *The* Gram matrix *of a lattice L with respect to a given basis $x = (x_1, \dots, x_n)$ is $I_x = (\langle x_i, x_j \rangle)_{i,j}$. The* discriminant *of L is defined by* $\operatorname{disc} L = \det I_x$ *for any basis x of L. A lattice L is called* unimodular *if it is integral and* $\operatorname{disc} L = \pm 1$.

Definition 3.3 *A* fibration *of a variety Y* over *a regular integral curve Z over k is a dominant morphism $g \colon Y \to Z$.*

Remark 3.4 If Y is integral in the definition above, then g is flat, see [Ha2], Prop. III.9.7. If also the characteristic of k equals 0 and the singular locus of Y is contained in finitely many fibers, then almost all fibers are nonsingular, see [Ha2], Thm. III.10.7. If Y is projective, then g is surjective, as projective morphisms are closed.

Definition 3.5 *A fibration of a smooth, projective, irreducible surface Y over a smooth, projective, irreducible curve Z is called* relatively minimal *if for every fibration of a smooth, projective, irreducible surface Y' over Z, every Z-birational morphism $Y \to Y'$ is necessarily an isomorphism.*

Theorem 3.6 *Let Y be a smooth, projective, irreducible surface, Z a smooth, projective, irreducible curve, and let $g \colon Y \to Z$ be a fibration such that no fiber contains an exceptional prime divisor E, i.e., a prime divisor with self-intersection number $E^2 = -1$ and $H^1(E, \mathcal{O}_E) = 0$. Then g is a relatively minimal fibration.*

Proof. This is a direct corollary of the Castelnuovo Criterion ([Ch], Thm. 3.1) and the Minimal Models Theorem ([Ch], Thm. 1.2). See also Lichtenbaum [Lic] and Shafarevich [Sha]. □

Definition 3.7 *A fibration is called* elliptic *if all but finitely many fibers are smooth curves of geometric genus* 1.

Theorem 3.8 *Let C be a smooth, irreducible, projective curve of genus $g(C)$ over an algebraically closed field k. Let S be a smooth, irreducible, projective surface over k with Euler characteristic $\chi = \chi(\mathcal{O}_S)$ and let $g \colon S \to C$ be an elliptic fibration that has a section. Then the following are equivalent.*

(i) *The morphism g is a relatively minimal fibration,*

(ii) *There is a divisor L on C of degree χ, such that any canonical divisor K_S on S is linearly equivalent to $g^*(K_C + L)$, where K_C is a canonical divisor on C.*

(iii) *The canonical divisor K_S is algebraically equivalent to $(2g(C) - 2 + \chi)F$, where F is any fiber of g.*

(iv) *The canonical divisor K_S on S is g-nef, i.e., for every irreducible curve D contained in a fiber of g we have $K_S \cdot D \geq 0$.*

Proof. (i) $\Rightarrow$ (ii): By [CD], Prop. 5.1.1, we have $g_*\mathcal{O}_S \cong \mathcal{O}_C$. Under that assumption, an explicit expression for K_S can be given, see [Ko1], § 12, for base fields of characteristic 0, and [BM], § 1, for characteristic $p > 0$. Since g has a section, there are no multiple fibers. In that case, the expression mentioned above implies that K_S is linearly equivalent to $g^*(K_C + L)$ for some divisor L on C of degree χ. (ii) $\Rightarrow$ (iii): The divisor $K_C + L$ is algebraically equivalent to $(2g(C) - 2 + \chi)P$ for any point P, so $g^*(K_C + L)$ is algebraically equivalent to $(2g(C) - 2 + \chi)g^*(P) = (2g(C) - 2 + \chi)F$ for any fiber F. (iii) $\Rightarrow$ (iv): Obvious. (iv) $\Rightarrow$ (i): See [Fr], Prop. 7.10. □

Definition 3.9 *Let C be a smooth, irreducible, projective curve over k. An* elliptic surface over C *is a smooth, irreducible, projective surface S over k together with a relatively minimal elliptic fibration $g\colon S \to C$ that is* **not smooth***, and a section $\mathcal{O}\colon C \to S$ of g.*

Remark 3.10 In order to rephrase what it means for g not to be smooth, note that by [EGA IV(2)], Déf. 6.8.1, a morphism of schemes $g\colon X \to Y$ is smooth if and only if g is flat, g is locally of finite presentation, and for all $y \in Y$ the fiber $X_y = X \times_Y \operatorname{Spec} k(y)$ over the residue field $k(y)$ is geometrically regular. See also [Ha2], Thm. III.10.2.

In the case that g is a fibration of an integral variety X over a smooth, irreducible, projective curve over an algebraically closed field k, it follows from Remark 3.4 that g is flat. As X is noetherian and of finite type over k, it also follows that g is locally of finite presentation. Hence g not being smooth is then equivalent to the existence of a singular fiber.

For the rest of this section, let S be an elliptic surface over a smooth, irreducible, projective curve C over k, fibered by $g\colon S \to C$ with a section $\mathcal{O}$. Let $K = k(C)$ denote the function field of C and let $\eta\colon \operatorname{Spec} K \to C$ be its generic point. Then the generic fiber $E = S \times_C \operatorname{Spec} K$ of g is a curve over K of genus 1. The curve E/K is smooth because g is flat and projective, see [Ha2], exercise III.10.2. The curve E/K is projective because being projective is stable under base extension, see [Ha2], exercise II.4.9. Let ξ denote the natural map $E \to S$.

$$\begin{tikzcd}
E \arrow[r, "\xi"] \arrow[d] & S \arrow[d, "g"] \\
\operatorname{Spec} K \arrow[r, "\eta"'] & C
\end{tikzcd} \tag{2}$$

Lemma 3.11 *Both maps ξ_* and η^* in*

$$E(K) = \operatorname{Hom}_K(\operatorname{Spec} K, E) \xrightarrow{\xi_*} \operatorname{Hom}_C(\operatorname{Spec} K, S) \xleftarrow{\eta^*} \operatorname{Hom}_C(C, S) = S(C)$$

are bijective.

Proof. By the universal property of fibered products, we find that every morphism $\sigma\colon \operatorname{Spec} K \to S$ with $g \circ \sigma = \eta$ comes from a unique section of the morphism $E \to \operatorname{Spec} K$. Hence, the map ξ_* is bijective. As C is a smooth curve and S is projective, any morphism from a dense open subset of C to S extends uniquely to a morphism from C, see [Ha2], Prop. I.6.8. As $\operatorname{Spec} K$ is dense in C, the map η^* is bijective as well. □

Whenever we implicitly identify the two sets $E(K)$ and $S(C)$, it will be done using the bijection $\xi_*^{-1} \circ \eta^*$ of Lemma 3.11. The section $\mathcal{O}$ of g corresponds to a point on E, which we will also denote by $\mathcal{O}$. It gives E the structure of an elliptic curve. This endows $E(K)$ with a group structure, which carries over to $S(C)$, see [Si1], Prop. III.3.4.

Recall that for any proper variety Y over an algebraically closed field, the Néron-Severi group $\operatorname{NS}(Y)$ of Y is the quotient of $\operatorname{Pic} Y$ by the group $\operatorname{Pic}^0 Y$ consisting of all divisor classes algebraically equivalent to 0. For a precise definition of algebraic equivalence, see [Ha2], exc. V.1.7, which is stated only for smooth surfaces, but holds in any dimension, see [SGA 6], Exp. XIII, p. 644, 4.4. We will write $D \sim D'$ and $D \approx D'$ to indicate that two divisors D and D' are linearly and algebraically equivalent respectively. Algebraic equivalence implies numerical equivalence, see [SGA 6], Exp. X, p. 537, Déf. 2.4.1, and p. 546, Cor. 4.5.3. If Y is proper, then $\operatorname{NS}(Y)$ is a finitely generated, abelian group, see [Ha2], exc. V.1.7–8, or [Mi], Thm. V.3.25 for surfaces, or [SGA 6], Exp. XIII, Thm. 5.1 in general. Its rank is called the Picard number of Y. Let $\rho = \operatorname{rk} \operatorname{NS}(S)$ denote the Picard number of the elliptic surface S.

Proposition 3.12 *On S, algebraic equivalence coincides with numerical equivalence. The group $\operatorname{NS}(S)$ is torsion-free. The intersection pairing induces a nondegenerate bilinear pairing on $\operatorname{NS}(S)$, making it into a lattice of signature $(1, \rho - 1)$.*

Proof. The first statement is proven by Shioda in [Shi], Thm. 3.1. It follows immediately that $\operatorname{NS}(S)$ has no torsion and that the bilinear intersection pairing is nondegenerate on $\operatorname{NS}(S)$, see [Shi], Thm. 2.1 or [Ha2], example V.1.9.1. The signature follows from the Hodge Index Theorem ([Ha2], Thm. V.1.9). □

Lemma 3.13 *The induced map $g^*\colon \operatorname{Pic}^0 C \to \operatorname{Pic}^0 S$ is an isomorphism.*

Proof. See [Shi], Thm. 4.1. □

The map ξ induces a homomorphism $\xi^*\colon \operatorname{Pic} S \to \operatorname{Pic} E$. Since $\xi^* \circ g^* = (g \circ \xi)^*$ factors through $\operatorname{Pic}(\operatorname{Spec} K) = 0$, we have an inclusion $g^* \operatorname{Pic}^0 C \subset \ker \xi^*$, so ξ^* factors through $\operatorname{Pic} S / g^* \operatorname{Pic}^0 C$, which is isomorphic to $\operatorname{NS}(S)$ by Lemma 3.13. Let $\varphi\colon \operatorname{NS}(S) \to E(K)$ denote the composition of the induced homomorphism $\operatorname{NS}(S) \to \operatorname{Pic} E$ with the homomorphism $\Sigma\colon \operatorname{Pic} E \to E(K)$, which uses the group law on $E(K)$ to add up all the points of a given divisor, with multiplicities.

$$\begin{tikzcd}
\operatorname{Pic} S \arrow[r] \arrow[d, "\xi^*"'] & \mathrm{NS}(S) \arrow[d, "\varphi"] \arrow[dl] \\
\operatorname{Pic} E \arrow[r, "\Sigma"'] & E(K)
\end{tikzcd}$$

Set $T = \ker \varphi$ and for $v \in C$, let m_v denote the number of irreducible components of the fiber of g at v. Let r denote the rank of the Mordell-Weil group $E(K)$. Finally, for every point $P \in E(K)$, let (P) denote the prime divisor on S that is the image of the section $C \to S$ corresponding to P by Lemma 3.11.

Proposition 3.14 *The homomorphism φ is surjective and maps (P) to P. The group T is a sublattice of $\mathrm{NS}(S)$, generated by $(\mathcal{O})$ and the irreducible components of the singular fibers of g. Its rank equals $\operatorname{rk} T = 2 + \sum_v (m_v - 1)$. We have $\rho = r + 2 + \sum_v (m_v - 1)$.*

Proof. For the first claim, see [Shi], Lemma 5.1. For the description of the kernel T and the fact that it is a lattice, see [Shi], Thm. 1.3. For its rank, see [Shi], Prop. 2.3. The last equality then follows from the exact sequence

$$0 \longrightarrow T \longrightarrow \mathrm{NS}(S) \longrightarrow E(K) \longrightarrow 0. \tag{3}$$

□

Shioda also shows that $\mathrm{NS}(S)$ is the orthogonal direct sum of a negative definite lattice L of rank $\rho - 2$ and the unimodular lattice U of rank 2 generated by $(\mathcal{O})$ and F, where F is any fiber, see [Shi], Thm. 7.5. Since U is contained in $T = \ker \varphi$, it follows from (3) that $E(K)$ is the quotient of the lattice L a sublattice. By general theory of definite lattices, the pairing on L induces a nondegenerate pairing on $E(K)/E(K)_{\mathrm{tors}}$. Shioda gives an explicit formula for the negative of this pairing, which equals the canonical height pairing, see [Shi], Thm. 8.6.

4 Two constructions of elliptic surfaces

In this section we will prove that under mild conditions a fan of hyperplane sections of a degree 3 surface in $\mathbb{P}^3$ gives rise to an elliptic surface. This statement is well known, at least for nonsingular surfaces in characteristic 0, but details such as the existence of singular fibers are often overlooked. Also under mild conditions a base extension of an elliptic surface gives rise again to an elliptic surface. Both statements appear to lack proofs in the literature, so we include them here.

Lemma 4.1 *Any connected, regular variety is integral.*

Proof. Let Z be such a variety. Then Z is reduced as it is regular, so it suffices to show that Z is irreducible. The minimal primes of the local ring of a point on Z correspond to the components it lies on. As a regular local ring has only one minimal prime ideal, we conclude that every point of Z lies on exactly one component. As Z is connected, Z is irreducible. □

Proposition 4.2 *Let k be any field of characteristic not equal to 2 or 3, contained in an algebraically closed field k'. Let X be a projective, normal cubic surface in $\mathbb{P}^3_k$ that is not a cone. Let L be a line that intersects X in three different points M_1, M_2, and M_3. Identify $\mathbb{P}^1$ with the family of hyperplanes in $\mathbb{P}^3$ through L and let $f\colon X \dashrightarrow \mathbb{P}^1$ be the rational map that sends every point of X to the hyperplane it lies in. Let $\pi\colon \widetilde{X} \to X$ be a minimal desingularization of the blow-up of X at the M_i. For $i = 1, 2, 3$, let $\widetilde{M_i}$ denote the exceptional curve above M_i on $\widetilde{X}$. Then $f \circ \pi$ extends to a morphism $\widetilde{f}$. It maps the $\widetilde{M_i}$ isomorphically to $\mathbb{P}^1$, yielding three sections. Together with any of its sections, $\widetilde{f}$ makes $\widetilde{X}_{k'}$ into a rational elliptic surface over $\mathbb{P}^1_{k'}$.*

Proof. Note that if L is defined over k, then so is f. If M_i is a k-point, then the section corresponding to $\widetilde{M_i}$ is defined over k as well. All other statements are geometric, so without loss of generality we will assume that $k = k'$.

The rational map f is defined everywhere, except at the M_i, whence the composition $f \circ \pi$ is well-defined outside the $\widetilde{M_i}$. Any point P on $\widetilde{M_i}$ corresponds to a direction at M_i on X. Since L intersects X in three different points and the total intersection $L \cdot X$ has degree 3 by Bézout's Theorem, it follows that the M_i are nonsingular points and that L is not tangent to X, so each direction at M_i is cut out by a unique plane through L. The map $f \circ \pi$ extends to a morphism $\widetilde{f}\colon \widetilde{X} \to \mathbb{P}^1$ by sending $P \in \widetilde{M_i}$ to that plane that cuts out the direction at M_i corresponding to P. Thus, it induces an isomorphism from the $\widetilde{M_i}$ to $\mathbb{P}^1$.

Every normal cubic surface in $\mathbb{P}^3$ is either a cone or an anticanonical Del Pezzo surface, see [CD], Prop. 0.3.3 and page 57. Thus, X is an anticanonical Del Pezzo surface of degree 3, which means that a minimal desingularization X' of X is isomorphic to $\mathbb{P}^2$ blown up at six points (possibly infinitely near), see [CD], §0.3. As $\widetilde{X}$ is the blow-up of X' in the points corresponding to the M_i, we obtain a birational morphism $\rho\colon \widetilde{X} \to \mathbb{P}^2$, which consists of blowing up the 9 base points of the linear system corresponding to $\widetilde{f} \circ \rho^{-1}\colon \mathbb{P}^2 \dashrightarrow \mathbb{P}^1$. This shows that $\widetilde{X}$ is rational. Also, as the 9 base points lie on a plane cubic, and the anticanonical divisor $-K_{\widetilde{X}}$ on $\widetilde{X}$ is the inverse image of any cubic under ρ minus the 9 exceptional curves, see [Ha2], Prop. V.3.3, we find that $-K_{\widetilde{X}}$ is the strict transform of any cubic through these 9 base points. This implies that $-K_{\widetilde{X}}$ is linearly equivalent to any fiber F, so $K_{\widetilde{X}}$ is nef. By construction, $\widetilde{X}$ is smooth. It is irreducible because X is and $\pi\colon \widetilde{X} \to X$ is birational.

Note that if a hyperplane H through L does not contain any singular points of X, then the fiber of $\widetilde{f}$ above H is isomorphic to $H \cap X$. Here the missing points M_i in $f^{-1}(H) = (H \cap X) \setminus \{M_1, M_2, M_3\}$ are filled in by the appropriate points on $\widetilde{M_i}$. This shows that almost all fibers are plane cubic curves, and thus geometrically connected. Therefore, the generic fiber $E = \widetilde{X} \times_{\mathbb{P}^1} \operatorname{Spec} k(t)$ above the generic point $\eta : \operatorname{Spec} k(t) \to \mathbb{P}^1$ of $\mathbb{P}^1$ is geometrically connected as well. The local ring at a point P on the generic fiber E is isomorphic to the local ring on $\widetilde{X}$ at the generic point of the curve on $\widetilde{X}$ corresponding to P. As $\widetilde{X}$ is regular, we conclude that E is regular. As separable extensions preserve regularity (see [EGA IV(2)], Prop. 6.7.4), we find that $E_{k(t)^{\mathrm{sep}}}$ is regular, where $k(t)^{\mathrm{sep}}$ is the separable closure of $k(t)$. As $E_{k(t)^{\mathrm{sep}}}$ is connected as well, it is integral by Lemma 4.1, whence irreducible. Over a separably closed field, irreducibility implies geometric irreducibility, see [EGA IV(2)], Prop. 4.5.9. Therefore E is geometrically irreducible. Thus, the composition of rational maps $\widetilde{f} \circ \rho^{-1}$ is given by a pencil of plane cubic curves, whose generic member is geometrically irreducible. By [CD], Prop. 5.6.1, this implies that a minimal resolution of the indeterminacy points of $\widetilde{f} \circ \rho^{-1}$ is an elliptic fibration. This uses the fact that the characteristic is at least 5. As $\widetilde{f}\colon \widetilde{X} \to \mathbb{P}^1$ is such a resolution and it is minimal by Theorem 3.8, we find that $\widetilde{f}\colon \widetilde{X} \to \mathbb{P}^1$ is a relatively minimal elliptic fibration.

Finally we show that $\widetilde{f}$ is not smooth. By Remark 3.10, it suffices to prove that there exists a singular fiber. As for almost all planes H through L the fiber $\widetilde{X}_H$ is isomorphic to the plane curve $X \cap H$, it is connected for all but finitely many H. Since $\widetilde{f}$ is flat (see Remark 3.4), it follows from the principle of connectedness (see [Ha2], exc. III.11.4) that the fiber $\widetilde{X}_H$ is connected for all H. If X contains a singular point, then the fiber $\widetilde{X}_H$ of $\widetilde{f}$ above the plane H that it lies in contains an exceptional curve, so it is reducible and connected, and thus singular by Lemma 4.1. Hence, we may assume that X is nonsingular. Then there is a well-defined morphism $d\colon X \to \check{\mathbb{P}}^3$, where $\check{\mathbb{P}}^3$ is the dual of $\mathbb{P}^3$, sending a point $P \in X$ to the plane tangent to X at P. The planes through L correspond to the points on a line in $\check{\mathbb{P}}^3$ that intersects the dual $d(X)$ of X in at least one point, say corresponding to the plane H. Then the fiber $\widetilde{X}_H = X \cap H$ of $\widetilde{f}$ above H is singular at the point where H is tangent to X. □

Remark 4.3 If L intersects X in one of its singular points, then one could still define a fibration $\widetilde{X} \to \mathbb{P}^1$ in the same way as in Proposition 4.2. For almost all hyperplanes H the fiber above H will be the normalization of the singular cubic curve $H \cap X$. Hence this will not be an elliptic fibration.

Remark 4.4 In characteristic 3, all fibers might be singular, as is the case when X is given by $y^2z + yz^2 + wxy + wxz + xz^2 + wy^2 = 0$ and L is given by $x = w = 0$. The intersection of X with the plane H_t given by $w = tx$ is singular at the point $[x : y : z : w] = [1 : t^{1/3} : t^{2/3} : t]$ on the twisted cubic curve in $\mathbb{P}^3$. The plane H_t is tangent to X at that point. The only singular points of X are three ordinary double points at $[1 : 0 : 0 : 0]$, $[0 : 0 : 0 : 1]$, and $[1 : 1 : 1 : 1]$.

In characteristic 2, we can also get all fibers to be singular, as one easily checks in case X is given by $x^3 + x^2z + x^2w + y^3 + yzw = 0$ and L is given by $w = z = 0$. The only singular points on X are the ordinary double points $[0 : 0 : 0 : 1]$ and $[0 : 0 : 1 : 0]$.

In the proof of Proposition 4.2 the fact that the characteristic of k is not equal to 2 or 3 is only needed to show that almost all fibers are nonsingular. Hence the conclusion of the proposition is also true in characteristic 2 and 3 if we add to the hypotheses that almost all planes through L are not tangent to X. By Bertini's Theorem, the set of planes that intersect X in a nonsingular curve is open (see [Ha2], Thm. II.8.18), so it suffices to require that there is at least one plane through L that is not tangent to X.

Remark 4.5 The singular points on X as in Proposition 4.2 can be used to find sections of $\widetilde{f}$. If X has two singular points P and Q, then the line l through P and Q lies on X, for if it did not, it would have intersection multiplicity at least 4 with X, but by Bézout's Theorem the intersection multiplicity should be 3. Therefore, either l intersects L and thus l is contained in the fiber above the plane that L, P, and Q all lie in, or l gives a section of $\widetilde{f}$.

The next proposition describes how to construct an elliptic surface by base extension of another elliptic surface. This construction will also be used in the proof of Theorem 1.1.

Proposition 4.6 *Let S be an elliptic surface over a smooth, irreducible, projective curve C over an algebraically closed field k, with fibration g and section $\mathcal{O}$ of g. Let $\gamma\colon C' \to C$ be a nonconstant map of curves from a smooth, irreducible, projective curve C', which is unramified above those points in C where g has singular fibers. Put $S' = S \times_C C'$, let g' be the projection $S' \to C'$, and let $\mathcal{O}'\colon C' \to S'$ denote the morphism induced by the identity on C' and the composition $\mathcal{O} \circ \gamma$. Then $\mathcal{O}'$ is a section of g' and they make S' into an elliptic surface over C'. The Euler characteristics $\chi_S = \chi(\mathcal{O}_S)$ and $\chi_{S'} = \chi(\mathcal{O}_{S'})$ are related by $\chi_{S'} = (\deg \gamma)\chi_S$.*

$$\begin{tikzcd}
S' \arrow[r] \arrow[d, "g'"] & S \arrow[d, "g"] \\
C' \arrow[r, "\gamma"'] \arrow[u, bend left, "\mathcal{O}'"] & C \arrow[u, bend left, "\mathcal{O}"]
\end{tikzcd}$$

Proof. Since projective morphisms are stable under base extension (see [Ha2], exc. II.4.9), we find that S' is projective over C', which is projective over $\operatorname{Spec} k$, so S' is projective. The composition $g' \circ \mathcal{O}'$ is by construction the identity on C', so $\mathcal{O}'$ is a section of g'.

As k is algebraically closed, the residue field $k(x)$ of a closed point $x \in C'$ is isomorphic to the residue field $k(\gamma(x))$. Hence the fiber above x is isomorphic to the fiber above $\gamma(x)$, as we have

$$\operatorname{Spec} k(x) \times_{C'} S' \cong \operatorname{Spec} k(x) \times_{C'} C' \times_C S \cong \operatorname{Spec} k(x) \times_C S \cong \operatorname{Spec} k(\gamma(x)) \times_C S.$$

Therefore, as for g, all fibers of g' are connected. As g is elliptic, all but finitely many fibers of g' will be smooth curves of genus 1. Since g has a singular fiber, so does g'.

Since g is flat and locally of finite presentation (S is noetherian), g is universally open by [EGA IV(2)], Thm. 2.4.6. Let $V \subset C$ denote the subset of points $v \in C$ such that $g^{-1}(v)$ is nonsingular. Then $g^{-1}(V)$ is a dense open subset of S and $g|_{g^{-1}(V)}$ is universally open, surjective, and all fibers of $g|_{g^{-1}(V)}$ are geometrically irreducible. Because $\gamma^{-1}(V)$ is a dense open subset of the irreducible curve C', it is also irreducible, so by [EGA IV(2)], Prop. 4.5.7, the fibered product $\gamma^{-1}(V) \times_V g^{-1}(V)$ is irreducible. As this is a dense open subset of the fibered product $S = C' \times_C S$, we conclude that S' is irreducible as well.

To prove that S' is smooth, set $h = \gamma \circ g'$. Note that $g|_{g^{-1}(V)}$ is smooth by Remark 3.10. Let $U \subset C$ be the largest subset such that $\gamma|_{\gamma^{-1}(U)}$ is unramified, whence smooth. By assumption we have $U \cup V = C$. As smooth morphisms are stable under base extension and composition (see [Ha2], Prop. II.10.1), we find first that $h^{-1}(U) = g^{-1}(U) \times_U \gamma^{-1}(U)$ is smooth over $g^{-1}(U) \subset S$. As S is smooth over k and $g^{-1}(U)$ is open in S, we conclude that $h^{-1}(U)$ is smooth over k. Similarly, $h^{-1}(V)$ is smooth over k, whence so is their union S'.

To prove that g' is relatively minimal, it suffices by Theorem 3.6 to show that no fiber S'_x above $x \in C'$ contains an exceptional prime divisor. Let D' be an irreducible component of the fiber S'_x, mapping isomorphically to the irreducible component D of $S_{\gamma(x)} \cong S'_x$ under the induced morphism $\gamma' \colon S' \to S$. Suppose that D' is an exceptional divisor, i.e., $D' \cong \mathbb{P}^1$ and $D'^2 = -1$. If $\gamma(x)$ is contained in V, then the fiber $S_{\gamma(x)}$, and hence S'_x, is smooth. As all fibers are connected, S'_x is then irreducible, so $D' = S'_x$. Since any fiber is numerically equivalent to any other, this implies $D'^2 = 0$, contradiction. Therefore, we may assume that $\gamma(x) \notin V$, so $\gamma(x) \in U$ and $D' \subset h^{-1}(U)$. As étale morphisms are stable under base extension and $\gamma|_{\gamma^{-1}(U)}$ is étale, we find that $\gamma'|_{h^{-1}(U)}$ is étale.

For any morphism of schemes $\varphi \colon X \to Y$, let $\Omega_{X/Y}$ denote the sheaf of relative differentials of X over Y. If X is a nonsingular variety over k, then let $\mathcal{T}_X$ denote the tangent sheaf $\mathcal{H}om(\Omega_{X/k}, \mathcal{O}_X)$. For any nonsingular subvariety $Z \subset X$, let $\mathcal{N}_{Z/X}$ denote the normal sheaf of Z in X, see [Ha2], § II.8.

We will show that the self-intersection number $D'^2 = \deg \mathcal{N}_{D'/S'}$ on S' (see [Ha2], example V.1.4.1) is equal to the self-intersection number $D^2 = \deg \mathcal{N}_{D/S}$. Since D is not an exceptional curve, that implies that $D'^2 \neq -1$, which is a contradiction. As γ' induces an isomorphism from D' to D, it suffices to show that $\mathcal{N}_{D'/S'}$ is isomorphic to $\gamma'^*\mathcal{N}_{D/S}$.

There is an exact sequence

$$0 \to \mathcal{T}_{D'} \to \mathcal{T}_{S'} \otimes \mathcal{O}_{D'} \to \mathcal{N}_{D'/S'} \to 0 \tag{4}$$

(see [Ha2], p. 182) and, because $\gamma'|_{D'}$ is an isomorphism, by applying the functor $(\gamma'|_{D'})^*$ to the similar sequence for D in S we also get the exact sequence

$$0 \to \gamma'^*\mathcal{T}_D \to \gamma'^*(\mathcal{T}_S \otimes \mathcal{O}_D) \to \gamma'^*\mathcal{N}_{D/S} \to 0. \tag{5}$$

The natural morphisms $\mathcal{T}_{D'} \to \gamma'^*\mathcal{T}_D$ and $\mathcal{T}_{S'} \otimes \mathcal{O}_{D'} \to \gamma'^*(\mathcal{T}_S \otimes \mathcal{O}_D)$ induce a morphism between the short exact sequences (4) and (5). To prove that the last morphism $\mathcal{N}_{D'/S'} \to \gamma'^*\mathcal{N}_{D/S}$ is an isomorphism, it suffices by the snake lemma to prove that the first two are. Clearly, $\mathcal{T}_{D'} \to \gamma'^*\mathcal{T}_D$ is an isomorphism of sheaves on D', as $\gamma'|_{D'}$ is an isomorphism. To show that

$$\mathcal{T}_{S'} \otimes \mathcal{O}_{D'} \to \gamma'^*(\mathcal{T}_S \otimes \mathcal{O}_D) \cong \gamma'^*\mathcal{T}_S \otimes \gamma'^*\mathcal{O}_D \cong \gamma'^*\mathcal{T}_S \otimes \mathcal{O}_{D'}$$

is an isomorphism, it suffices to show that $\mathcal{T}_{S'} \to \gamma'^*\mathcal{T}_S$ is an isomorphism on the open subset $h^{-1}(U) \subset S'$ containing D'. This is true, as by [SGA 1], Exposé II, Cor. 4.6, a morphism $f\colon X \to Y$ of smooth T-schemes is étale if and only if the morphism $f^*\Omega_{Y/T} \to \Omega_{X/T}$ is an isomorphism. Taking the dual gives what we need, if we choose $T = \operatorname{Spec} k$, and $f = \gamma'|_{h^{-1}(U)}$.

For the last statement we will use that by [Fr], Cor. 7.16 and p. 178, we have

$$12\chi_S = \sum_F e(F), \tag{6}$$

where the sum is taken over all singular fibers F of g and $e(F)$ is the Euler characteristic of F. As the morphism γ is unramified above the points of C where g has singular fibers, it follows that the singular fibers of g' come in n-tuples, with $n = \deg \gamma$. Each n-tuple consists of n copies of one of the singular fibers of g. From (6) and its analogue for S' we conclude that $\chi_{S'} = n\chi_S$. □

5 Proof of the main theorem

Let X, G, and $f\colon X \dashrightarrow \mathbb{P}^1$ be as in section 2. The rational map f is defined everywhere, except at the three intersection points $M_1 = [0:0:1:-1]$, $M_2 = [0:1:0:-1]$, and $M_3 = [0:1:-1:0]$ of X with the line L given by $r = x+y+z = 0$. A straightforward computation shows that X has exactly three singular points $N_1 = [0:1:0:0]$, $N_2 = [0:0:1:0]$, and $N_3 = [0:0:0:1]$. They are all ordinary double points, forming a full orbit under G, and all mapping to $[0:1]$ under f. Let $\pi\colon \widetilde{X} \to X$ be the blow-up of X at the six points M_i and N_i. Let $\widetilde{M_i}$ and $\widetilde{N}_i$ denote the exceptional curves above M_i and N_i respectively.

Proposition 5.1 *The surface $\widetilde{X}$ is smooth. The rational map $f \circ \pi$ extends to a morphism $\widetilde{f}\colon \widetilde{X} \to \mathbb{P}^1$. It maps the $\widetilde{M_i}$ isomorphically to $\mathbb{P}^1$ and together with the section $\mathcal{O} = \widetilde{f}|_{\widetilde{M_3}}^{-1}$ it makes $\widetilde{X}_k$ into an elliptic surface over $\mathbb{P}^1$ for any algebraically closed field k of characteristic 0.*

Proof. Ordinary double points are resolved by blowing up once, see [Ha2], exc. I.5.7. Hence $\widetilde{X}$ is the minimal desingularization of X blown up at the M_i. The rational map f sends all points of X (except for the M_i) in the plane through L given by $t_1 r = t_0(x+y+z)$ to the point $[t_0 : t_1]$. Hence this proposition follows from Proposition 4.2. □

Remark 5.2 Proposition 4.2 is useful for future reference, but in this specific case it would have been easier to check by hand that $\widetilde{f}$ makes $\widetilde{X}_k$ into an elliptic surface over $\mathbb{P}^1$. From Theorem 3.6 it follows that, in order to prove that $\widetilde{f}$ is a minimal fibration, it suffices to check that no reducible fiber contains a rational curve with self-intersection -1. As the only singular points of X lie above $[0:1] \in \mathbb{P}^1$, it follows that for all $\tau \neq 0, \infty$, the fiber $\widetilde{X}_\tau$ above $[\tau : 1]$ is given by the intersection of X with the plane given by $r = \tau(x+y+z)$. Hence for $\tau \neq 0, \infty$, the fiber is isomorphic to the plane curve given by $\tau^2(x+y+z)^3 = xyz$, which is nonsingular as long as $\tau(27\tau^2-1) \neq 0$. For τ with $27\tau^2 = 1$ we get a nodal curve, whence a fiber of type I_1, following the Kodaira-Néron classification of special fibers, see [Si2], IV.8 and [Ko2]. At $\tau = 0$ and $\tau = \infty$ one checks that the fibers are of type I_6 and IV respectively. None of these fibers contains an exceptional curve.

There is another easy way of showing that $\widetilde{f}$ makes $\widetilde{X}_k$ into an elliptic surface over $\mathbb{P}^1$. Through the birational map of Remark 2.2, the rational map $f \colon X \dashrightarrow \mathbb{P}^1$ gives a pencil of cubics in $\mathbb{P}^2$, generated by $vw(u-v)$ and $u(uv+w^2)$. The base points of this pencil are $[u:v:w] = [1:0:0]$, $[0:1:0]$, $[0:0:1]$, $[1:1:i]$, $[1:1:-i]$, the point P infinitely near $[1:0:0]$, corresponding to the direction of $v=0$, and three points infinitely near $[0:0:1]$, $[0:1:0]$, and P. Blowing the first six of these points gives gives the cubic surface whose embedding in $\mathbb{P}^3$ is X, which is singular because these six points are not in general position. On X the lines given by $u=v$ and $v=0$ and the exceptional curve above $[1:0:0]$ are blown down to give the singular points $[0:1:0:0]$, $[0:0:1:0]$, and $[0:0:0:1]$. The points where f is not defined correspond to the remaining three of the nine base points. This implies that $\widetilde{X}$ is the minimal resolution of the base points of the pencil of cubics in $\mathbb{P}^2$. It is therefore a minimal elliptic fibration by [CD], Prop. 5.6.1. It is worth noting that geometrically (over $\mathbb{Q}(i)$) the surface $\widetilde{X}$ is isomorphic to the minimal resolution of the pencil $\mathcal{A}(1)$ studied in [SB]. The fiber at 0 is given by the three lines determined by $vw(u-v) = 0$ together with the three exceptional curves above the points P, $[1:0:0]$, and $[0:0:1]$. This gives a fiber of type I_6. The fiber at ∞ consists of the line and the conic determined by $u(uv+w^2) = 0$ and the exceptional curve above the point $[0:1:0]$. This is a fiber of type IV.

Remark 5.3 From the previous remark, it follows that the fiber of $\widetilde{f}$ above every *rational* point $[\tau:1] \in \mathbb{P}^1$ with $\tau > 0$, is a curve of genus 1, which can not be rationally parametrized. Therefore, there is no rational parametrization of infinitely many rational triangles, all having the same area and the same perimeter.

Remark 5.4 Later we will see a Weierstrass form for the generic fiber of $\widetilde{f}$. Based on that, Tate's algorithm (see [Si2], IV.9 and [Ta3]) describes the special fibers of a minimal proper regular model. They coincide with the fibers described in Remark 5.2, which gives another proof of the fact that $\widetilde{f}$ is relatively minimal.

Let E denote the generic fiber of $\widetilde{f}$, an elliptic curve over $k(\mathbb{P}^1) \cong \mathbb{Q}(t)$. By Lemma 3.11 we can identify the sets $\widetilde{X}(\mathbb{P}^1)$ and $E(k(\mathbb{P}^1))$. The curve E is isomorphic to the plane curve in $\mathbb{P}^2_{\mathbb{Q}(t)}$ given by

$$t^2(x+y+z)^3 = xyz. \tag{7}$$

The origin $\mathcal{O} = \widetilde{M_3}$ then has coordinates $[x : y : z] = [1 : -1 : 0]$. Let P denote the section $\widetilde{M_1} = [0 : 1 : -1]$. A standard computation shows that the $\widetilde{M_i}$ correspond with inflection points. As they all lie on the line given by $x + y + z = 0$, we find that P has order 3 and $2P = \widetilde{M_2} = [1 : 0 : -1]$. This also follows from the following lemma, which gives a different interpretation of the action of G.

Lemma 5.5 *The automorphism $\widetilde{X} \to \widetilde{X}$ induced by the 3-cycle $(x\,y\,z)$ on the coordinates of X corresponds with translation by P on each nonsingular fiber and on the generic fiber of $\widetilde{f}$. Similarly, the automorphism induced by $(x\,y)$ corresponds with multiplication by -1.*

Proof. Let $\mathrm{Aut}\,(E)$ be the group of all automorphisms of the generic fiber E and let $\mathrm{Aut}\,(E, \mathcal{O})$ be the subgroup of those automorphisms that fix the point $\mathcal{O}$. Then $\mathrm{Aut}\,(E)$ is isomorphic to the semi-direct product $E(\mathbb{Q}(t)) \ltimes \mathrm{Aut}\,(E, \mathcal{O})$ of the group of translations, isomorphic to $E(\mathbb{Q}(t))$, and the group $\mathrm{Aut}\,(E, \mathcal{O})$. Consider the composition

$$S_3 = G \to \mathrm{Aut}\,(E) \cong E(\mathbb{Q}(t)) \ltimes \mathrm{Aut}\,(E, \mathcal{O}) \to \mathrm{Aut}\,(E, \mathcal{O}).$$

As the automorphism group $\mathrm{Aut}\,(E, \mathcal{O})$ is abelian over a field of characteristic 0, we find that the commutator subgroup A_3 of S_3 is contained in the kernel of this composition. We conclude that the automorphism φ induced by $(x\,y\,z)$ is a translation by $\varphi(\mathcal{O}) = P$. Hence $\varphi = T_P$ on E. As E is dense in $\widetilde{X}$, we find $\varphi = T_P$ on $\widetilde{X}$, see [Ha2], exc. II.4.2. Let $\mathrm{End}\,(E, \mathcal{O})$ denote the ring of all endomorphisms of E that fix $\mathcal{O}$. The automorphism ψ induced by $(x\,y)$ fixes $\mathcal{O}$, so we have $\psi \in \mathrm{Aut}\,(E, \mathcal{O}) \subset \mathrm{End}\,(E, \mathcal{O})$. As the endomorphism ring of an elliptic curve over a field of characteristic 0 is a commutative integral domain, and we have $\psi^2 = 1$ and $\psi \neq 1$, we find $\psi = [-1]$. □

As mentioned before, we want infinitely many τ for which the fiber X_τ above $[\tau : 1]$ has infinitely many rational points $[r_i : x_i : y_i : z_i]$ with x_i/r_i, y_i/r_i, $z_i/r_i > 0$, and all in different orbits under G. If the Mordell-Weil rank of $E(\mathbb{Q}(t)) \cong \widetilde{X}(\mathbb{P}^1)$ had been positive, we might have been able to find infinitely many such points for almost all rational τ satisfying some inequalities. Unfortunately, the next theorem tells us that this is not the case.

Theorem 5.6 *The Mordell-Weil group $E(\mathbb{C}(t))$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. It is generated by the 3-torsion point P and the point Q given by $[r : x : y : z] = [t : it : -it : 1]$. The Mordell-Weil group $E(\mathbb{R}(t))$ is equal to $\langle P \rangle \cong \mathbb{Z}/3\mathbb{Z}$.*

Proof. As $\widetilde{X}$ is rational, the Néron-Severi group $\mathrm{NS}(\widetilde{X}_{\mathbb{C}})$ is a unimodular lattice of rank 10, see [Shi], Lemma 10.1. Let $T \subset \mathrm{NS}(\widetilde{X}_{\mathbb{C}})$ be as in Proposition 3.14. From Remark 5.2 and Proposition 3.14, we find that T has rank $2 + (6-1) + (3-1) + (1-1) + (1-1) = 9$ and we can find explicit generators. Consider the lattice $T + \langle (P), (Q) \rangle$. Computing the explicit intersections of our generators, we find that the lattice $T + \langle (P), (Q) \rangle$ has rank 10, and thus it has finite index in $\mathrm{NS}(\widetilde{X}_{\mathbb{C}})$. Also, it is already unimodular, so it is equal to $\mathrm{NS}(\widetilde{X}_{\mathbb{C}})$. Hence, $E(\mathbb{C}(t))$ is generated by P and Q and has rank 1.

Complex conjugation on Q permutes the x- and y-coordinates, so by Lemma 5.5 we find $\overline{Q} = -Q$ in $E(\mathbb{C}(t))$. If $mQ + nP$ is real for some integers m, n, then so is mQ and hence $mQ = m\overline{Q} = -mQ$, so $2mQ = 0$. Since Q has infinite order, we conclude that $m = 0$, so $E(\mathbb{R}(t)) = \langle P \rangle$. □

Remark 5.7 There is another way to prove that P and Q generate the full Mordell-Weil group. From the existence of a singular fiber of type IV, which gives additive reduction and three components in the reduction, one immediately concludes (as the characteristic is different from 3) that the torsion group has order at most 3, so it is generated by P. As the Néron-Severi group has rank 10 and the sublattice T as in Proposition 3.14 has rank 9, the rank of the Mordell-Weil group is equal to 1 by Proposition 3.14. This implies that the group generated by P and Q has finite index in the Mordell-Weil group. Using Shioda's explicit formula for the height pairing, see [Shi], Thm. 8.6, one can show that the index equals 1.

To find more curves over $\mathbb{Q}$, we will apply a base change to our base curve $\mathbb{P}^1$ by a rational curve on $\widetilde{X}$. As we have a parametrization of X, it is easy to find such a curve. Taking $u = s$ and $v = w = 1$ in the parametrization of Remark 2.2, we find a curve C on X parametrized by

$$\beta \colon \mathbb{P}^1 \to C, \quad [s:1] \mapsto [r:x:y:z] = [s-1 : s+1 : s-1 : s(s-1)].$$

We will denote its strict transform on $\widetilde{X}$ by C as well. The map $\widetilde{f}$ induces a 2-1 map from C to $\mathbb{P}^1$. The composition $\widetilde{f} \circ \beta$ is given by $[s:1] \mapsto [s-1 : s(s+1)]$. Hence, if we identify the function field $K = k(C)$ of C with $\mathbb{Q}(s)$, then the field extension $K/k(\mathbb{P}^1)$ is given by $\mathbb{Q}(t) \hookrightarrow \mathbb{Q}(s)$, $t \mapsto (s-1)s^{-1}(s+1)^{-1}$. Throughout the rest of this section, as in Theorem 1.1 and Remarks 5.2 and 5.3, one should think of σ and τ as specific values for the indeterminates s and t respectively.

Let Y denote the fibered product $\widetilde{X} \times_{\mathbb{P}^1} C$, let δ denote the projection $Y \to \widetilde{X}$, and let g denote the projection $Y \to C$. The generic fiber of g is isomorphic to $E_K = E \times_{k(\mathbb{P}^1)} K$. The identity on C and the composition $\mathcal{O} \circ \widetilde{f}|_C \colon C \to \widetilde{X}$ together induce a section $C \to Y$ of g, which we will also denote by $\mathcal{O}$. The closed immersion $C \to \widetilde{X}$ and the identity on C together induce a section of g which we will denote by R.

$$\begin{tikzcd}
& Y \arrow[r, "\delta"] \arrow[dd, "g"] & \widetilde{X} \arrow[dd, "\widetilde{f}"] \arrow[dr, "\pi"] & \\
& & & X \arrow[dl, dashed, "f"] \\
\mathbb{P}^1 \arrow[r, "\cong", "\beta"'] & C \arrow[uu, bend left, "R"] \arrow[uur, hook] \arrow[r, "\widetilde{f}|_C"'] & \mathbb{P}^1 &
\end{tikzcd}$$

Proposition 5.8 *The fibration g and its section $\mathcal{O}$ make Y_k into an elliptic surface over C_k for any algebraically closed field k of characteristic* 0.

Proof. One easily checks that $\widetilde{f}|_C \colon C \to \mathbb{P}^1$ is unramified at the points of $\mathbb{P}^1$ where $\widetilde{f}$ has singular fibers. Hence, this proposition follows immediately from Proposition 4.6 and Proposition 5.1. □

From (7) we find that E_K is isomorphic to the plane cubic over K given by

$$(s-1)^2(x+y+z)^3 = s^2(s+1)^2xyz.$$

The linear transformation

$$p = -4(s-1)^2(x+y)z^{-1}, \qquad q = 4(s-1)^2s(s+1)(x-y)z^{-1}, \tag{8}$$

or, equivalently,

$$\begin{aligned} x &= -s(s+1)p + q, \\ y &= -s(s+1)p - q, \\ z &= 8(s-1)^2s(s+1), \end{aligned} \tag{9}$$

gives the Weierstrass equation

$$q^2 = (p-4(s-1)^2)^3 + s^2(s+1)^2p^2 = F(s,p) \tag{10}$$

with

$$\begin{aligned} j = j(E_K) = j(E) &= \frac{(24t^2-1)^3}{t^6(27t^2-1)}, \\ \Delta = 2^{12}&(s-1)^6s^4(s+1)^4(s^4+2s^3-26s^2+54s-27). \end{aligned} \tag{11}$$

The Weierstrass coordinates of P and R are given by

$$\begin{aligned} &(p_P, q_P) = (4(s-1)^2, 4s(s+1)(s-1)^2) \qquad \text{and} \\ &(p_R, q_R) = (8-8s, 8s^2-8). \end{aligned}$$

Proposition 5.9 *The section R has infinite order in the group $Y(C) \cong E_K(K)$.*

Proof. The p-coordinate of $2R+P$ equals $4(s^4-6s^3+10s^2-2s+1)(s-1)^{-2}$, so $2R+P$ is contained in the kernel of reduction at $s-1$. In characteristic 0 the kernel of reduction has no nontrivial torsion (see [Si1], Prop. VII.3.1), so we find that $2R+P$ has infinite order, and thus so does R. □

For every integer $n \geq 1$, let $\gamma_n \colon \mathbb{P}^1 \to X$ denote the composition

$$\mathbb{P}^1 \xrightarrow{\beta} C \xrightarrow{(2n-1)R} Y \xrightarrow{\delta} \widetilde{X} \xrightarrow{\pi} X. \tag{12}$$

Theorem 1.1 will follow from the following proposition.

Proposition 5.10 *Let $\sigma > 1$ be a real number. For every integer $n \geq 1$, let r_n, x_n, y_n, and z_n be such that $\gamma_n([\sigma : 1]) = [r_n : x_n : y_n : z_n]$ and set*

$$a_n = \frac{(\sigma-1)(y_n+z_n)}{r_n}, \quad b_n = \frac{(\sigma-1)(x_n+z_n)}{r_n}, \quad c_n = \frac{(\sigma-1)(x_n+y_n)}{r_n}.$$

Then for every $n \geq 1$ there is a triangle Δ_n with sides a_n, b_n, c_n, perimeter $2\sigma(\sigma+1)$, inradius $\sigma-1$, and area $\sigma(\sigma^2-1)$. If σ is rational, then the triangles Δ_n are pairwise nonsimilar.

Proof. Let a real number $\sigma > 1$ be given and set $c = \beta([\sigma : 1]) \in C$. Then for $\tau = (\sigma-1)\sigma^{-1}(\sigma+1)^{-1} > 0$ we have $\widetilde{f}|_C(c) = [\tau : 1]$, so the fiber Y_c is isomorphic to the fiber $\widetilde{X}_\tau$ of $\widetilde{f}$ above $[\tau : 1]$. The roots of Δ in (11) are at most 1, so this fiber is nonsingular. By Remark 5.2, it is isomorphic to the intersection E_τ of X with the hyperplane given by $r = \tau(x+y+z)$. This intersection E_τ can be given the structure of an elliptic curve with M_3 as origin. The specialization map $Y(C) \to Y_c(\mathbb{Q}) \colon S \mapsto S \cap Y_c = S(c)$ induces a homomorphism $\psi \colon Y(C) \to E_\tau \subset X$ sending a section S of g to $\pi(\delta(S(c)))$. Set $\Theta_n = \gamma_n([\sigma : 1]) \in X = [r_n : x_n : y_n : z_n]$. Then we have $\Theta_n = \psi((2n-1)R) \in E_\tau$, so on E_τ we get $\Theta_n = (2n-1)\Theta_1$. The elliptic curve E_τ has a Weierstrass model $q^2 = F(\sigma, p)$, see (10). For $n \geq 1$, let (p_n, q_n) denote the Weierstrass coordinates of Θ_n, so $(p_1, q_1) = (8-8\sigma, 8\sigma^2-8)$.

Note that $F(\sigma, 0) = -64(\sigma-1)^6 < 0$, but for $p_1 = 8-8\sigma < 0$ we have $F(\sigma, p_1) = q_1^2 > 0$. We conclude that for any real point on E_τ with Weierstrass coordinates (p, q), the condition $p < 0$ is equivalent to the point lying on the real connected component of E_τ that does not contain $\mathcal{O}$. Since Θ_1 lies on this component, so do all its odd multiples Θ_n.

If $\Theta_n = M_i$ for $i = 1, 2$, or 3, then $3\Theta_n = \mathcal{O}$, which contradicts the fact that Θ_n lies on the real component of E_τ that does not contain $\mathcal{O}$. Hence f is well-defined at Θ_n and from $[r_n : x_n+y_n+z_n] = f(\Theta_n) = [\tau : 1]$, with $\tau > 0$, we find $r_n \neq 0$ and $x_n + y_n + z_n \neq 0$, whence $x_n y_n z_n \neq 0$. To make computations easier, we may assume $z_n = 8(\sigma-1)^2\sigma(\sigma+1) > 0$. As Θ_n lies on the real connected component that does not contain $\mathcal{O}$, we have $p_n < 0$ and therefore also $p_n < 4(\sigma-1)^2$. That implies

$$(\sigma(\sigma+1)p_n)^2 = q_n^2 - (p_n - 4(\sigma-1)^2)^3 > q_n^2$$

and combined with $p_n < 0$ this gives $-\sigma(\sigma+1)p_n > |q_n|$. By (9) we get

$$\begin{aligned} x_n &= -\sigma(\sigma+1)p_n + q_n > 0, \\ y_n &= -\sigma(\sigma+1)p_n - q_n > 0. \end{aligned}$$

From $r_n = \tau(x_n+y_n+z_n)$ we find $r_n > 0$. We conclude $x_n/r_n, y_n/r_n, z_n/r_n > 0$, which proves that there is a triangle with sides a_n, b_n, and c_n. This triangle has inradius $\sigma - 1$, perimeter $2(\sigma-1)(x_n+y_n+z_n)/r_n = 2(\sigma-1)/\tau = 2\sigma(\sigma+1)$ and hence area $\sigma(\sigma^2-1)$.

Now suppose σ is rational. We will show that Θ_1 has infinite order. Assume that Θ_1 has finite order. As Θ_1 lies on the real component that does not contain $\mathcal{O}$, it has even order, so by Mazur's Theorem (see [Si1], Thm. III.7.5 for statement, [Maz], Thm. 8 for a proof) we find that $m\Theta_1 = \mathcal{O}$ for $m = 8, 10$, or 12. For each of these three values for m we can compute explicit rational functions $\xi_m, \eta_m \in \mathbb{Q}(s)$ such that the coordinates of $m\Theta_1$ are given by $(\xi_m(\sigma), \eta_m(\sigma))$. For $m = 8, 10$, or 12, these rational functions turn out to not have any rational poles, so Θ_1 has infinite order. To show that the triangles are pairwise nonsimilar, it suffices by Lemma 2.1 to show that the Θ_n lie in different orbits under G. Suppose that Θ_n and $\Theta_{n'}$ are in the same orbit under G for some $n, n' \geq 1$. Then by Lemma 5.5 we get $\Theta_n = \pm\Theta_{n'} + kP$ for $k = 0, 1$ or 2. Hence $3\left((2n-1) \mp (2n'-1)\right)\Theta_1 = 3(\Theta_n \mp \Theta_{n'}) = 3kP = \mathcal{O}$, so $2n - 1 = \pm(2n'-1)$, as Θ_1 has infinite order. From $n, n' \geq 1$ we find $n = n'$ and $\Theta_n = +\Theta_{n'} + kP$, so $k = 0$. Thus, $\Theta_n = \Theta_{n'}$. □

Proof of Theorem 1.1. Consider the open affine subset $U \subset X$ defined by $r \neq 0$, which is isomorphic to $\operatorname{Spec} A$ for $A = \mathbb{Q}[x,y,z]/\big(x+y+z-xyz\big)$. For each $n \geq 1$, let $V_n \subset \mathbb{P}^1$ be a dense open affine subset such that the composition γ_n of morphisms in (12) maps V_n to U. This is possible because the image of $\mathbb{P}^1$ is not entirely contained in the closed subset of X given by $r = 0$. Then there is a ring $B_n \subset \mathbb{Q}(s)$ such that V_n is isomorphic to $\operatorname{Spec} B_n$ and the composition in (12) is given by a ring homomorphism $\varphi_n \colon A \to B_n \subset \mathbb{Q}(s)$. Let $x_n(s)$, $y_n(s)$, $z_n(s) \in \mathbb{Q}(s)$ be the images under φ_n of $x, y, z \in A$ respectively. Then for any real number $\sigma > 1$ the values r_n, x_n, y_n, and z_n from Proposition 5.10 can be given by 1, $x_n(\sigma)$, $y_n(\sigma)$, and $z_n(\sigma)$ respectively. It follows from Proposition 5.10 that (1) and (2) of Theorem 1.1 are true for $a_n(s) = (y_n(s)+z_n(s))(s-1)$, $b_n(s) = (x_n(s)+z_n(s))(s-1)$, and $c_n(s) = (x_n(s)+y_n(s))(s-1)$. Note that if $\sigma_0 \neq \sigma_1$, then $\Delta_n(\sigma_0)$ is automatically not similar to $\Delta_m(\sigma_1)$ for any $m, n \geq 1$. □

Corollary 5.11 *The set of rational points on Y is Zariski dense in Y.*

Proof. The infinitely many multiples of the section R give infinitely many curves on Y, each with infinitely many rational points. Hence the Zariski closure of the set of rational points is Y. □

Remark 5.12 The four triples given in Remark 1.2 correspond to the sections $R, 3R, 5R$, and $7R$.

Remark 5.13 As mentioned before, Randall Rathbun found with a computer search a set of 8 Heron triangles with the same area and perimeter. His triangles correspond to $\tau = r/(x+y+z) = 28/195$. The 8 points on the corresponding elliptic curve above $[\tau : 1] = [28 : 195]$ generate a group of rank 4. This yields relatively many points of relatively low height. As in the proof of Proposition 5.10 we can take any n points on the real connected component that does not contain $\mathcal{O}$ and scale them to have the same perimeter and area. This is how we found the values in Table 1.

6 The Néron-Severi group under good reduction

In this section we will see how the Néron-Severi group of a surface behaves under good reduction. Proposition 6.2 is known among specialists, but by lack of reference, we will include a proof, as sketched by Bas Edixhoven. D. Harari proves a similar result about Brauer groups, see [Hr2]. Arguments similar to the ones used in this section can also be found in [Hr1] and [CR]. Proposition 6.2 will be used in the next section to find the Néron-Severi group of the elliptic surface $Y_{\overline{\mathbb{Q}}}$ from the previous section and the Mordell-Weil group $E(\overline{\mathbb{Q}}(s))$ of its generic fiber E.

For all of this section, let A be a discrete valuation ring of a number field K with maximal ideal $\mathfrak{m}$, whose residue field k has $q = p^r$ elements with p prime. Note that this gives a new meaning to all the symbols p, q, and r, which only holds for this section. Let S be an integral scheme with a morphism $S \to \operatorname{Spec} A$ that is projective and smooth of relative dimension 2. Then the projective surfaces $\overline{S} = S_{\overline{\mathbb{Q}}}$ and $\widetilde{S} = S_{\overline{k}}$ are smooth over the algebraically closed fields $\overline{\mathbb{Q}}$ and $\overline{k}$ respectively. We will assume that $\overline{S}$ and $\widetilde{S}$ are integral, i.e., they are irreducible, nonsingular, projective surfaces.

Let $l \neq p$ be a prime number. For any scheme Z we set

$$H^i(Z_{\text{ét}}, \mathbb{Q}_l) = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} \left(\varprojlim H^i(Z_{\text{ét}}, \mathbb{Z}/l^n\mathbb{Z}) \right).$$

Furthermore, for every integer m and every vector space H over $\mathbb{Q}_l$ with the Galois group $G(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ acting on it, we define the twistings of H to be the $G(\overline{\mathbb{F}_q}/\mathbb{F}_q)$-spaces $H(m) = H \otimes_{\mathbb{Q}_l} W^{\otimes m}$, where

$$W = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} (\varprojlim \mu_{l^n})$$

is the one-dimensional l-adic vector space on which $G(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ operates according to its action on the group $\mu_{l^n} \subset \overline{\mathbb{F}_q}$ of l^n-th roots of unity. Here we use $W^{\otimes 0} = \mathbb{Q}_l$ and $W^{\otimes m} = \operatorname{Hom}(W^{\otimes -m}, \mathbb{Q}_l)$ for $m < 0$.

For the rest of this article, all cohomology will be étale cohomology, so we will often leave out the subscript ét.

Lemma 6.1 *Let L denote the maximal subextension of $\overline{\mathbb{Q}}/K$ that is unramified at $\mathfrak{m}$. Let B denote the localization at some maximal ideal of the integral closure of A in L. Then for all integers i, m the natural homomorphisms*

$$\begin{aligned} &H^i(S_B, \mathbb{Q}_l)(m) \to H^i(\widetilde{S}, \mathbb{Q}_l)(m) \qquad \textit{and} \\ &H^i(S_B, \mathbb{Q}_l)(m) \to H^i(\overline{S}, \mathbb{Q}_l)(m) \end{aligned}$$

are isomorphisms.

Proof. As tensoring with W is exact, it suffices to prove this for $m = 0$. The ring B is a strictly Henselian ring, see [Mi], p. 38 (for the definition, see [EGA IV(4)], Déf. 18.8.2, or [Mi], § I.4). The surface $\widetilde{S}$ is the closed fiber of $S_B \to \operatorname{Spec} B$. As B is strictly Henselian, it follows from the proper base change theorem that the maps $H^i(S_B, \mathbb{Z}/l^n\mathbb{Z}) \to H^i(\widetilde{S}, \mathbb{Z}/l^n\mathbb{Z})$ are isomorphisms for all $n \geq 0$, see [Mi], Cor. VI.2.7, and [SGA $4\frac{1}{2}$], p. 39, Thm. IV.1.2. Hence, also the map $H^i(S_B, \mathbb{Q}_l) \to H^i(\widetilde{S}, \mathbb{Q}_l)$ obtained from taking the projective limit and tensoring with $\mathbb{Q}_l$ is an isomorphism. The surface $\overline{S}$ is the base change of S_B from $\operatorname{Spec} B$ to its geometric point $\operatorname{Spec} \overline{\mathbb{Q}}$. From the smooth base change theorem ([Mi], Thm. VI.4.1, and [SGA $4\frac{1}{2}$], p. 63, Thm. V.3.2) it follows that $H^i(S_B, \mathbb{Z}/l^n\mathbb{Z}) \to H^i(\overline{S}, \mathbb{Z}/l^n\mathbb{Z})$ is an isomorphism. For this exact statement, see [SGA $4\frac{1}{2}$], p. 54–56: Lemme V.1.5, (1.6), and Variante (for their S take $S = \operatorname{Spec} B$; as B is a strictly Henselian local ring which is integrally closed in its fraction field L already, we get that their S' equals their S). These statements assume that the morphism $S_B \to \operatorname{Spec} B$ is locally acyclic, which follows from the fact that it is smooth, see [SGA $4\frac{1}{2}$], p. 58, Thm. (2.1). Passing to the limit and tensoring with $\mathbb{Q}_l$, we find that also the map $H^i(S_B, \mathbb{Q}_l) \to H^i(\overline{S}, \mathbb{Q}_l)$ is an isomorphism. □

Proposition 6.2 *There are natural injective homomorphisms*

$$\operatorname{NS}(\overline{S}) \otimes_{\mathbb{Z}} \mathbb{Q}_l \hookrightarrow \operatorname{NS}(\widetilde{S}) \otimes_{\mathbb{Z}} \mathbb{Q}_l \hookrightarrow H^2(\widetilde{S}, \mathbb{Q}_l)(1) \tag{13}$$

of finite dimensional vector spaces over $\mathbb{Q}_l$. The second injection respects the Galois action of $G(\overline{k}/k)$.

Proof. After replacing K and A by a finite extension if necessary, we may assume without loss of generality that the natural map $\operatorname{NS}(S_K) \to \operatorname{NS}(\overline{S})$ is surjective (take generators for $\operatorname{NS}(\overline{S})$, lift them to $\operatorname{Div} \overline{S}$ and let K be a field over which all these lifts are defined). For any scheme Z, we have $H^1(Z_{\text{ét}}, \mathbb{G}_m) \cong \operatorname{Pic} Z$, see [SGA $4\frac{1}{2}$], p. 20, Prop. 2.3, or [Mi], Prop. III.4.9. As long as $l \neq \operatorname{char} k(z)$ for any $z \in Z$, the Kummer sequence

$$0 \to \mu_{l^n} \to \mathbb{G}_m \xrightarrow{[l^n]} \mathbb{G}_m \to 0$$

is a short exact sequence of sheaves on $Z_{\text{ét}}$, see [SGA $4\frac{1}{2}$], p. 21, (2.5), or [Mi], p. 66. Hence, from the long exact sequence we get a δ-map

$$\operatorname{Pic} Z \cong H^1(Z_{\text{ét}}, \mathbb{G}_m) \xrightarrow{\delta} H^2(Z_{\text{ét}}, \mu_{l^n}).$$

Taking the projective limit over n, we get a homomorphism

$$\operatorname{Pic} Z \to \varprojlim H^2(Z, \mu_{l^n}) \cong \varprojlim H^2(Z, \mathbb{Z}/l^n\mathbb{Z}) \otimes \mu_{l^n} \to H^2(Z, \mathbb{Q}_l)(1).$$

Let L and B be as in Lemma 6.1. Note that B is a discrete valuation ring. Because S_B is smooth and projective over $\operatorname{Spec} B$, with geometrically integral fibers, it follows that the map $\operatorname{Pic} S_B \to \operatorname{Pic} S_L$ is an isomorphism, see [Hr1], Lem. 3.1.1. From the above we get the diagram below, which commutes by functoriality. The maps $H^2(S_B, \mathbb{Q}_l)(1) \to H^2(\widetilde{S}, \mathbb{Q}_l)(1)$ and $H^2(S_B, \mathbb{Q}_l)(1) \to H^2(\overline{S}, \mathbb{Q}_l)(1)$ in the bottom line of the diagram are isomorphisms by Lemma 6.1.

$$\begin{tikzcd}
\operatorname{Pic} \overline{S} \arrow[d] & \operatorname{Pic} S_L \arrow[l] \arrow[d] & \operatorname{Pic} S_B \arrow[l, "\cong"'] \arrow[r] \arrow[d] & \operatorname{Pic} \widetilde{S} \arrow[d] \\
H^2(\overline{S}, \mathbb{Q}_l)(1) & H^2(S_L, \mathbb{Q}_l)(1) \arrow[l] & H^2(S_B, \mathbb{Q}_l)(1) \arrow[l] \arrow[r, "\cong"] \arrow[ll, bend left, "\cong"] & H^2(\widetilde{S}, \mathbb{Q}_l)(1)
\end{tikzcd}$$

For any proper variety Z, let $\operatorname{Pic}^{\mathrm{n}} Z$ denote the subgroup of $\operatorname{Pic} Z$ of all divisor classes on Z that are numerically equivalent with 0, i.e., those whose intersection number with every closed, integral curve on Z is 0, see [SGA 6], Exp. XIII, p. 644, 4.4. Then $\operatorname{Pic} Z / \operatorname{Pic}^{\mathrm{n}} Z$ is a finitely generated free abelian group. In fact, if the base field is algebraically closed, we have an isomorphism $\operatorname{NS}(Z)/\operatorname{NS}(Z)_{\mathrm{tors}} \cong \operatorname{Pic} Z/\operatorname{Pic}^{\mathrm{n}} Z$ (see [Ha1], Prop. 3.1, and [SGA 6], Exp. XIII, p.645, Thm. 4.6.) and by [Ta2], p. 97–98, the kernel of $\operatorname{Pic} Z \to H^2(Z, \mathbb{Q}_l)(1)$ is $\operatorname{Pic}^{\mathrm{n}} Z$. From the diagram above, it follows that the composition

$$\gamma\colon \operatorname{Pic} S_L \cong \operatorname{Pic} S_B \to \operatorname{Pic} \widetilde{S} \to H^2(\widetilde{S}, \mathbb{Q}_l)(1)$$

factors as

$$\begin{aligned}
\gamma\colon \operatorname{Pic} S_L \to \operatorname{NS}(\widetilde{S})/\operatorname{NS}(\widetilde{S})_{\mathrm{tors}} \hookrightarrow H^2(\widetilde{S}, \mathbb{Q}_l)(1) \qquad \text{and as} \\
\gamma\colon \operatorname{Pic} S_L \to \operatorname{Pic} \overline{S} \to H^2(\overline{S}, \mathbb{Q}_l)(1) \cong H^2(S_B, \mathbb{Q}_l)(1) \cong H^2(\widetilde{S}, \mathbb{Q}_l)(1).
\end{aligned} \tag{14}$$

Set $M = \operatorname{Pic} S_L/\ker \gamma$. From the first factorization of γ in (14) we find that there are injections

$$M \hookrightarrow \operatorname{NS}(\widetilde{S})/\operatorname{NS}(\widetilde{S})_{\mathrm{tors}} \hookrightarrow H^2(\widetilde{S}, \mathbb{Q}_l)(1). \tag{15}$$

The second map in the second line of (14) has kernel $\operatorname{Pic}^{\mathrm{n}} \overline{S}$, so γ also factors as

$$\gamma\colon \operatorname{Pic} S_L \to \operatorname{NS}(\overline{S})/\operatorname{NS}(\overline{S})_{\mathrm{tors}} \hookrightarrow H^2(\widetilde{S}, \mathbb{Q}_l)(1). \tag{16}$$

As the map $\operatorname{NS}(S_L) \to \operatorname{NS}(\overline{S})$ is surjective, so is the first map of (16). We conclude that M is isomorphic to $\operatorname{NS}(\overline{S})/\operatorname{NS}(\overline{S})_{\mathrm{tors}}$. Combining this with (15) and tensoring with $\mathbb{Q}_l$, we find the desired homomorphisms. □

Remark 6.3 Proposition 6.2 implies $\operatorname{rk}\mathrm{NS}(\overline{S}) \leq \operatorname{rk}\mathrm{NS}(\widetilde{S})$. For a shorter proof of this fact, note that without loss of generality, by enlarging A, we may assume that $\mathrm{NS}(\overline{S})$ and $\mathrm{NS}(\widetilde{S})$ are defined over the quotient field $K = Q(A)$ and the residue field k of A respectively. Let $\hat{K}$ denote the quotient field of the completion $\hat{A}$ of A, and let K' be the algebraic closure of $\hat{K}$. Then by [Fu], Exm. 20.3.6, the intersection numbers do not change under reduction, so we get $\operatorname{rk}\mathrm{NS}(S_{K'}) \leq \operatorname{rk}\mathrm{NS}(\widetilde{S})$. Thus, we find

$$\operatorname{rk}\mathrm{NS}(\overline{S}) = \operatorname{rk}\mathrm{NS}(S_K) \leq \operatorname{rk}\mathrm{NS}(S_{K'}) \leq \operatorname{rk}\mathrm{NS}(\widetilde{S}).$$

However, this does not imply that there exists a well-defined homomorphism $\mathrm{NS}(\overline{S}) \otimes_{\mathbb{Z}} \mathbb{Q}_l \hookrightarrow \mathrm{NS}(\widetilde{S}) \otimes_{\mathbb{Z}} \mathbb{Q}_l$, so Proposition 6.2 gives more information.

For any variety X over k, let $F_X \colon X \to X$ denote the *absolute Frobenius of* X, which acts as the identity on points, and by $f \mapsto f^p$ on the structure sheaf. Set $\varphi = F_{S_k}^r$ and let φ^* denote the automorphism on $H^2(\widetilde{S}, \mathbb{Q}_l)$ induced by $\varphi \times 1$ acting on $S_k \times_k \overline{k} \cong \widetilde{S}$. The next corollary gives an explicit method to bound the Picard number of a surface. This method was conveyed to the author by Jasper Scholten.

Corollary 6.4 *The ranks of* $\mathrm{NS}(\widetilde{S})$ *and* $\mathrm{NS}(\overline{S})$ *are bounded from above by the number of eigenvalues* λ *of* φ^* *for which* λ/q *is a root of unity, counted with multiplicity.*

Proof. By Proposition 6.2, any upper bound for the rank of $\mathrm{NS}(\widetilde{S})$ is an upper bound for the rank of $\mathrm{NS}(\overline{S})$. For any k-variety X, the absolute Frobenius F_X acts as the identity on the site $X_{\text{ét}}$. Hence, if we set $\overline{X} = X \times_k \overline{k}$, then $F_{\overline{X}} = F_X \times F_{\overline{k}}$ acts as the identity on $H^i(\overline{X}, \mathbb{Q}_l)(m)$ for any m, see [Ta2], § 3. Therefore, $F_X = F_X \times 1$ and $F_{\overline{k}} = 1 \times F_{\overline{k}}$ act as each other's inverses.

Let $\sigma \colon x \mapsto x^q$ denote the canonical topological generator of $G(\overline{k}/k)$. Then $\sigma = F_{\overline{k}}^r$ and as we have $\widetilde{S} \cong S_k \times_k \overline{k}$, we find $\varphi \times \sigma = F_{S_k}^r \times F_{\overline{k}}^r = F_{\widetilde{S}}^r$. By the above we find that the induced automorphisms $\varphi^{*(m)}$ and $\sigma^{*(m)}$ on $H^2(\widetilde{S}, \mathbb{Q}_l)(m)$ act as each other's inverses for any m.

As every divisor on $\widetilde{S}$ is defined over a finite field extension of k, some power of $\sigma^{*(1)}$ acts as the identity on $\mathrm{NS}(\widetilde{S}) \subset H^2(\widetilde{S}, \mathbb{Q}_l)(1)$. It follows from Proposition 6.2 that an upper bound for $\operatorname{rk}\mathrm{NS}(\widetilde{S})$ is given by the number of eigenvalues (with multiplicity) of $\sigma^{*(1)}$ that are roots of unity. As σ^* acts as multiplication by q on W, this equals the number of eigenvalues ν of $\sigma^{*(0)}$ for which νq is a root of unity. The corollary follows as $\varphi^* = \varphi^{*(0)}$ acts as the inverse of $\sigma^{*(0)}$. □

Remark 6.5 Tate's conjecture states that the upper bound mentioned is actually equal to the rank of $\mathrm{NS}(\widetilde{S})$, see [Ta2]. Tate's conjecture has been proven for ordinary K3 surfaces over fields of characteristic ≥ 5, see [NO], Thm. 0.2.

7 Computing the Néron-Severi group and the Mordell-Weil group

Note that also in this section all cohomology is étale cohomology, so we often will leave out the subscript ét. We consider the elliptic surface $Y \to C$ of section 5 over the algebraic closure and let $\overline{Y}$ and $\overline{C}$ denote $Y_{\overline{\mathbb{Q}}}$ and $C_{\overline{\mathbb{Q}}}$ respectively. Set $L = k(\overline{C}) \cong \overline{\mathbb{Q}}(s) \supset \mathbb{Q}(s) = k(C) = K$ and recall that we have encountered several points of $E(L)$, such as $P = \widetilde{M_1}$, the point Q from Theorem 5.6, and R induced by the closed immersion $C \to \widetilde{X}$. By Theorem 5.6 and Proposition 5.9 the points Q and R both have infinite order in $E(L)$. Suppose there are integers m, n such that $mQ + nR = 0$. Since complex conjugation sends Q and R to $-Q$ and R respectively, we find that also $-mQ + nR = 0$, whence $2mQ = 2nR = 0$. Therefore $m = n = 0$, so Q and R are linearly independent, and P, Q, and R generate a group isomorphic to $\mathbb{Z}^2 \times \mathbb{Z}/3\mathbb{Z}$. We will show that this is the full Mordell-Weil group $E(L)$.

Proposition 7.1 *The surface $\overline{Y}$ is a K3 surface. Its Néron-Severi lattice has rank* 18*. The rank of the Mordell-Weil group $\overline{Y}(\overline{C}) \cong E(L)$ equals* 2*.*

Proof. To prove that $\overline{Y}$ is a K3 surface, it suffices by definition to show that we have $\dim H^1(\overline{Y}, \mathcal{O}_{\overline{Y}}) = 0$ and that any canonical divisor $K_{\overline{Y}}$ is linearly equivalent to 0.

By Lemma 3.13 we get $\operatorname{Pic}^0 \overline{Y} \cong \operatorname{Pic}^0 \overline{C} = 0$, as C is isomorphic to $\mathbb{P}^1$. We conclude that $\mathrm{NS}(\overline{Y}) \cong \operatorname{Pic}(\overline{Y})$, so algebraic and numerical equivalence on $\overline{Y}$ coincide with linear equivalence. As $\widetilde{X}$ is rational, we have $\chi(\mathcal{O}_{\widetilde{X}}) = \chi(\mathcal{O}_{\mathbb{P}^2}) = 1$, see [Ha2], Cor. V.5.6. By Proposition 4.6 we get $\chi(\mathcal{O}_{\overline{Y}}) = (\deg \widetilde{f}|_C) \cdot \chi(\mathcal{O}_{\widetilde{X}_{\overline{\mathbb{Q}}}}) = 2$. From Theorem 3.8 we then find that $K_{\overline{Y}} = 0$ in $\operatorname{Pic} \overline{Y}$. Hence, the canonical sheaf $\omega_{\overline{Y}}$ is isomorphic to $\mathcal{O}_{\overline{Y}}$. From Serre duality we find $H^2(\overline{Y}, \mathcal{O}_{\overline{Y}}) \cong H^0(\overline{Y}, \omega_{\overline{Y}}) \cong H^0(\overline{Y}, \mathcal{O}_{\overline{Y}})$. Since $\overline{Y}$ is connected and projective, we get $\dim H^2(\overline{Y}, \mathcal{O}_{\overline{Y}}) = \dim H^0(\overline{Y}, \mathcal{O}_{\overline{Y}}) = 1$. Therefore, we get

$$\dim H^1(\overline{Y}, \mathcal{O}_{\overline{Y}}) = \dim H^0(\overline{Y}, \mathcal{O}_{\overline{Y}}) + \dim H^2(\overline{Y}, \mathcal{O}_{\overline{Y}}) - \chi(\mathcal{O}_{\overline{Y}}) = 1 + 1 - 2 = 0.$$

As seen in the proof of Proposition 4.6, the singular fibers of g come in pairs of copies of a singular fiber of $\widetilde{f}$. Hence, from Remark 5.2 and Theorem 3.14 we find $\rho = 2 + 2\left((6-1) + (3-1) + (1-1) + (1-1)\right) + \operatorname{rk} E(L) = 16 + \operatorname{rk} E(L)$ with $\rho = \operatorname{rk} NS(\overline{Y})$. Since Q and R are linearly independent, we have $\operatorname{rk} E(L) \geq 2$, so we get $\rho \geq 18$.

We will show $\rho \leq 18$ by reduction modulo a prime of good reduction. Take $p = 11$ and let $A = \mathbb{Z}_{(p)}$ be the localization of $\mathbb{Z}$ at p with residue field $k = A/p \cong \mathbb{F}_p$. Let $\mathfrak{X}$ be the closed subscheme of $\mathbb{P}^3_A$ given by $r^2(x + y + z) = xyz$ and $\mathfrak{f} \colon \mathfrak{X} \dashrightarrow \mathbb{P}^1_A$ the rational map that sends $[r : x : y : z]$ to $[r : x + y + z]$.

As $\mathfrak{X}$ is projective and $\mathfrak{X}_{\mathbb{Q}} \cong X$, there are A-points $\mathfrak{M}_i$ and $\mathfrak{N}_i$ on $\mathfrak{X}$ such that $(\mathfrak{N}_i)_{\mathbb{Q}} = N_i$ and $(\mathfrak{M}_i)_{\mathbb{Q}} = M_i$. Let $\pi' \colon \widetilde{\mathfrak{X}} \to \mathfrak{X}$ be the blow-up at the 6 points

$\mathfrak{N}_i$ and $\mathfrak{M}_i$, and let $\widetilde{\mathfrak{f}}\colon \widetilde{\mathfrak{X}} \to \mathbb{P}^1_A$ be the morphism induced by the composition $\mathfrak{f} \circ \pi'$. Let $\mathfrak{C} \subset \widetilde{\mathfrak{X}}$ be the strict transform of the curve in $\mathfrak{X}$ parametrized by

$$[r : x : y : z] = [s-1 : s+1 : s-1 : s(s-1)].$$

Let $\mathfrak{Y}$ denote the fibered product $\mathfrak{Y} = \mathfrak{C} \times_{\mathbb{P}^1_A} \widetilde{\mathfrak{X}}$, and let $\mathfrak{g}$ denote the projection $\mathfrak{Y} \to \mathfrak{C}$. Then $\mathfrak{Y}$ is a model of Y over A, i.e., $\mathfrak{Y}_{\mathbb{Q}} \cong Y$. Note that $\overline{Y} \cong \mathfrak{Y}_{\overline{\mathbb{Q}}}$. Set $\widetilde{Y} = \mathfrak{Y}_{\overline{k}}$ and $\widetilde{C} = \mathfrak{C}_{\overline{k}}$. The following diagram shows how the base changes of $\mathfrak{Y}$ that we will deal with are related. A similar diagram holds for $\mathfrak{C}$.

$$\begin{tikzcd}
\overline{Y} \arrow[d, "\cong"'] & Y \arrow[d, "\cong"'] & & & \widetilde{Y} \arrow[d, "\cong"'] \\
\mathfrak{Y}_{\overline{Q}} \arrow[r] \arrow[d] & \mathfrak{Y}_{\mathbb{Q}} \arrow[r] \arrow[d] & \mathfrak{Y} \arrow[d] & \mathfrak{Y}_k \arrow[l] \arrow[d] & \mathfrak{Y}_{\overline{k}} \arrow[l] \arrow[d] \\
\operatorname{Spec}\overline{\mathbb{Q}} \arrow[r] & \operatorname{Spec}\mathbb{Q} \arrow[r] & \operatorname{Spec} A & \operatorname{Spec} k \arrow[l] & \operatorname{Spec}\overline{k} \arrow[l]
\end{tikzcd}$$

We will show that $\mathfrak{Y}$ is smooth over $\operatorname{Spec} A$. Note that for each of the $\mathfrak{N}_i$ and $\mathfrak{M}_i$ there is an affine neighborhood $U = \operatorname{Spec} S \subset \mathfrak{X}$ for some A-algebra S, on which that point corresponds to an ideal $I \subset S$ satisfying $pS \cap I^n = pI^n$ for all $n \geq 0$. Set $T = S \otimes_A k \cong S/pS$ and $J = IT$. Then $U_k = \operatorname{Spec} T$ and we have

$$I^n \otimes_A k \cong I^n/pI^n \cong I^n/(pS \cap I^n) \cong I^n \cdot S/pS \cong I^n T = J^n.$$

This implies

$$\operatorname{Proj}\left(T \oplus J \oplus J^2 \oplus \ldots\right) \cong \operatorname{Proj}\left(S \oplus I \oplus I^2 \oplus \ldots\right) \times_{\operatorname{Spec} A} \operatorname{Spec} k,$$

which tells us that the blow-up of the reduction $\mathfrak{X}_k$ at the points $(\mathfrak{M}_i)_k$ and $(\mathfrak{N}_i)_k$ is isomorphic to $\widetilde{\mathfrak{X}} \times_A k$, i.e., the reduction $\widetilde{\mathfrak{X}}_k$ of $\widetilde{\mathfrak{X}}$. One easily checks that $\mathfrak{X}_k$ is geometrically regular outside the three ordinary double points $(\mathfrak{M}_i)_k$. Hence, this blow-up of $\mathfrak{X}_k$ at the points $(\mathfrak{M}_i)_k$ and $(\mathfrak{N}_i)_k$ is smooth over k, see [Ha2], exc. I.5.7. Thus $\widetilde{\mathfrak{X}}_k$ is smooth over k. As the morphism $\mathfrak{C}_k \to \mathbb{P}^1_k$ is unramified at the points of $\mathbb{P}^1_k$ where $\widetilde{\mathfrak{f}}_k$ has singular fibers (as is easily checked), $\mathfrak{Y}_k$ is smooth over k as well (cf. Proposition 4.6). Since the other fiber $\mathfrak{Y}_{\mathbb{Q}} \cong Y$ of $\mathfrak{Y} \to \operatorname{Spec} A$ is also smooth over its ground field $\mathbb{Q}$, we conclude that $\mathfrak{Y}$ is smooth over $\operatorname{Spec} A$ (cf. Remark 3.10).

Let $\varphi\colon \mathfrak{Y}_k \to \mathfrak{Y}_k$ denote the absolute Frobenius of $\mathfrak{Y}_k$ as in section 6. Let φ_i^* denote the induced automorphism on $H^i(\widetilde{Y}, \mathbb{Q}_l)$. By Corollary 6.4 the Picard number ρ is bounded from above by the number of eigenvalues λ of φ_2^* for which λ/p is a root of unity. We will count these eigenvalues using the Lefschetz trace formula and the Weil conjectures. The characteristic polynomial of $(\varphi_i^*)^n$ acting on $H^i(\widetilde{Y}, \mathbb{Q}_l)$ is

$$P_i(X) = \det\left(X \cdot \mathrm{Id} - (\varphi_i^*)^n\right) = \prod_{j=1}^{b_i} (X - \alpha_{ij}).$$

n	1	2	3
$\mathrm{Tr}(\varphi_0^*)^n$	1	1	1
$\mathrm{Tr}(\varphi_1^*)^n$	0	0	0
$\mathrm{Tr}(\varphi_3^*)^n$	0	0	0
$\mathrm{Tr}(\varphi_4^*)^n$	p^2	p^4	p^6
$\#\mathfrak{Y}_k(\mathbb{F}_{p^n})$	298	16908	1792858
$\mathrm{Tr}(\varphi_2^*)^n$	176	2266	21296
$\mathrm{Tr}(\varphi_2^*)^n\vert V$	$16p$	$18p^2$	$16p^3$
$\mathrm{Tr}(\varphi_{2,W}^*)^n$	0	88	0

Table 2: computing $\mathrm{Tr}(\varphi_{2,W}^*)^n$

By the Weil conjectures, $P_i(X)$ is a rational polynomial and the roots have absolute value $|\alpha_{ij}| = p^{ni/2}$, see [De], Thm. 1.6.

By Lemma 6.1 we have $\dim H^i(\overline{Y}, \mathbb{Q}_l) = \dim H^i(\widetilde{Y}, \mathbb{Q}_l)$ for $0 \leq i \leq 4$. Since $\overline{Y}$ is a K3 surface, the Betti numbers equal $\dim H^i(\widetilde{Y}, \mathbb{Q}_l) = b_i = 1, 0, 22, 0, 1$ for $i = 0, 1, 2, 3, 4$ respectively. Therefore, from the Weil conjectures we find $P_i(X) = X-1, 1, 1, X-p^2$ for $i = 0, 1, 3, 4$ respectively, whence $\mathrm{Tr}\,\varphi_i^* = 1, 0, 0, p^2$ for $i = 0, 1, 3, 4$. Similarly, we get $\mathrm{Tr}(\varphi_i^*)^n = 1, 0, 0, p^{2n}$ for $i = 0, 1, 3, 4$ and $n \geq 1$. That means that for any $n \geq 1$, if we know the number of $\mathbb{F}_{p^n}$-points of $\mathfrak{Y}_k$, then from the Lefschetz Trace Formula (see [Mi], Thm. VI.12.3)

$$\#\mathfrak{Y}_k(\mathbb{F}_{p^n}) = \sum_{i=0}^{4} (-1)^i \,\mathrm{Tr}\left((\varphi_i^*)^n\right)$$

we can compute $\mathrm{Tr}((\varphi_2^*)^n)$.

Let V denote the image in $H^2(\widetilde{Y}, \mathbb{Q}_l)$ under the composed map in (13) of the 18-dimensional subspace of $\mathrm{NS}(\overline{Y}) \otimes \mathbb{Q}_l$ that we already know, i.e., generated by the irreducible components of the singular fibers of g and the sections $\mathcal{O}$, Q, and R.

All these generators of V are defined over $k = \mathbb{F}_p$, except for the image of Q, which is defined over $\mathbb{F}_{p^2}$. In the Mordell-Weil group modulo torsion $\widetilde{Y}(\widetilde{C})/\widetilde{Y}(\widetilde{C})_{\mathrm{tors}}$ we have $\varphi(Q) = -Q$. Hence V is φ_2^*-invariant and we find that $\mathrm{Tr}(\varphi_2^*)^n|V = 17p^n + (-1)^n p^n$.

Set $W = H^2(\widetilde{Y}, \mathbb{Q}_l)/V$ and let $\varphi_{2,W}^*$ denote the automorphism on W induced by φ_2^*. Then W has dimension 4 and from linear algebra we get

$$\mathrm{char}(\varphi_2^*) = \mathrm{char}(\varphi_2^*|V) \cdot \mathrm{char}(\varphi_{2,W}^*) \tag{17}$$

and

$$\mathrm{Tr}(\varphi_2^*)^n = \mathrm{Tr}(\varphi_2^*)^n|V + \mathrm{Tr}(\varphi_{2,W}^*)^n.$$

This last equality allows us to compute $\mathrm{Tr}(\varphi_{2,W}^*)^n$ for $n \geq 1$, which is done for $n = 1, 2, 3$ in Table 2.

We computed the number of points on $\mathfrak{Y}_k(\mathbb{F}_{p^n})$ as follows. As $\mathfrak{Y}_k$ has the structure of elliptic surface over $\mathfrak{C}_k$, we can let the computer package Magma compute the number of points above every point of $\mathfrak{C}_k(\mathbb{F}_{p^n})$ with a nonsingular elliptic fiber. Adding to that the contribution of the singular fibers gives the total number of points.

For any linear operator T on an m-dimensional vector space with characteristic polynomial

$$\operatorname{char} T = X^m + c_1 X^{m-1} + c_2 X^{m-2} + \ldots + c_{m-1} X + c_m,$$

we have $c_1 = -t_1$, $c_2 = \frac{1}{2}(t_1^2 - t_2)$, and $c_3 = -\frac{1}{6}(t_1^3 + 2t_3 - 3t_1 t_2)$ with $t_n = \operatorname{Tr} T^n$. From this and Table 2 we find that the characteristic polynomial of $\varphi_{2,W}^*$ equals $h = X^4 - 44X^2 + c_4$ for some c_4. By the Weil conjectures, and (17), the roots of h have absolute value p and their product c_4 is rational, so $c_4 = \pm p^4$. As not all roots of $X^4 - 44X^2 - 11^4$ have absolute value 11, we get $h = X^4 - 44X^2 + 11^4$. If α is a root of h then $\beta = (\alpha/p)^2$ satisfies $11\beta^2 - 4\beta + 11 = 0$. As the only quadratic roots of unity are $\pm\sqrt{-1}$ and ζ_6^i, we find that β is not a root of unity, and thus neither is α/p. From (17) it follows that α/p is a root of unity for at most $22 - 4 = 18$ roots α of $\operatorname{char}(\varphi_2^*)$. From Corollary 6.4 we find $\rho \leq 18$. □

Corollary 7.2 *The Mordell-Weil group $E(L)$ is generated by P, Q, and R and is isomorphic to $\mathbb{Z}^2 \times \mathbb{Z}/3\mathbb{Z}$.*

Proof. As $\overline{Y} \to \overline{C}$ is a relatively minimal fibration and $\overline{Y}$ is regular and projective, the Néron model of $\overline{Y}/\overline{C}$ is obtained from $\overline{Y}$ by deleting the singular points of the singular fibers, see [Si2], Thm. IV.6.1, and [BLR], § 1.5, Prop. 1. Note that at $\sigma = 0$ and $\sigma = -1$ we have additive reduction (type IV), whence the identity component of the reduction has no torsion as we are in characteristic 0. Also because we are in characteristic 0, the kernel of reduction $E_1(L)$ has no torsion either, see [Si1], Prop. VII.3.1. It follows that the group $E_0(L)$ of nonsingular reduction has no torsion, see [Si2], Rem. IV.9.2.2. By the classification of singular fibers we find that $E(L)/E_0(L)$ has order at most 3, see [Si2], Cor. IV.9.2 and Tate's Algorithm IV.9.4. We conclude that $E(L)_{\text{tors}}$ has order 3 and is generated by P.

With Shioda's explicit formula for the Mordell-Weil pairing ([Shi], Thm. 8.6), we find $\langle Q, R\rangle = 0$ and $\langle Q, Q\rangle = \langle R, R\rangle = 1$. Hence, as seen before, Q and R are linearly independent. As the rank $\operatorname{rk} E(L)$ equals 2 by Proposition 7.1, the group generated by Q and R has finite index in the Mordell-Weil lattice $E(L)/E(L)_{\text{tors}}$. If the Mordell-Weil lattice were not generated by Q and R, then it would contain a nonzero element $S = aQ + bR$ with $a, b \in \mathbb{Q}$ and $-\frac{1}{2} < a, b \leq \frac{1}{2}$, so that $\langle S, S\rangle = a^2 + b^2 \leq \frac{1}{2}$. On the other hand, based on the type of singularities, it follows from the explicit formulas for the Mordell-Weil pairing that its values are contained in $\frac{1}{6}\mathbb{Z}$. As for any rational a, b the 3-adic valuation of $a^2 + b^2$ is even, we conclude that in fact we have $\langle S, S\rangle \in \frac{1}{2}\mathbb{Z}$, so that $a^2 + b^2 \geq \frac{1}{2}$. Thus, we find $a^2 + b^2 = \frac{1}{2}$, so $a = b = \frac{1}{2}$. Therefore, $2S = Q + R + \varepsilon P$ for some $\varepsilon \in \{0, 1, 2\}$. After adding εP to S if necessary, we may assume $\varepsilon = 0$ without loss of generality.

It suffices to check $Q+R \notin 2E(K)$. Let (p_S, q_S), (p_{2S}, q_{2S}), and (p_{Q+R}, q_{Q+R}) denote the Weierstrass coordinates of S, $2S$, and $Q+R$ respectively. Using addition formulas, we can compute $p_{Q+R} \in \mathbb{Q}(i)(s)$ explicitly and express p_{2S} in terms of p_S. Let u be defined by $p_S - 4(s-1)^2 = 2(s-1)u$. Then in terms of u, the equation $p_{2S} = p_{Q+R}$ simplifies to

$$u^4 + 4(s-1)(s+1)(s+i)u^3 + 2(s^2 + (1+i)s - 2 + i)s^2(s+1)^2u^2 + \\ 8(s^2 + (1+i)s - 2 + i)(s-1)s^2(s+1)^2u + 8(s+i)s^2(s-1)^2(s+1)^3 = 0 \tag{18}$$

By Gauss's Theorem any root $u \in L = \overline{\mathbb{Q}}(s)$ of this equation is contained in $\overline{\mathbb{Q}}[s]$ and divides the constant term $8(s+i)s^2(s-1)^2(s+1)^3$. Hence, any root u is of the form

$$u = cs^k(s+1)^l(s-1)^m(s+i)^n, \tag{19}$$

for some constant c and exponents k, l, m, and n. Considering the four Newton polygons, we find $k = 0$, $l = 1$, and $m, n \in \{0, 1\}$. One easily checks that for none of the four possibilities for m, n there is a c such that (18) is satisfied for u as in (19). □

Corollary 7.3 *The discriminant of the Néron-Severi lattice* $\mathrm{NS}(\overline{Y})$ *equals* -36.

Proof. From the short exact sequence (3), we find the following equation, relating the discriminant of the Néron-Severi lattice to that of the Mordell-Weil lattice, see [Shi], Thm. 8.7.

$$|\operatorname{disc} \mathrm{NS}(\overline{Y})| = \frac{\operatorname{disc} E(L)/E(L)_{\mathrm{tors}} \cdot \prod m_v^{(1)}}{|E(L)_{\mathrm{tors}}|^2}$$

Here $m_v^{(1)}$ is the number of irreducible components of multiplicity 1 of the fiber of g above $v \in C$. Note that we used $\operatorname{disc} T = \prod m_v^{(1)}$, see [Shi], (7.9). In the proof of Corollary 7.2 we have seen $\operatorname{disc} E(L)/E(L)_{\mathrm{tors}} = 1$, so we get

$$|\operatorname{disc} \mathrm{NS}(\overline{Y})| = \frac{1 \cdot 6 \cdot 6 \cdot 3 \cdot 3}{3^2} = 36.$$

By the Hodge index Theorem $\operatorname{disc} \mathrm{NS}(\overline{Y})$ is negative, so we find $\operatorname{disc} \mathrm{NS}(\overline{Y}) = -36$. □

References

[Aa] Aassila, M., Some results on Heron triangles, *Elem. Math.*, **56** (2001), pp. 143–146.

[BLR] Bosch, S., Lütkebohmert, W., and Raynaud, M., *Néron Models*, Springer-Verlag, Berlin, 1990.

[BM] Bombieri, E. and Mumford, D., Enriques' classification of surfaces in char. p, II, *Complex Analysis and Algebraic Geometry — Collection of papers dedicated to K. Kodaira*, ed. W.L. Baily and T. Shioda, Iwanami and Cambridge Univ. Press (1977), pp. 23–42.

[BT] Bogomolov, F. and Tschinkel, Yu., Density of rational points on elliptic K3 surfaces, *Asian J. Math.*, **4**, 2 (2000), pp. 351–368.

[BW] Bruce, J. and Wall, C., On the classification of cubic surfaces, *J. London Math. Soc. (2)*, **19** (1979), pp. 245–256.

[CD] Cossec, F. and Dolgachev, I., *Enriques Surfaces I*, Progress in Math., Vol. **76**, 1989.

[Ch] Chinburg, T., Minimal Models of Curves over Dedekind Rings, *Arithmetic Geometry*, ed. Cornell, G. & Silverman, J. (1986), pp. 309–326.

[CR] Colliot-Thélène, J.-L. and Raskind, W., Groupe de Chow de codimension deux des variétés définies sur un corps de nombres: un théorème de finitude pour la torsion, *Invent. Math.*, **105** (1991), pp. 221–245.

[De] Deligne, P., La Conjecture de Weil. I, *Publ. Math. IHES*, **43** (1974), pp. 273–307.

[Du] Du Val, P., On isolated singularities which do not affect the conditions of adjunction, Part I, *Proc. Cambridge Phil. Soc.*, **30** (1934), pp. 453–465.

[EGA II] Grothendieck, A., *Éléments de géométrie algébrique. IV. Étude globale élémentaire de quelques classes de morphismes*, IHES Publ. Math., no. **8**, 1961.

[EGA IV(1)] Grothendieck, A., *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas, Première partie*, IHES Publ. Math., no. **20**, 1964.

[EGA IV(2)] Grothendieck, A., *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas, Seconde partie*, IHES Publ. Math., no. **24**, 1965.

[EGA IV(4)] Grothendieck, A., *Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas, Quatrième partie*, IHES Publ. Math., no. **32**, 1967.

[Fr] Friedman, R., *Algebraic surfaces and holomorphic vector bundles*, Universitext, Springer, 1998.

[Guy] Guy, R., *Unsolved Problems in Number Theory*, Problem Books in Math., Springer-Verlag, New-York, 1994.

[Ha1] Hartshorne, R., Equivalence relations of algebraic cycles and subvarieties of small codimension, *Algebraic Geometry, Arcata 1974*, Amer. Math. Soc. Proc. Symp. Pure Math. **29** (1975), pp. 129–164.

[Ha2] Hartshorne, R., *Algebraic Geometry*, GTM **52**, Springer-Verlag, New-York, 1977.

[Hr1] Harari, D., Méthode des fibrations et obstruction de Manin, *Duke Math. J.*, **75**, no. 1 (1994), pp. 221–260.

[Hr2] Harari, D., Flèches de spécialisations en cohomologie étale et applications arithmétiques, *Bull. Soc. Math. France*, **125**, no. 2 (1997), pp. 143–166.

[KL] Kramer, A.-V. and Luca, F., Some remarks on Heron triangles, *Acta Acad. Paedagog. Agriensis Sect. Mat. (N.S.)*, **27** (2000), pp. 25–38 (2001).

[Ko1] Kodaira, K., On compact analytic surfaces II–III, *Ann. of Math.*, **77** (1963), pp. 563–626; **78** (1963), pp. 1–40.

[Ko2] Kodaira, K., On the structure of compact complex analytic surfaces I, II, *Amer. J. Math.*, **86** (1964), pp. 751–798; **88** (1966), pp. 682–721.

[Lic] Lichtenbaum, S., Curves over discrete valuation rings, *Amer. J. Math.*, **90** (1968), pp. 380–405.

[Man] Manin, Y., *Cubic forms: Algebra, Geometry, Arithmetic*, North-Holland, Amsterdam, 1974.

[Maz] Mazur, B., Modular curves and the Eisenstein ideal, *IHES Publ. Math.*, **47** (1977), pp. 33–186.

[Mi] Milne, J.S., *Étale Cohomology*, Princeton Mathematical Series **33**, Princeton University Press, New Jersey, 1980.

[Na] Nagata, M., On rational surfaces I, II, *Mem. Coll. Sci. Kyoto (A)*, **32** (1960), pp. 351–370; **33** (1960), pp. 271–293.

[NO] Nygaard, N. and Ogus, A., Tate's conjecture for K3 surfaces of finite height, *Ann. of Math.*, **122** (1985), pp. 461–507.

[Pi] Pinkham, H., Singularités Rationnelles de Surfaces, *Séminaire sur les Singularités des Surfaces*, Lect. Notes in Math. **777**, ed. M. Demazure, H. Pinkham, and B. Teissier, Springer-Verlag (1980), pp. 147–172.

[SB] Stienstra, J. and Beukers, F., On the Picard-Fuchs Equation and the Formal Brauer Group of Certain Elliptic K3-Surfaces, *Math. Ann.*, **271** (1985), pp. 269–304.

[SGA 1] Grothendieck, A., *Revêtements étales et groupe fondamental*, Lect. Notes in Math. **224**, Springer-Verlag, Heidelberg, 1971.

[SGA $4\frac{1}{2}$] Grothendieck, A. et al., *Cohomologie étale*, Lect. Notes in Math. **569**, Springer-Verlag, Heidelberg, 1977.

[SGA 6] Grothendieck, A. et al., *Théorie des Intersections et Théorème de Riemann-Roch*, Lect. Notes in Math. **225**, Springer-Verlag, Heidelberg, 1971.

[Sha] Shafarevich, I., *Lectures on Minimal Models and Birational Transformations of Two-dimensional Schemes*, Tata Institute, Bombay, 1966.

[Shi] Shioda, T., On the Mordell-Weil Lattices, *Comm. Math. Univ. Sancti Pauli*, **39**, 2 (1990), pp. 211–240.

[Si1] Silverman, J.H., *The Arithmetic of Elliptic Curves*, GTM **106**, Springer-Verlag, New-York, 1986.

[Si2] Silverman, J.H., *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM **151**, Springer-Verlag, New-York, 1994.

[Ta1] Tate, J., Genus change in inseparable extensions of function fields, *Proc. AMS*, **3** (1952), pp. 400–406.

[Ta2] Tate, J., Algebraic cycles and poles of zeta functions, *Arithmetical Algebraic Geometry*, ed. O.F.G. Schilling (1965), pp. 93–110.

[Ta3] Tate, J., Algorithm for determining the type of a singular fiber in an elliptic pencil, *Modular functions of one variable IV*, Lect. Notes in Math. **476**, ed. B.J. Birch and W. Kuyk, Springer-Verlag, Berlin (1975), pp. 33–52.