Potential density of rational points on algebraic varieties

Brendan Hassett *

September 2002

1 Introduction

Let K be a number field and consider a collection of equations

$$f_1(x_1, \ldots, x_n) = f_2(x_1, \ldots, x_n) = \ldots = f_r(x_1, \ldots, x_n) = 0$$

where the f_j are polynomials with coefficients in K. What are the solutions to these equations over K? Sometimes, every solution $(a_1, \ldots, a_n) \in K^n$ necessarily satisfies further equations which are not algebraic consequences of our original collection. For instance, every solution over $\mathbb{Q}$ to $x_1^3 + x_2^3 = 1$ satisfies the additional equation $x_1 x_2 = 0$. Of course, solutions over extensions L/K may fail to satisfy these further equations, e.g., the solution $(-1, \sqrt[3]{2})$ to the Fermat equation.

This paper is dedicated to studying collections of equations with the following desideratum: All the equations satisfied by the solutions over K are algebraic consequences of the equations we start with. For instance, the solutions to $x_1^2 + x_2^2 = 1$ over $\mathbb{Q}$ satisfy no equations that are not multiples of the original equation.

Our approach is geometric. The desired property may be restated in the language of algebraic geometry: We seek classes of algebraic varieties whose K-rational points are dense in the Zariski topology. Here 'classes' of algebraic varieties are distinguished by invariants, like the geometric genus

*The author was partially supported by National Science Foundation Grant 0196187.

or plurigenera, or by geometric properties, like the existence of fibrations by rational or elliptic curves. One of the most profound questions of higher dimensional geometry is the logical relationship between the values of the invariants and the presence of fibrations.

However, there is a price to be paid for working geometrically: It is exceedingly rare for all the varieties with common geometric properties to have dense rational points. Even varieties which are geometrically $\mathbb{P}^n$ may or may not have rational points over a given number field, so we allow ourselves finite extensions of the given field. Then more uniform statements on rational points, depending only on the underlying geometry, are possible.

The paper is organized as follows. Basic definitions and notation are laid out in §2. General properties of density are discussed systematically in §3. The remainder of the paper is devoted to classes of examples. Abelian varieties and fibrations are addressed in §4. Fano varieties, especially those of small dimension, are discussed in §5. K3 surfaces, the simplest class of varieties where density of rational points remains a matter of controversy, are studied in §6. Several sections are devoted to the twisting method of Bogomolov and Tschinkel, as applied to elliptic K3 surfaces (Theorem 6.4.) Basic properties of the Tate-Shafarevich group are reviewed in §7. The simplest application of the method, to nonisotrivial elliptic K3 surfaces, is given in §8. This approach yields an infinite number of irreducible, nodal, rational curves in the K3 surface (see Corollaries 8.12 and 8.13). A more refined approach covering the isotrivial cases, and closer in spirit to the original paper [BT3] of Bogomolov and Tschinkel, can be found in §9. A third, independent approach, originating from a letter of J. Kollár, is given in §10. Finally, §11 contains the strongest results now known for general K3 surfaces, as well as some statements for higher dimensional varieties. The Appendix is a short resumé of Galois cohomology and principal homogeneous spaces.

Acknowledgments: The author is very grateful to F. Bogomolov and Y. Tschinkel for their generosity in explaining the ideas in their work, both through conversations and correspondence. He would also like to thank J.L. Colliot-Thélène for his encouragement and for sharing unpublished expository accounts of some of the results covered here. The argument of §10 is due to J. Kollár, who provided numerous other constructive suggestions. The author also benefitted from conversations with D. Abramovich and A. Kresch, who proposed Remark 6.5 and Proposition 8.2 respectively. The manuscript

was greatly improved by insightful comments from T. Szamuely.

This paper is based on lectures given at the European Summer School *Higher Dimensional Varieties and Rational Points*, held at the Alfréd Rényi Institute of Mathematics of the Hungarian Academy of Sciences.

2 The notion of potential density

We fix some notation. Throughout this paper, we work over a number field K. A variety X/K is a geometrically integral scheme of finite type over K. Its K-rational points are denoted $X(K)$.

Definition 2.1 Let X be a variety over K. The K-rational points of X are *dense* if $X(K)$ is not contained in any Zariski closed subset of X. Rational points of X are *potentially* dense if there exists a finite field extension L/K over which rational points are dense.

In the sequel, when we say that 'potential density holds for X' we mean that rational points are potentially dense on X.

Our motivation for considering *potential* density is to isolate properties of rational points that follow from the *geometric properties* of X, rather than those that depend on the ground field.

Example 2.2 Rational points of $\mathbb{P}^n$ are dense over $\mathbb{Q}$.

Example 2.3 Consider the curve

$$X = \{x^2 + y^2 = -z^2\} \subset \mathbb{P}^2_{\mathbb{Q}}.$$

This has no rational points whatsoever, but rational points are potentially dense. Indeed, over $\mathbb{Q}(i)$ we have an isomorphism

$$\begin{array}{ccc} X & \stackrel{\simeq}{\longrightarrow} & \{x^2 + y^2 = z^2\} \\ (x, y, z) & \to & (x, y, iz). \end{array}$$

However, the curve $\{x^2 + y^2 = z^2\}$ is isomorphic to $\mathbb{P}^1$

$$\begin{array}{ccc} \mathbb{P}^1 & \stackrel{\simeq}{\longrightarrow} & \{x^2 + y^2 = z^2\} \\ (s, t) & \to & (2st, s^2 - t^2, s^2 + t^2), \end{array}$$

which has dense rational points.

Example 2.4 The example above admits generalizations to higher dimensions. A *Brauer-Severi* variety X/K is a variety such that $X_{K^a} \simeq \mathbb{P}^N_{K^a}$, i.e., a variety geometrically isomorphic to $\mathbb{P}^n$. Of course, such an isomorphism may be realized over some finite extension L/K, and L-rational points of X are dense. The conic curve of Example 2.3 is the simplest example of a Brauer-Severi variety.

From an arithmetic standpoint, the precise nature of the field extensions L/K over which rational points become dense is an extremely interesting topic. Indeed, Brauer-Severi varieties first arose in the study of 'generic splitting fields' for central simple algebras [Am][Ro]. However, our primary interest lies in the interaction between density of rational points and geometric properties of algebraic varieties. Consequently, we will not keep track of the field extension over which points become dense. Indeed, in the sequel we will take finite extensions of the ground field without explicit comment, and even suppress the notation for the ground field.

3 Basic properties of potential density

3.1 Behavior under morphisms

Proposition 3.1 *Let $g : X \dashrightarrow Y$ be a dominant rational map of projective varieties over a number field. Assume that rational points of X are potentially dense. Then rational points of Y are potentially dense.*

In particular, potential density is a birational property.
Proof: Choose a number field L over which X, Y, and g are defined, and $X(L)$ is Zariski dense. Let $U \subset X$ be an open subset over which g is a morphism. We have $g(U(L)) \subset Y(L)$, and the image of a dense set under a dominant rational map remains dense. □

Definition 3.2 A variety Y defined over a number field is *unirational* if, over some finite field extension, there exists a dominant rational map $g : \mathbb{P}^N \dashrightarrow Y$.

Combining Proposition 3.1 with Example 2.2, we obtain

Corollary 3.3 Let Y be a variety over a number field and assume that Y is unirational. Then rational points of Y are potentially dense.

Proposition 3.4 (Chevalley-Weil Theorem [We]) *Let $\phi : X \to Y$ be an étale morphism of proper varieties over a number field. Assume rational points of Y are potentially dense. Then rational points of X are also potentially dense.*

Sketch Proof: A good modern account can be found in [Se2]. Let L be a number field over which X, Y, and g are defined, and over which rational points of Y are dense. Choose a ring of integers $\mathcal{O} = \mathcal{O}_{L,S}$ (with S a finite set of places, including the infinite ones) over which we have the following:

1. X and Y have models $\mathcal{X}$ and $\mathcal{Y}$ over $\mathcal{O}$, i.e., $\mathcal{X} \to \mathrm{Spec}(\mathcal{O})$ and $\mathcal{Y} \to \mathrm{Spec}(\mathcal{O})$ are flat and projective, with generic fibers X_L and Y_L respectively;

2. g extends to an étale morphism $g : \mathcal{X} \to \mathcal{Y}$.

We choose S to exclude primes over which g has ramification or indeterminacy. Since $\mathcal{Y}$ is proper, the valuative criterion implies each L-rational point of $\mathcal{Y}$ extends to a $\mathcal{O}$-integral point. The $\mathcal{O}$-integral points of $\mathcal{Y}$ yield points of X defined over extensions of L of degree $\leq \deg(\phi)$, with discriminant contained in S. It is a classical theorem of Hermite that there are a finite number of such extensions $M_1, \ldots, M_r$. Over one of them rational points of X are Zariski dense. $\square$

Question 3.5 What classes of morphisms $X \to Y$ share the lifting property of Proposition 3.4?

One other class of such morphisms is étale projective bundles (cf. [HT2]).

3.2 Negative results

Any dense subset of a curve is infinite, so we have the following restatement of the Mordell Conjecture:

Proposition 3.6 (Faltings Theorem [Fa1]) *Let X be a curve of genus ≥ 2 over a number field. Then rational points are not potentially dense.*

Example 3.7 Colliot-Thélène, Skorobogatov, and Swinnerton-Dyer [CSS] give an example of a variety for which rational points are not potentially dense, and the proof of nondensity requires Propositions 3.1, 3.4, and 3.6.

They describe a smooth projective surface Y, which itself does not dominate any curve of genus ≥ 2 (or, indeed, any variety of general type), but admits an étale double cover X that does dominate a curve of genus two:

$$\begin{array}{rccc} & X & \rightarrow & C \\ \text{étale double cover} & \downarrow & & \\ & Y & & \end{array} .$$

If rational points were potentially dense on Y they would be potentially dense on X by Proposition 3.4, and thus potentially dense on C as well, contradicting Proposition 3.6.

Let X be smooth and projective with canonical bundle ω_X. We say X is of *general type* if ω_X is *big*, i.e.,

$$h^0(\omega_X^{\otimes n}) \sim Cn^{\dim(X)}, \quad C > 0,$$

for sufficiently large n. The following conjecture would preclude potential density of rational points for such varieties:

Conjecture 3.8 (Lang-Bombieri Conjecture) Let X be a projective variety of general type defined over a number field. Then rational points on X are not potentially dense.

This is known for subvarieties of abelian varieties which are of general type [Fa2].

Remark 3.9 What is the largest class of projective varieties for which potential density might hold? In light of Conjecture 3.8 and Propositions 3.1 and 3.4, a variety with dense rational points should admit no étale covers that dominate varieties of general type. It is not known whether there are any further constraints. We refer the reader to [HT2] and [Ca2] for further discussion of this question.

4 Abelian fibrations

4.1 Abelian varieties

We start with some definitions:

Definition 4.1 Let $(A, 0)$ be an abelian variety defined over a field F of characteristic zero. A point $p \in A(F)$ is *nontorsion* if the set

$$\mathbb{Z}p = \{np : n \in \mathbb{Z}\}$$

is infinite and *nondegenerate* if this set is dense.

Proposition 4.2 *Let A be an abelian variety over a number field K. After passage to a finite extension L/K, $A(L)$ contains a nondegenerate point and L-rational points are dense.*

Sketch Proof: (cf. Proposition 3.1 of [HT], where a second argument can be found) The Mordell-Weil Theorem (see [Se2]) says that $A(K)$ is a finitely generated abelian group for any number field K; the *rank* of $A(K)$ is just the rank of this group. The main ingredient in the proof is a result of Jarden and Frey [FJ], Theorem 10.1: After passage to a suitable finite extension L/K we have

$$\text{rank } A(L) > \text{rank } A(K).$$

The argument of [FJ] uses $\mathfrak{p}$-adic techniques: Consider primes $\mathfrak{p}$ totally ramified over a fixed prime of K. One creates a point, over a suitable extension of K, with prescribed reduction mod $\mathfrak{p}^n$. The condition on the reduction mod $\mathfrak{p}^n$ is used to show that this point is not in the span of $A(K)$.

This result proves the proposition when A is geometrically simple: For any nontorsion point $p \in A(L)$, the Zariski closure of $\mathbb{Z}p \subset A(L)$ contains a positive-dimensional abelian subvariety, and hence is equal to A. In general, the argument proceeds by induction on the number of simple components. We assume $A = A_1 \times A_2$ where A_2 is simple and $p_1 \in A_1(K), p_2 \in A_2(K)$ are nondegenerate. If $(p_1, p_2) \in A_1 \times A_2$ is degenerate then it is contained in a proper abelian subvariety $B \subset A_1 \times A_2$, which corresponds to a rational homomorphism $\beta \in \text{Hom}(A_1, A_2) \otimes \mathbb{Q}$. It follows that $d\beta(p_1) = dp_2$ for some positive d. However, the group $\text{Hom}(A_1, A_2)$ is finitely generated. Again applying the result of [FJ], we obtain a finite extension L/K and a point $q \in A_2(L)$ so that $q \notin \beta(p_1)$ for any $\beta \in \text{Hom}(A_1, A_2) \otimes \mathbb{Q}$. $\square$

4.2 Abelian fibrations over a field and principal homogeneous spaces

Throughout this section, F is a field of characteristic zero with algebraic closure F^a.

Definition 4.3 A variety X_F over F is an *abelian fibration* if it is geometrically an abelian variety, i.e., $X_{F^a} := X_F \times_F F^a$ is isomorphic to an abelian variety over F^a.

Remark 4.4 (Warning) We do *not* assume that X_F has a point over F. In particular, there may not be a group law on X_F defined over F (cf. Definition 4.12.)

There are a number of auxiliary abelian fibrations associated to X_F. Let $J^0(X_F)$ denote the *Albanese* of X_F, an abelian variety over F satisfying the following ([La] II §3):

1. The formation of the Albanese commutes with field extensions E/F, i.e., $J^0(X_E) = J^0(X_F) \times_F E$.

2. There is a morphism over F

$$s : X_F \times_F X_F \to J^0(X_F).$$

   If E/F is an extension over which there is a point $x \in X_F(E)$ then $s|(X_F \times \{x\})$ induces an isomorphism $i_x : X_E \simeq J^0(X_E)$ so that $s(x_1, x_2) = i_x(x_1) - i_x(x_2)$.

3. Suppose we have another morphism to an abelian variety

$$s' : X_F \times_F X_F \to A,$$

   such that $s'(x_1, x_2) = i(x_1) - i(x_2)$, for some $i : X_E \to A_E$ defined over an extension E/F. Then factors s' through s.

Of course, X_F always has a point over its function field $F(X)$ (the generic point x), and we may consider the composition

$$J^0(X_F) \times_F F(X) = J^0(X_{F(X)}) \xrightarrow{i_x^{-1}} X_{F(X)} = X_F \times_F F(X) \xrightarrow{\pi_1} X_F$$

as a rational map $J^0(X_F) \times_F X_F \dashrightarrow X_F$. Any such rational map extends uniquely to a morphism $a : J^0(X_F) \times_F X_F \to X_F$ [La] II §1. Over any field extension over which $X_E \neq \emptyset$ we can write $a(j, x) = j + x$. Thus we conclude:

> X_F has the structure of a *principal homogeneous space* for $J^0(X_F)$, classified by a cocycle $[X_F] \in H^1(\Gamma, J^0(X_F))$ (see the Appendix).

For each $m \in \mathbb{Z}$, let $J^m(X_F)$ denote the principal homogeneous space corresponding to $m[X_F]$, which by descent is also an abelian fibration over F [LT]§2, Prop. 4. Descent also gives the following morphisms over F:

1. the cycle-class morphism

$$\begin{array}{rcl} \underbrace{X_F \times_F \ldots \times_F X_F}_{m \text{ times}} & \to & J^m(X_F) \\ (x_1, \ldots, x_m) & \to & x_1 + \ldots + x_m; \end{array}$$

2. the addition morphism

$$J^n(X_F) \times_F J^m(X_F) \to J^{m+n}(X_F),$$

   compatible with the cycle class morphism;

3. the multiplication by N morphism

$$\mu_N : J^m(X_F) \to J^{mN}(X_F).$$

Any zero-cycle on X_F of degree m, defined over F, yields an F-rational point of $J^m(X_F)$; each point of X_F defined over an extension E/F of degree m gives such a point. The existence of such a cycle implies $[X_F] = [J^1(X_F)] \in H^1(\Gamma, J^0(X_F))$ has order dividing m [LT], §2, Prop. 5.

Definition 4.5 A *multisection* of an abelian fibration X_F is a point defined over a finite extension of F. The *degree* of the multisection is the smallest degree of an extension E/F over which the point can be defined. We shall identify multisections of degree d with collections of d conjugate points of $X(F^a)$

$$M = \{m_1, \ldots, m_d\}.$$

The zero-cycle $m_1 + \ldots + m_d$ is defined over F and thus yields an F-rational point of $J^d(X_F)$. If E/F is a degree-d extension over which some m_i is defined then we may consider the point

$$\tau_M = (m_1 + m_2 + \ldots + m_d) - dm_i \in J^0(X_F)(E).$$

This may be zero even when $d > 1$.

Definition 4.6 A multisection M of an abelian fibration X_F is *torsion* (resp. *degenerate*) if τ_M is torsion (resp. degenerate.) The *order* of a multisection is the smallest positive integer N such that $N(m_i - m_j) = 0$ for each $i, j = 1, \dots, d$. The order is *infinite* when no such integer exists.

Proposition 4.7 *A multisection is torsion if and only if it has finite order.*

Proof: Let L/F be a Galois extension containing E, and let $\tau_{M,i} \in J^0(X_F)(L)$ be associated to the various conjugate points $m_i, i = 1, \dots, d$. If one $\tau_{M,i}$ is torsion then all are, and we have

$$d(m_i - m_j) = \tau_{M,j} - \tau_{M,i},$$

so each $m_i - m_j$ must also be torsion. Conversely, if each $m_i - m_j$ is torsion then

$$\tau_{M,i} = \sum_{j=1}^{d} (m_j - m_i)$$

is also torsion. □

Proposition 4.8 *Let $M \subset X_F$ be a torsion multisection of order N. Then M is contained in a principal homogeneous space for $J^0(X_F)[N]$, the N-torsion subgroup scheme.*

Proof: Suppose that the multisection M has order N, so that $Nm_i = Nm_j$ for each i, j. Then multiplication by N

$$\mu_N : X = J^1(X_F) \to J^N(X_F)$$

takes M to a single point $\Sigma \in J^N(X_F)$, defined over F. It follows that $M \subset \mu_N^{-1}(\Sigma)$, which is a principal homogeneous space for $J^0(X_F)[N]$. □

Remark 4.9 A torsion multisection M in an abelian variety A need not be contained in the torsion of A, only in a principal homogeneous space for the torsion!

Remark 4.10 Given a multisection $M' = \{m_1, \dots, m_d\}$ of an abelian fibration X_F, it may happen that $m_i - m_j, i \neq j$, is torsion for certain pairs (i, j) but not all such pairs. Let N denote the smallest positive integer so that $N(m_i - m_j) = 0$ for each difference that is torsion. Then μ_N maps M' onto multisection $M \subset J^N(X_F)$, which is nontorsion if and only if M' is nontorsion. Furthermore, M' is contained in a $J^0(X_E)[N]$-principal homogeneous space over M, where E is the field of definition of M.

4.3 Potential density argument

Let B be a variety over a field of characteristic zero.

Definition 4.11 An *abelian fibration* $\eta : \overline{A} \to B$ is a projective morphism of varieties with generic fiber an abelian fibration over the function field of B. An abelian fibration of relative dimension one is an *elliptic fibration.*

A *multisection* is an irreducible closed subvariety $M \hookrightarrow \overline{A}$ so that the induced $M \to B$ is generically finite, i.e., the closure of a multisection of the generic fiber. A multisection of η is *nontorsion* or *nondegenerate* if the induced multisection of the generic fiber is.

Additional assumptions are necessary if one wants a good group law:

Definition 4.12 An abelian fibration $\eta : \overline{A} \to B$ is *Jacobian* if it satisfies the following conditions

1. η is a flat morphism;
2. the locus $A \subset \overline{A}$ where η is smooth admits a group law

$$A \times_B A \to A$$

with identity $0 : B \to A$.

For any abelian fibration admitting a rational section $0 : B \dashrightarrow \overline{A}$, there is a nonempty open subset $B' \subset B$ so that $\overline{A}_{B'} := \overline{A} \times_B B' \to B'$ is Jacobian, e.g., the open subset over which η is smooth. Given an arbitrary fibration $\overline{A} \to B$ with multisection M, after basechange to M there exists a rational section: the image of the diagonal in $M \times_B M \subset \overline{A} \times_B M$.

Proposition 4.13 *Let $\eta : \overline{A} \to B$ be an abelian fibration with multisection M, defined over a number field K. Assume that*

1. *M is nondegenerate;*
2. *K-rational points of M are dense.*

Then K-rational points of $\overline{A}$ are also dense.

In the case of an elliptic fibration, nondegeneracy and nontorsion are equivalent conditions.
Proof: After basechange to an open subset of M, we obtain a Jacobian abelian fibration $\overline{A}_M$ with a nondegenerate section τ_M. Thus $\mathbb{Z}\tau_M$ is dense in A_M and each multiple $n\tau_M$ has dense rational points. It follows that rational points in A_M are dense. Since A_M dominates $\overline{A}$, rational points in $\overline{A}$ are also dense. □

5 Fano varieties

In the remainder of this paper, we identify classes of algebraic varieties for which rational points are potentially dense.

Definition 5.1 A smooth projective variety X is Fano if ω_X^{-1} is ample.

Fano varieties admit no nontrivial étale covers [Ca] [De] and cannot dominate varieties of general type.

Here are the Fano varieties known to have potentially dense rational points:

Example 5.2 (Del Pezzo surfaces) Fano varieties of dimension two are called *Del Pezzo surfaces.* Classically, it was known that any Del Pezzo surface X is birational to $\mathbb{P}^2$, and thus has potentially dense rational points.

Example 5.3 (Cubic hypersurfaces) Nonsingular cubic hypersurfaces of dimension ≥ 2 are unirational and therefore have potentially dense rational points (Cor. 3.3).

Example 5.4 (Fano threefolds) Smooth Fano threefolds are known to be unirational, except in three cases [IP] (see also [HarT]):

1. quartic hypersurfaces in $\mathbb{P}^4$;
2. weighted hypersurfaces of degree six in $\mathbb{P}(1,1,1,2,3)$;
3. double covers of $\mathbb{P}^3$ totally branched over a sextic.

The first two cases admit elliptic fibrations over $\mathbb{P}^2$. Arguments similar to those in the second half of this survey prove potential density (see [HarT] and [BT2]). The third case remains completely open.

Example 5.5 ($\mathbb{Q}$-Fano threefolds) There are many examples remaining where potential density has not yet been studied. For example, there are altogether 95 different families of $\mathbb{Q}$-Fano hypersurfaces in weighted projective spaces. See [CPR] for a concrete account of their geometry.

6 K3 surfaces

Definition 6.1 A smooth projective surface X is a *K3 surface* if

1. $h^0(\Omega^1_X) = 0$;
2. $\omega_X \simeq \mathcal{O}_X$, i.e., the canonical bundle is trivial.

Such surfaces have been classified in great detail (see, for example, [BPV] VIII and [LP]). In particular, the underlying complex manifolds $X(\mathbb{C})$ are all deformation equivalent and simply connected. K3 surfaces do not dominate varieties of general type, so they could very well have potentially dense rational points.

A *polarization* f of X is a primitive, ample class in the Néron-Severi group $\mathrm{NS}(X)$. The degree of (X, f) is the self-intersection $f.f$, a positive even integer. The K3 surfaces of degree d admit common realizations as projective varieties.

Example 6.2
$d = 2$ a surface X admitting a degree-two cover $X \to \mathbb{P}^2$ branched over a smooth plane sextic curve.
$d = 4$ a nonsingular quartic hypersurface $X \subset \mathbb{P}^3$, e.g., $x_0^4 + x_1^4 = x_2^4 + x_3^4$.
$d = 6$ a complete intersection of quadric and cubic hypersurfaces in $\mathbb{P}^4$.

We summarize the known results for K3 surfaces:

Theorem 6.3 (Infinite automorphism group) *[BT3] Let X be a K3 surface defined over a number field. Assume that the complex manifold $X(\mathbb{C})$ admits an infinite automorphism group. Then rational points on X are potentially dense.*

A proof is sketched in §6.1.

Theorem 6.4 (Elliptic K3 surfaces) *[BT3] Let X be a K3 surface defined over a number field. Suppose that X admits an elliptic fibration $\eta : X \to \mathbb{P}^1$. Then rational points on X are potentially dense.*

More precise results on quartic surfaces containing a line (see Theorem 6.19) can be found in [HarT].

We give several approaches to Theorem 6.4; in each the key technical tool is the Tate-Shafarevich group, discussed in §7. The basic insight–that twisting an elliptic fibrations should make it easier to find rational points–is due to Bogomolov and Tschinkel. The first approach in §8 works primarily in the nonisotrivial case. It relies on the irreducibility of the p-torsion points for large p (see Theorem 8.3). One interesting by-product is the existence of rational multisections of unbounded degree (see Theorem 8.7 and its corollaries.) The second approach in §9 is perhaps the most natural, although logically it depends on the first. Essentially, one shows that torsion multisections have large genera so that rational multisections must be nontorsion. Our genus estimates for the p-torsion and the associated principal homogeneous spaces closely follow [BT3]. However, the presentation of the intermediate technical results and the analysis of the isotrivial cases differ to some extent. (Lemma 3.25 of [BT3] is not quite correct as stated: The Kummer surface associated to a product of general elliptic curves is a counterexample. This necessitates further *ad hoc* analysis in the isotrivial case.) The third approach in §10 is based on a letter of J. Kollár. Most of the detailed computation of the previous approaches is replaced by deformation-theoretic properties of rational and elliptic curves in K3 surfaces. The only classification results needed are the multiplicities of the components of degenerate fibers (see Figure 2 of §10).

Remark 6.5 (Conditional potential density for elliptic surfaces) Let $\iota : \overline{J} \to B$ be a nonisotrivial Jacobian elliptic fibration over a curve of genus zero or one. In particular, $\overline{J}$ is smooth and projective and ι admits a section (cf. §7.2). If $\overline{J}$ is defined over a number field we expect its rational points to be potentially dense. Indeed, Grant and Manduchi [GM1] [GM2] prove this conditionally, assuming a strong version of the Birch/Swinnerton-Dyer Conjecture formulated by Deligne and Gross. However, there are *isotrivial* elliptic fibrations $X \to \mathbb{P}^1$ for which rational points are known not to be potentially dense [CSS] (see example 3.7).

Remark 6.6 (Enriques surfaces) Potential density results for K3 surfaces have application to other classes of surfaces dominated by them. By definition, an *Enriques surface* Y is a quotient of a K3 surface X by a fixed-point free involution. Propositions 3.1 and 3.4 imply that potential density of rational points for X and Y are equivalent. For results on Enriques surfaces and their K3 double covers, we refer the reader to [BT1].

6.1 K3 surfaces with automorphisms

We sketch the proof of Theorem 6.3, following [BT3].

Lemma 6.7 Let X be a K3 surface. Then the automorphism group of X acts faithfully on the cohomology $H^2(X, \mathbb{Z})$. In particular, an automorphism $a : X \to X$ is uniquely determined by the homology class of its graph in $X \times X$.

This follows from the strong version of the Torelli Theorem for K3 surfaces (see [LP] for one account.)

Lemma 6.8 Let X be a K3 surface defined over a number field K. There exists a finite extension L/K so that each automorphism of the complex manifold $X(\mathbb{C})$ is realized as an algebraic morphism defined over L.

Proof: The automorphism group of X is finitely generated [St], so it suffices to show that any automorphism $a : X \to X$ can be defined over a finite extension of K. Choose a realization of $X \times X$ as a projective variety over K. The graph $\Gamma(a) \subset X \times X$ is a projective subvariety by the GAGA principle. Consider the connected component $\mathcal{H}$ of the Hilbert scheme of subschemes of $X \times X$ containing $\Gamma(a)$, which is defined over a finite extension L/K. The locus in $\mathcal{H}$ corresponding to graphs of automorphisms of X is clearly open, but $\Gamma(a)$ is the only graph of an automorphism of X in its homology class. It follows that $\mathcal{H} = [\Gamma(a)]$, so $\Gamma(a)$ and a are defined over L.□

Lemma 6.9 Let X be a K3 surface with infinite automorphism group. Then there exists an indecomposible effective divisor class D so that the orbit of D is infinite.

We refer the reader to §2 of [LP] for a good description of the indecomposible elements in the monoid of effective divisors on a K3 surface.
Proof: The indecomposible effective divisors D with fixed (even) $d := D.D \geq -2$ divide into a finite number of orbits under the action of the automorphism group [St]. Suppose that there exists such a divisor with $d > 0$. This is always the case when the effective cone admit an irrational extremal ray; just take indecomposible divisors near this ray. The automorphisms fixing such a D

admit a faithful representation in $D^\perp \subset \mathrm{NS}(X)$, a negative definite lattice by the Hodge index theorem. Thus each such stabilizer is finite.

Suppose X has no indecomposible effective divisors with $d > 0$. It follows that the effective cone of X is generated by divisors with $d = 0, -2$, permuted by the automorphism group. If the Néron-Severi group $\mathrm{NS}(X)$ had rank two, then the automorphism group would admit a subgroup of finite index fixing the generators of the effective cone, but all such automorphisms are trivial. If the Néron-Severi group has rank greater than two then we apply the 'alternative theorem' of Kovács [Ko]. Either X contains no (-2)-curves or the effective cone of X is generated by (-2)-curves. In the first case, the effective cone is 'circular' and admits an irrational extremal ray; hence the argument of the previous paragraph applies. In the second case, there must be an infinite number of (-2)-curves. If not, a finite index subgroup of the automorphism acts trivially on the effective cone, a contradiction. □

Lemma 6.10 Let X be a K3 surface and D an indecomposible effective divisor class. Then D contains a (possibly singular) rational curve.

Proof: In the case where $D.D = -2$ this is clear. When $D.D = 0$, D is the class of an elliptic fibration, which admits degenerate fibers. In the case where $D.D > 0$, we use the results of [MM]: A generic polarized K3 surface contains a singular rational curve in the polarization class f. However, since D is indecomposible with $D.D > 0$, (X, D) arises as the specialization of a polarized K3 surface. The rational curves of the polarized K3 surface specialize to rational curves on X in the class D. □

We complete the proof of Theorem 6.3. Let X be a K3 surface with infinite automorphism group, defined over a number field K. Let D be a indecomposible effective divisor class with infinite orbit under the automorphism group. Then after passage to a finite extension L/K, we may assume that

1. the automorphisms of X are defined over L;
2. there is a rational curve R with class $[R] = D$, defined over L, with dense rational points $R(L) \subset R$.

The orbit $\cup_{a \in \mathrm{Aut}(X)} a(R)$ is dense in X and L-rational points are dense in the orbit, so L-rational points are dense in X. □

Example 6.11 [Si] Consider K3 surfaces X, defined over a number field, which are realized as a complete intersection

$$X = \{F_{11} = 0\} \cap \{F_{22} = 0\} \subset \mathbb{P}^2 \times \mathbb{P}^2$$

of bihomogeneous forms of bidegree $(1, 1)$ and $(2, 2)$ respectively. The Néron-Severi lattice is

	f_1	f_2
f_1	2	4
f_2	4	2

where f_1 and f_2 are the pull-backs of the polarizations from the $\mathbb{P}^2$-factors. The projections $X \to \mathbb{P}^2$ are degree-two covers, and the corresponding pair of involutions generate an infinite group of automorphism on X. These K3 surfaces have potentially dense rational points.

More generally, we may consider K3 surfaces with Néron-Severi lattice

	f_1	f_2
f_1	2	n
f_2	n	2

with $n \geq 4$. These also admit pairs of noncommuting involutions.

6.2 Examples of elliptic K3 surfaces

Example 6.12 Harris and Tschinkel [HarT] consider the following special class of elliptic K3 surfaces. Let $X \subset \mathbb{P}^3$ be a quartic surface containing a line ℓ. Choose coordinates so that $\ell = \{(w, x, y, z) : w = x = 0\}$ and consider the morphism

$$\begin{aligned} \eta : \quad & X \to \mathbb{P}^1 \\ & (w, x, y, z) \to (w, x). \end{aligned}$$

This is an elliptic fibration: Each hyperplane containing ℓ intersects X in the union of ℓ and a cubic plane curve

$$\{w + \alpha x = 0\} \cap X = \ell \cup E_\alpha \quad E_\alpha \text{ a plane cubic curve.}$$

We have $\eta^{-1}(\alpha) = E_\alpha$ and E_α is a smooth genus one curve for generic α, hence η is an elliptic fibration.

A particularly simple example is the Fermat surface $x_0^4 + x_1^4 = x_2^4 + x_3^4$, which contains the line $x_0 - x_2 = x_1 - x_3 = 0$.

Of course, there are numerous other examples of elliptic K3 surfaces. We give characterizations of elliptic K3 surfaces in Proposition 11.1.

6.3 Salient ramification and torsion multisections

In this section, we sketch some particularly elegant geometric methods for finding nontorsion multisections. We work in characteristic zero.

Definition 6.13 [BT1] Consider an elliptic fibration $\eta : X \to \mathbb{P}^1$ and a multisection M. We say that M is *saliently ramified* if $M \to \mathbb{P}^1$ ramifies over a point in a smooth fiber of η.

Proposition 6.14 *Let $\eta : X \to \mathbb{P}^1$ be an elliptic fibration and M a saliently ramified multisection. Then M is nontorsion.*

Proof: Consider the fibration

$$X \times_{\mathbb{P}^1} M \to M$$

obtained after base change. This has a section (see §4.3). If the morphism $M \to \mathbb{P}^1$ ramifies at m then the morphism $M \times_{\mathbb{P}^1} M \to M$ ramifies at (m, m). Indeed, for a finite flat morphism, ramification occurs precisely where the cardinality of fibers drops; this cardinality is unchanged under base extension. (Also, being ramified is a local property in the faithfully flat topology [EGAIV] 17.7.4.) Observe that we do *not* normalize $M \times_{\mathbb{P}^1} M$, as this would destroy some of the ramification.

However, the torsion of any group scheme in characteristic zero is étale over the base, and we have a contradiction. □

Combining this with Proposition 4.13, we obtain:

Corollary 6.15 Let $\eta : X \to \mathbb{P}^1$ be an elliptic fibration, defined over a number field. Assume that η admits a saliently ramified multisection of genus zero or one. Then rational points of X are potentially dense.

Remark 6.16 This approach has advantages and disadvantages. The main disadvantage is the difficulty in producing saliently ramified multisections for large classes of varieties: In general, there is no easy way to produce them out of 'thin air'.

The main advantage is that, once we are given a multisection, it is relatively easy to check whether it is saliently ramified. Furthermore, if X, η, and M are defined over K and $M(K)$ is dense, then $X(K)$ is also dense. This gives a good tool for checking density over a *given* field.

6.4 Reprieve: Quartic surfaces containing a line

We return to Example 6.12, again following [HarT]. Assume that the quartic surface X and the line ℓ are defined over a number field K. The line ℓ itself intersects fibers of η in three points and defines a degree-three multisection. This multisection is saliently ramified provided the following geometric condition is satisfied:

> **Tangency condition** Some *smooth* fiber of η intersects the line ℓ tangentially.

Rational points of $\ell \simeq \mathbb{P}^1$ are clearly dense over K, so the Tangency condition suffices to guarantee density of $X(K)$.

The geometric condition is satisfied for the *generic* quartic surface containing a line–but not every such surface. It fails for the Fermat surface $x_0^4 + x_1^4 = x_2^4 + x_3^4$ with $\ell = \{x_0 - x_2 = x_1 - x_3 = 0\}$. The morphism $\eta : X \to \mathbb{P}^1$ is given by the rational function

$$\frac{x_0 - x_2}{x_3 - x_1} = \frac{x_1^3 + x_1^2 x_3 + x_1 x_3^2 + x_3^3}{x_0^3 + x_0^2 x_2 + x_0 x_2^2 + x_2^3}.$$

Taking x_0 and x_1 as coordinates on ℓ, the rational function restricts to x_1^3/x_0^3, which ramifies (to order three) at the points $(1,0,1,0)$ and $(0,1,0,1)$. Here the fibers of η are three coincident lines.

Combining the analysis of the salient ramification with a case-by-case study of the possible torsion multisections, Harris and Tschinkel obtain the following:

Theorem 6.17 ([HarT] Theorem 4.1) *Let X be a smooth quartic surface containing a line ℓ and $\eta : X \to \mathbb{P}^1$ the elliptic fibration obtained by projecting from ℓ. Assume there do not exist six lines contained in X and meeting ℓ. Then ℓ is a nontorsion multisection of ℓ.*

Corollary 6.18 ([HarT] Theorem 1.5.a) Retain the assumptions above, and assume that X and ℓ are defined over a number field K. Then the rational points $X(K)$ are dense.

After further analysis of degenerate cases, Harris and Tschinkel prove the following general result, which is a special case of Theorem 6.4:

Theorem 6.19 *Let X be a smooth quartic surface defined over a number field. If X contains a line ℓ then rational points of X are potentially dense.*

7 Twisting elliptic fibrations

7.1 The Tate-Shafarevich group

We refer the reader to [Kod], [Shaf1], and [Ogg] for full details.

Let $F = \mathbb{C}(\mathbb{P}^1)$ be the function field of $\mathbb{P}^1$, with absolute Galois group Γ. Let $(J_F, 0)$ be an elliptic curve over F. The *Tate-Shafarevich group* $\mathrm{Sh}(J_F)$ is defined as the J_F-principal homogeneous spaces which are locally trivial at each place, i.e., the kernel

$$H^1(\Gamma, J_F) \to \prod_{b\in\mathbb{P}^1} H^1(\hat{\Gamma}_b, J_{\hat{F}_b})$$

where $\hat{F}_b$ is the completion/henselization of F at b and $\hat{\Gamma}_b$ its absolute Galois group.

We recall some properties of $\mathrm{Sh}(J_F)$.

Proposition 7.1 *1) Let X_F be a J_F-principal homogeneous space. Then $[X_F] \in H^1(\Gamma, J_F)$ has order m if and only if there is a point of X_F defined over a field extension of degree m.*
2) There are exact sequences

$$\begin{array}{ccccccccc} 0 & \to & J_{\hat{F}_b}(\hat{F}_b)/mJ_{\hat{F}_b}(\hat{F}_b) & \to & H^1(\hat{\Gamma}_b, J_{\hat{F}_b}[m]) & \to & H^1(\hat{\Gamma}_b, J_{\hat{F}_b})[m] & \to & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \to & J_F(F)/mJ_F(F) & \to & H^1(\Gamma, J_F[m]) & \to & H^1(\Gamma, J_F)[m] & \to & 0. \end{array}$$

3) $\mathrm{Sh}(J_F)$ *is infinitely divisible.*

Proof: We have already seen that $J^m(X_F)(F) \neq \emptyset$ whenever X_F has a point over a degree m extension of F. Conversely, suppose we have an F-rational point of $J^m(X_F)$. Such a point need not come from a line bundle L on X_F defined over F; the obstruction lies in the Brauer group of F (by the Hochschild-Serre spectral sequence

$$0 \to H^1(\mathcal{O}^*_{X_F}) \to H^0(\Gamma, H^1(\mathcal{O}^*_{X_{Fa}})) \to H^2(\Gamma, H^0(\mathcal{O}^*_{X_{Fa}})) = H^2(\Gamma, F^{a*}).)$$

The Brauer group of $F = \mathbb{C}(\mathbb{P}^1)$ is trivial because it is a C^1 field. The Riemann-Roch formula applied to L gives a degree-m cycle on X_F.

The second assertion is quite standard (see §1, 2.1 of [Shaf1]). The third statement may be found in [Shaf1] §2.5. It uses the fact that there are no nontrivial families of elliptic curves over $\mathbb{P}^1$ without degenerate fibers. □

In light of the exact seqences above, the reduction homomorphism

$$H^1(\Gamma, J_F[m]) \to H^1(\hat{\Gamma}_b, J_{\hat{F}_b}[m])$$

can often shed light on Tate-Shafarevich group:

Proposition 7.2 (Corollary of [Shaf1], §1.2.) *Let $\hat{F} = \mathbb{C}((t))$ with absolute Galois group $\hat{\Gamma}$, and $J_{\hat{F}}$ an elliptic curve over $\hat{F}$. Then for each m*

$$|H^1(\hat{\Gamma}, J_{\hat{F}}[m])| = |J_{\hat{F}}[m]|.$$

7.2 Models of elliptic surfaces

Recall that an elliptic fibration $\eta : X \to \mathbb{P}^1$ is *relatively minimal* if its fibers contain no (-1)-curves, i.e., K_X is numerically effective relative to η. Given an elliptic curve X_F over $F = \mathbb{C}(\mathbb{P}^1)$, there is a unique (smooth, projective) relatively minimal model $\eta : X \to \mathbb{P}^1$. In particular, for each elliptic fibration $\eta : X \to \mathbb{P}^1$ there is an associated Jacobian fibration $\iota : \overline{J} \to \mathbb{P}^1$, which admits a zero-section. It is obtained by taking the relative minimal model of the Jacobian $J_F := J^0(X_F)$. We also have $J^m(X)$, associated to $J^m(X_F)$. Multiplication by N,

$$\mu_N : J^m(X_F) \to J^{mN}(X_F),$$

induces a dominant rational map over $\mathbb{P}^1$

$$\mu_N : J^m(X) \dashrightarrow J^{mN}(X).$$

Definition 7.3 Let $\eta : X \to \mathbb{P}^1$ be a relatively minimal elliptic fibration. A fiber $\eta^{-1}(b), b \in \mathbb{P}^1$, is *multiple* if each of its irreducible components has multiplicity > 1.

A Jacobian fibration always has a zero section, and thus has no multiple fibers. A fiber may have some nonreduced irreducible components without being multiple.

Proposition 7.4 *Let* $X \to \mathbb{P}^1$ *be a relatively minimal elliptic fibration. Then* X *has no multiple fibers if and only if* X_F *is an element of* $\mathrm{Sh}(J(X_F))$.

Proof: The fiber $\eta^{-1}(b)$ is not multiple if and only if η has a section in an analytic/étale neighborhood of b. This is equivalent to $X_{\hat{F}_b} \neq \emptyset$. □

Proposition 7.5 *Let* $\eta : X \to \mathbb{P}^1$ *be an elliptic surface without multiple fibers, with Jacobian* J_F. *Then* $m[X_F] = 0$ *in* $\mathrm{Sh}(J_F)$ *if and only if there is a multisection* $M \subset X$ *of relative degree* m *over* $\mathbb{P}^1$.

Proof: The first part of Proposition 7.1 gives this; M is obtained by taking the closure of the cycle in X_F of relative degree m. □

Proposition 7.6 *Let* $\eta : X \to \mathbb{P}^1$ *be a relatively minimal elliptic fibration without multiple fibers, with Jacobian fibration* $\iota : \overline{J} \to \mathbb{P}^1$. *For each* $b \in \mathbb{P}^1$, X *and* $\overline{J}$ *are isomorphic over an analytic/étale neighborhood of* b.

Proof: Since X and $\overline{J}$ are relatively minimal, they remain relatively minimal after completion/henselization, and minimal models of surfaces (and Néron models of elliptic curves) are unique. □

We remarked in Proposition 7.1 that $\mathrm{Sh}(J_F)$ is infinitely divisible for an elliptic curve J_F over $F = \mathbb{C}(\mathbb{P}^1)$. The precise structure of this group admits an elegant interpretation in terms of the transcendental cohomology of the compact Kähler manifold $\overline{J}$:

Proposition 7.7 *([Shaf2] § VII.8, Theorems 11 and 12,[Shi]) Let* $\overline{J} \to \mathbb{P}^1$ *be a nontrivial Jacobian elliptic surface with generic fiber* J_F. *Then*

$$\mathrm{Sh}(J_F) = H^2(\overline{J}, \mathbb{Z})_{\mathrm{tran}} \otimes \mathbb{Q}/\mathbb{Z},$$

where

$$H^2(\overline{J}, \mathbb{Z})_{\mathrm{tran}} = H^2(\overline{J}, \mathbb{Z})/(H^2(\overline{J}, \mathbb{Z}) \cap H^1(\overline{J}, \Omega^1_{\overline{J}})) = H^2(\overline{J}, \mathbb{Z})/\mathrm{NS}(\overline{J}),$$

the integral classes modulo the Néron-Severi group.

Remark 7.8 For elliptic K3 surfaces, the formula

$$\mathrm{Sh}(J_F) \simeq (\mathbb{Q}/\mathbb{Z})^e, \quad e = \mathrm{rank}\ H^2(\overline{J}, \mathbb{Z})_{\mathrm{tran}}$$

may also be deduced from the Ogg-Shafarevich formula ([Shaf1] §2.3, Theorem 3, [Ogg] Theorem 2) and the formula for the rank of the transcendental classes quoted in §7.4 [SI]. This allows us to deduce e from the rank of J_F and the degenerate fibers of $\overline{J} \to \mathbb{P}^1$.

7.3 Twisting elliptic K3 surfaces

Proposition 7.9 *An elliptic K3 surface $\eta : X \to \mathbb{P}^1$ is relatively minimal and never has multiple fibers.*

Proof: The relative minimality follows because $K_X = 0$. We may then use the classification of singular fibers for minimal elliptic surfaces [BPV] pp. 151. The possible multiple fibers take the form mD, where D is one of the degenerate fibers enumerated in Kodaira's classification. Now $D \subset X$ is effective and numerically effective, with self-intersection $D.D = 0$. The classification theory of linear series on K3 surfaces [SD] implies $|D|$ induces an elliptic fibration (cf. Proposition 11.1). □

Proposition 7.10 *Let X be a smooth projective variety, $\eta : X \to \mathbb{P}^1$ a relatively minimal elliptic fibration, and $\iota : \overline{J} \to \mathbb{P}^1$ its Jacobian fibration. If X is a K3 surface then $\overline{J}$ is a K3 surface. If $\overline{J}$ is a K3 surface and X has no multiple fibers then X is a K3 surface.*

Proof: Proposition 7.9 and our assumptions imply that X and $\overline{J}$ are both relatively minimal elliptic surfaces without multiple fibers. In particular, they have isomorphic fibers (cf. Prop. 7.6.) The topological Euler characteristics $\chi(X)$ and $\chi(\overline{J})$ are therefore equal. Both $\overline{J}$ and X are elliptic surfaces, so $K^2_{\overline{J}} = K^2_X = 0$ and Noether's formula implies $\chi(\mathcal{O}_X) = \chi(\mathcal{O}_{\overline{J}}) = 2$. The canonical bundle formula for elliptic surfaces [BPV] V.12.1,12.2 implies $K_X = 0$ if and only if $K_{\overline{J}} = 0$. Any surface with $K = 0$ and $\chi(\mathcal{O}) = 2$ is a K3 surface. □

Remark 7.11 Let B be a smooth projective curve, $X \to B$ an abelian fibration, and $\overline{J} \to B$ the Néron model of its Albanese. Then $h^i(X, \omega_X) = h^i(\overline{J}, \omega_{\overline{J}})$ for each i (by [Kol2], Theorem 2.6 and Corollary 3.2).

One distinguishing property of elliptic K3 surfaces is that they admit *rational* multisections.

Proposition 7.12 *Let $X \to \mathbb{P}^1$ be an elliptic K3 surface with Jacobian J_F, so that $[X_F] \in \mathrm{Sh}(J_F)$ has order m. Then there exists a rational multisection $M \subset X$ of relative degree m.*

Proof: Proposition 7.5 gives a multisection $\hat{M}$ of relative degree m. There exists an indecomposible effective divisor class D so that $\hat{M} - D$ is effective and D has positive degree over the base. It must have degree exactly m

because the order of $[X_F]$ equals m. Lemma 6.10 implies D contains an irreducible rational curve M. □

Combining Propositions 7.10, 7.5, and 7.7 with the multiplication map introduced in §7.2, we obtain

Corollary 7.13 Let $X \to \mathbb{P}^1$ be an elliptic K3 surface, with Jacobian $\overline{J}$ and generic fiber J_F. For each integer N, there exists an elliptic K3 surface $X' \to \mathbb{P}^1$ with Jacobian $\overline{J}$ so that

$$N[X'_F] = [X_F] \text{ and order } [X'_F] = N \cdot \text{ order } [X_F]$$

in $\mathrm{Sh}(J_F)$. There is a dominant rational map $X' \dashrightarrow X$ over $\mathbb{P}^1$.

7.4 Results of Shioda-Inose

To compute transcendental cohomology and the Tate-Shafarevich group in particular examples, we use the following (see [SI]):

Proposition 7.14 *Let $\eta : X \to \mathbb{P}^1$ be a elliptic K3 surface with Jacobian $\iota : \overline{J} \to \mathbb{P}^1$. Then the Néron Severi group has rank*

$$\textit{rank}\ \mathrm{NS}(X) = 2 + r(J_F) + \sum_b (m_b - 1)$$

and the topological Euler characteristic is

$$\chi(X) = 24 = \sum_b \epsilon_b,$$

where $r(J_F)$ is the rank of the group of sections and m_b and ϵ_b are given by the following table:

Kodaira type	$I_a, a > 0$	II	III	IV	$I_a^*, a \geq 0$	II^*	III^*	IV^*
m_b	a	1	2	3	$a+5$	9	8	7
ϵ_b	a	2	3	4	$a+6$	10	9	8

Subtracting the two formulas of Proposition 7.14 we obtain find

Corollary 7.15 Let $\eta : X \to \mathbb{P}^1$ be an elliptic K3 surface. Let N_1 denote the number of degenerate fibers of type $I_a, a > 0$, and N_2 the number of degenerate fibers of other types. Then we have

$$\text{rank } \mathrm{NS}(X) + N_1 + 2N_2 = 26 + r(J_F).$$

7.5 A remark on Fourier-Mukai transforms

Perhaps the simplest way to construct isogenies of K3 surfaces is by taking twists of elliptic fibrations. This is not widely known, so we give a brief account here.

By definition, two K3 surfaces X and Y are *isogenous* if the Hodge structures $H^2(X)$ and $H^2(Y)$ are isomorphic over $\mathbb{Q}$. A natural problem, first studied systematically by Mukai [Mu], is how such isogenies are induced by correspondences between X and Y. Indeed the Hodge conjecture, applied to $X \times Y$, predicts that each isogeny between X and Y should be induced by an algebraic cycle, which ideally should admit a geometric description. Typically, Y arises as a moduli space of simple sheaves on X, with the isogeny induced by Chern classes of the universal bundle on $X \times Y$.

Assume that $\iota : \overline{J} \to \mathbb{P}^1$ is a Jacobian elliptic K3 suface and $\eta : X \to \mathbb{P}^1$ represents an element $[X_F] \in \mathrm{Sh}(J_F)$ of order $m > 1$. We interpret $\overline{J}$ as $J^m(X)$, the degree-m component of the Picard group relative to η. The generic point of $\overline{J}$ parametrizes a line bundle $\mathcal{L}$ of degree m supported on some fiber of η. We extract a simple sheaf $\mathcal{E}$ from the kernel of the global section map

$$0 \to \mathcal{E} \to H^0(X, \mathcal{L}) \otimes \mathcal{O}_X \to \mathcal{L} \to 0,$$

with rank m and Chern classes $c_1(\mathcal{E}) = -D$ and $c_2(\mathcal{E}) = m$, where D is the class of a fiber of η. The moduli space of such sheaves is the K3 surface $\overline{J}$.

We recall Mukai's procedure for computing the isogeny between X and $\overline{J}$. Consider

$$\Lambda := \{a \in H^2(X, \mathbb{Z}) : a.D \equiv 0 \pmod{m}\} \subset H^2(X, \mathbb{Z}),$$

a sublattice of index m. We assumed that $[X_F] \in \mathrm{Sh}(J_F)$ has order m, so the algebraic classes

$$H^2(X, \mathbb{Z})_{\mathrm{alg}} := H^2(X, \mathbb{Z}) \cap H^1(X, \Omega^1_X) \subset \Lambda.$$

Set $D' = D/m$ and take Λ' to be the lattice obtained from Λ by adjoining D', so that Λ'/Λ is cyclic of order m. Observe also that

1. The intersection form on $H^2(X, \mathbb{Z})$ induces quadratic forms on Λ and Λ'; the form on Λ' is integral and unimodular.

2. $\Lambda \otimes \mathbb{C}$ and $\Lambda' \otimes \mathbb{C}$ inherit Hodge structures from $H^2(X)$, so we may define Λ_{alg} (resp. Λ'_{alg}) as the integral $(1,1)$-classes and $\Lambda_{\mathrm{tran}} = \Lambda/\Lambda_{\mathrm{alg}}$ (resp. $\Lambda'_{\mathrm{tran}} = \Lambda'/\Lambda'_{\mathrm{alg}}$).

3. $D' \in \Lambda'_{\mathrm{alg}}$ with $D' \cdot D' = 0$, and there exists a class $\Sigma \in \Lambda'_{\mathrm{alg}}$ with $D' \cdot \Sigma = 1$ (see Proposition 7.5).

4. $\Lambda_{\mathrm{tran}} = \Lambda'_{\mathrm{tran}}$ and $\Lambda_{\mathrm{tran}} \subset H^2(X, \mathbb{Z})_{\mathrm{tran}}$ so that the quotient is cyclic of order m.

Indeed, Mukai proves that Λ' is the Hodge structure for the moduli space of sheaves of type $\mathcal{E}$, which coincides with the Jacobian elliptic fibration $\overline{J}$. Finally, $H^2(X, \mathbb{Z})_{\mathrm{tran}}/H^2(\overline{J}, \mathbb{Z})_{\mathrm{tran}}$ is cyclic of order m and thus determines an element of $H^2(\overline{J}, \mathbb{Z})_{\mathrm{tran}} \otimes (\mathbb{Q}/\mathbb{Z})$ of order m. This coincides with the element alluded to in Proposition 7.7.

8 Approach I: Irreducibility of torsion in the nonisotrivial case

8.1 Group-theoretic results

We use the notation of the Appendix, in particular, the exact sequence

$$1 \to (\mathbb{Z}/p\mathbb{Z})^{\oplus 2} \to \mathrm{AffSL}_2(\mathbb{Z}/p\mathbb{Z}) \stackrel{q}{\to} \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \to 1, \tag{1}$$

with splitting $\sigma : \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \hookrightarrow \mathrm{AffSL}_2(\mathbb{Z}/p\mathbb{Z})$.

Proposition 8.1 *Let $p \neq 2, 3$ be prime. Let $H' \subset \mathrm{AffSL}_2(\mathbb{Z}/p\mathbb{Z})$ be a subgroup with $q(H') = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Then one of the following is true:*

1. *there is a point in $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$ fixed by each element in H', so this group is conjugate to $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$;*

2. *$H' = \mathrm{AffSL}_2(\mathbb{Z}/p\mathbb{Z})$.*

Proof: First, assume that $q : H' \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ has nontrivial kernel. Each element of the kernel is in $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2} \subset \mathrm{AffSL}_2(\mathbb{Z}/p\mathbb{Z})$ and acts via translation by a nonzero element $v \in (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$. Any other nonzero element $w \in (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$ can be obtained by applying an element of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, which acts by conjugation on $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2} \subset \mathrm{AffSL}_2(\mathbb{Z}/p\mathbb{Z})$. The surjectivity assumption implies w can also be obtained conjugating with an element of H'. Hence every translation is contained in H' and the second alternative holds.

Now we assume $q : H' \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is an isomorphism. Consider the action of $H' \simeq \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ on polynomials over $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$ of degree ≤ 1

$$c_0 + c_1 x_1 + c_2 x_2, \quad c_0, c_1, c_2 \in \mathbb{Z}/p\mathbb{Z}.$$

We claim the resulting representation is completely reducible

$$\langle 1 \rangle \oplus \langle x_1 - v_1, x_2 - v_2 \rangle, \quad \dagger$$

where (v_1, v_2) is the fixed point of the action. We know that $\phi(-I)$, where I is the identity, is semisimple and the ± 1-eigenvalue decomposition of the linear polynomials takes the form $\dagger$. It suffices to show that every other element of H' respects this decomposition. Consider

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad T = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

which *generate* $\mathrm{SL}_2(\mathbb{Z})$; [Se1] §7.1 contains a proof they generate $\mathrm{SL}_2(\mathbb{Z})/\pm I$ and they obviously yield $\pm I$. These matrices therefore generate $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ as well, so it suffices to show they respect decomposition $\dagger$. These matrices are semisimple over $\mathbb{Z}/p\mathbb{Z}$ and satisfy the relations

$$S^2 = T^3 = -I,$$

i.e., they have eigenspace decompositions respecting our decomposition. $\square$

Proposition 8.2 *For any proper subgroup $H \subsetneq \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, the index of H is at least p.*

Proof: We have $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ the symmetric group $\mathfrak{S}_3$ and $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ a central extension of the alternating group A_4 by a group of order two. The result holds in these special cases, so we may restrict attention to cases where $p \neq 2, 3$. Let $r = \mathrm{index}(H) = |\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})/H|$ and consider the associated coset representation

$$\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \to \mathfrak{S}_r.$$

The kernel $K \subset \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ is a normal subgroup, as is its image $K' \subset \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})/\langle \pm I \rangle$. For $p > 3$ the group $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})/\langle \pm I \rangle$ is simple, so either K' is trivial or the entire group, which is impossible. If K' is trivial then $|\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})/\langle \pm I \rangle| = p(p^2-1)/2$ divides $r!$, so the index $r \geq p$. $\square$

8.2 Irreducibility of torsion

Throughout this section, F denotes the function field of $\mathbb{P}^1$. We consider the irreducibility of certain schemes over F:

Theorem 8.3 *Let $\overline{J} \to \mathbb{P}^1$ be a nonisotrivial Jacobian elliptic fibration, with generic fiber J_F. Let p be a sufficiently large prime number.*

1. *The nonzero p-torsion $J_F[p] - \{0\}$ is irreducible.*

2. *Any nontrivial $J_F[p]$-prinicipal homogeneous space P_F is irreducible.*

Proof: Let $U \subset \mathbb{P}^1$ be the open subset over which the fibration is smooth. Consider the monodromy representation

$$\varrho : \pi_1(U) \to \mathrm{SL}_2(\mathbb{Z}),$$

with image Γ'.

Lemma 8.4 $\Gamma' \subset \mathrm{SL}_2(\mathbb{Z})$ has finite index.

Proof: Let $V \to U$ be the covering space with covering group Γ', so that $U = \Gamma' \setminus V$. The pull-back of $\overline{J}$ to V has trivial monodromy, so we have

$$\begin{array}{ccc} V & \to & H \\ \downarrow & & \downarrow \\ U & \stackrel{j}{\to} & \mathbb{A}^1 \simeq \mathrm{SL}_2(\mathbb{Z}) \setminus H \end{array}$$

where H is the upper half plane and $\mathbb{A}^1$ is the j-line. Both vertical maps are Γ'-equivariant, so we have a factorization

$$\begin{array}{ccccc} & & \Gamma' \setminus H & & \\ & \nearrow & & \searrow & \\ U & & \stackrel{j}{\longrightarrow} & & \mathrm{SL}_2(\mathbb{Z}) \setminus H. \end{array}$$

Since j has finite degree, Γ' has finite index.$\square$

In the sequel, we take Γ to be the absolute Galois group of the function field $F = \mathbb{C}(\mathbb{P}^1)$. The profinite completion of the fundamental group $\pi_1(U)$ is a quotient of Γ, corresponding to the maximal extension of F unramified over U. The (mod p) reduction of the monodromy

$$\rho : \pi_1(U) \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$$

factors through the profinite completion and induces a representation

$$\Gamma \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}).$$

We use the notation of the Appendix. The p-torsion $J_F[p]$ is a Γ-twist of $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$ and is classified by a representation $\alpha : \Gamma \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, which coincides with the representation $\rho(\mathrm{mod}\ p)$.

Lemma 8.5 For sufficiently large primes p, α is surjective.

This proves the first assertion of the Theorem.
Proof of lemma: The index of $\alpha(\Gamma)$ in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ divides the index of Γ' in $\mathrm{SL}_2(\mathbb{Z})$. By Proposition 8.2, any proper subgroup of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ has index at least p. It follows that $\alpha(\Gamma) = \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ for p greater than the index. The irreducible components of $J_F[p] - \{0\}$ correspond to the orbits of $\alpha(\Gamma)$ on $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2} - \{0\}$. $\square$

To each $J_F[p]$-principal homogenenous space P_F, Proposition A.2 assigns a representation $\phi : \Gamma \to \mathrm{AffSL}_2(\mathbb{Z}/p\mathbb{Z})$ with $q \circ \phi = \alpha$.

Lemma 8.6 For sufficiently large primes p, ϕ is surjective provided P_F is nontrivial.

Then $\phi(\Gamma)$ acts transitively on $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$ and P_F is irreducible, and the second assertion of the Theorem is proved.
Proof of lemma: We may assume α is surjective. If $\phi(\Gamma)$ were contained in some conjugate of $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \subset \mathrm{AffSL}_2(\mathbb{Z}/p\mathbb{Z})$, then it would fix an element of $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$, contradicting the nontriviality of P_F. Then Proposition 8.1 implies $\phi(\Gamma) = \mathrm{AffSL}_2(\mathbb{Z}/p\mathbb{Z})$. $\square$

8.3 Production of rational multisections

To prove potential density for an elliptic K3 surface $\eta : X \to \mathbb{P}^1$, we produce a plethora of rational multisections, with the hope that some might be nontorsion. The next result gives an infinite sequence of such multisections, with unbounded degree.

Theorem 8.7 *Let $X \to \mathbb{P}^1$ be a nonisotrivial elliptic K3 surface, with Jacobian fibration $\overline{J} \to \mathbb{P}^1$ and generic fiber J_F. Suppose that $[X_F] \in \mathrm{Sh}(J_F)$ has order m and let $p \gg m$ be prime. Then there exists a rational, nontorsion, multisection $M \subset X$ of degree mp.*

Combining this with Proposition 4.13, we easily deduce the following special case of Theorem 6.4:

Theorem 8.8 *Let $\eta : X \to \mathbb{P}^1$ be a nonisotrivial elliptic K3 surface over a number field K. Then rational points of X are potentially dense.*

Proof of Theorem 8.7: Corollary 7.13 yields an elliptic K3 surface $X' \to \mathbb{P}^1$ with Jacobian $\overline{J}$ so that

$$\text{order } [X'_F] = p \cdot \text{order } [X_F] \text{ and } p[X'_F] = [X_F]$$

as well as a dominant rational map

$$\mu_p : X' \dashrightarrow J^p(X') = X.$$

Proposition 7.12 gives a rational curve $M' \subset X'$ of relative degree mp. Let M be the image $\mu_p(M')$, which is also a rational curve, and consider the induced finite morphism

$$\mu_p : M' \to M.$$

Lemma 8.9 μ_p maps M' birationally onto M, which thus has degree mp over $\mathbb{P}^1$.

Proof of lemma: Suppose not, so that M has degree strictly smaller than mp. Since $[X_F] \in \mathrm{Sh}(J_F)$ has order m, Proposition 7.5 guarantees M has relative degree equal to m. Furthermore, the induced $M' \to M$ has degree p.

Let $\{m'_1, \ldots, m'_{mp}\}$ denote the geometric points of M'_F, lying over the generic point of the base $\mathbb{P}^1$. Since $\mu_p(m'_{i_1}) = \mu_p(m'_{i_2})$ for some $i_1 \neq i_2$, we deduce that some of the $m'_{i_1} - m'_{i_2}$ are p-torsion, e.g., the points lying over a given $m_i \in M_F$. We basechange to M to obtain a elliptic fibration $X' \times_{\mathbb{P}^1} M \to M$. Using the inclusion and the map μ_p, imbed $M' \hookrightarrow X' \times_{\mathbb{P}^1} M$ so the image is a p-torsion multisection of degree p over M. Let E denote the function field of M, a degree m extension of F, and J_E the basechange of J_F to E. Then M'_E is contained in a principal homogeneous space P_E for $J_E[p]$ (see Remark 4.10).

We analyze the structure of $J_E[p]$. First, if p is chosen sufficiently large, we may assume the monodromy representation

$$\alpha : \Gamma \to \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$$

is surjective (see Lemma 8.5). By Proposition 8.2, the degree-m extension E/F is linearly disjoint from the $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ extension of F associated with $J_F[p]$. Indeed, the associated Galois extension of F has no subextensions with degree dividing m. Hence, even after base extension to E, the monodromy representation still surjects onto $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$.

We return to the principal homogeneous space P_E. If it is trivial then Theorem 8.3 shows it has just two components, the identity and the non-identity, neither of which has degree p. If it is nontrivial then an application of Proposition 8.1, as in the argument for Lemma 8.6, shows it is irreducible with just one component of degree p^2. In either case we deduce a contradiction, so M must be a multisection of degree mp in X. □

It remains to show that M is nontorsion, which is the case if M' is nontorsion:

Lemma 8.10 $M' \subset X'$ is nontorsion.

Proof of lemma: Suppose that M' is torsion of order N, so that $\mu_N(M') \subset J^N(X')$ is a section. Proposition 7.5 implies that $mp = \mathrm{order}[X'_F]$ divides N. Write $N = np$ and consider the image

$$M'' = \mu_n(M') \subset J^n(X'),$$

a multisection of order p and degree $d > 1$, where $d|mp$. By Proposition 4.8, M'' is contained in a principal homogeneous space P_F for the p-torsion $J_F[p]$. We apply Theorem 8.3: If P_F is nontrivial then it is irreducible of degree p^2 and $p|m$, a contradiction. If P_F is trivial then $d = p^2 - 1$, whence $(p^2-1)|m$, a contradiction. □

Remark 8.11 For the application to Theorem 8.8, we only really need M' to be nontorsion. Then we may apply Proposition 4.13 to X' and potential density for X follows from Proposition 3.1. (If X is defined over a number field then X' and M' are as well.)

The precise description of the multisection M does give interesting consequences:

Corollary 8.12 Every nonisotrivial elliptic K3 surface contains an infinite number of irreducible rational curves.

Corollary 8.13 For each nonisotrivial Jacobian elliptic K3 surface with Néron-Severi group of rank two, there exists an infinite sequence of irreducible rational curves with decomposible divisor classes.

These cannot be (-2)-curves [LP] §2.

Proof of corollary: A Jacobian elliptic K3 surface with Néron-Severi rank two has effective cone generated by the classes of a fiber E and the zero section Σ [SD]

$$\begin{array}{c|cc} & E & \Sigma \\ \hline E & 0 & 1 \\ \Sigma & 1 & -2 \end{array}.$$

Thus any multisection of relative degree > 1 is decomposible. □

9 Approach II: genus estimates

Before diving into technical details, we indicate the main idea of this approach. Consider the modular curve

$$X_1(n) = \{(E, P) : E \text{ an elliptic curve }, P \in E \text{ of order } n\}/\simeq.$$

Any family of elliptic curves $\mathcal{E} \to B$ with n-torsion section gives a morphism $B \to X_1(n)$. For large primes $X_1(p)$ has positive genus [Miy] §4.2, so there are no nonisotrivial families of elliptic curves with p-torsion section over $\mathbb{P}^1$. We shall prove similar results for torsion multisections: If they have large torsion order they must have positive genus.

9.1 The Riemann-Hurwitz formula

Let F be the function field of a smooth projective curve B, M_F a finite reduced scheme over F, M the normalization of B in the fraction ring of M_F, and $f : M \to B$ the induced finite morphism. We do not assume M is irreducible. The *genus* $g(M_F)$ is defined as the arithmetic genus of M, and is computed by the Riemann-Hurwitz formula

$$2g(M) - 2 = \deg(f)(2g(B) - 2) + \sum_{m \in M} e_m,$$

where e_m is the local ramification order at m.

Let Γ be the absolute Galois group of F (or the fundamental group of the open subset $U \subset B$ over which f is unbranched). For each $b \in B$, write

$$f^{-1}(b) = \{m_1, \dots, m_{r(b)}\}.$$

Let $\gamma_b \in \Gamma$ represent the conjugacy class of a generator for the Galois group of the completion $\hat{F}_b$ of F at b (or the class of a small loop around b.) The cover f yields a representation into the symmetric group

$$\varphi : \Gamma \to \mathfrak{S}_{\deg f}$$

where $\varphi(\gamma_b)$ gives the local monodromy at b. If we represent this as a product of disjoint cycles

$$\varphi(\gamma_b) = \sigma_1 \dots \sigma_{r(b)},$$

then the cycles are in one-to-one correspondence with the points $\{m_1, \dots, m_{r(b)}\}$ and

$$\text{length}(\sigma_i) = e_{m_i} + 1.$$

This allows us to rewrite the Riemann-Hurwitz formula

$$2g(M) - 2 = \deg f(2g(B) - 2) + \sum_{b \in B} (\deg(f) - r(b)),$$

where $r(b)$ is the number of orbits of $\varphi(\gamma_b) \in \mathfrak{S}_{\deg f}$.

9.2 Genera of principal homogeneous spaces

Theorem 9.1 *Let F be the function field of a smooth projective curve B; for each $b \in B$, let $\hat{F}_b$ denote the completion of F at b. Let H_F be a finite group scheme over F and P_F a H_F-principal homogeneous space over F. Then $g(H_F) \leq g(P_F)$, with equality only when $P_{\hat{F}_b}$ is a trivial $H_{\hat{F}_b}$-principal homogeneous space for each $b \in B$.*

Proof of theorem: We use the notation of the Appendix and §9.1, and use H and P to denote the normalizations of B in H_F and P_F respectively. Let Γ denote the absolute Galois group of F, $G = H_{F^a}$ the group of points of H_F over the algebraic closure, and G' the associated twisted form, with classifying cocycle

$$\alpha \in H^1(\Gamma, \text{Aut}(G)) = \text{Hom}(\Gamma, \text{Aut}(G)).$$

By Proposition A.2, P_F is classified by a representation

$$\phi : \Gamma \to \mathrm{Aff}(G)$$

so that $q \circ \phi = \alpha$, where $q : \mathrm{Aff}(G) \to \mathrm{Aut}(G)$ is the quotient map.

For each $b \in B$ let $\gamma_b \in \Gamma$ correspond to the generator of the absolute Galois group of $\hat{F}_b$ (or the class of a loop around b in the fundamental group.) As we saw in §9.1, the ramification of $H \to B$ (resp. $P \to B$) over b is determined by the number of orbits of $\alpha(\gamma_b)$ (resp. $\phi(\gamma_b)$) on G. By Proposition A.2, the $H_{\hat{F}_b}$-principal homogeneous space $P_{\hat{F}_b}$ is trivial only if $\phi(\gamma_b)$ is conjugate to $\alpha(\gamma_b)$ by some $\tau_g \in G$.

To apply the Riemann-Hurwitz formula, it suffices to establish the following:

Proposition 9.2 *Let G be a finite group, $a \in \sigma(\mathrm{Aut}(G))$, and $\psi \in \mathrm{Aff}(G)$ so that $q(\psi) = q(a)$. Then we have*

$$\#\, orbits(\psi) \leq \#\, orbits(a),$$

with equality only if $\psi = \tau_g a \tau_g^{-1}$ for some $g \in G$.

Proof of proposition: Let $\mathrm{Aut}(G)$ and $\mathrm{Aff}(G)$ act on G from the left. Since $\mathrm{Aff}(G)$ is a semidirect product of G by $\mathrm{Aut}(G)$ and $q(\psi) = q(a)$, we may represent $\psi = \tau_h a$ for some τ_h, with $h \in G$ acting on G by left translation.

For each $\beta \in \mathrm{Aff}(G)$ and $N \in \mathbb{N}$, define

$$\mathrm{Fix}(\beta, N) = \{g \in G : \beta^N(g) = g\},$$

the elements fixed by the Nth power of β; $\mathrm{Fix}(\beta, 1)$ is the set of β-fixed points. We write $O(\beta, N) = |\mathrm{Fix}(\beta, N)|$. Observe the following properties:

1. $\mathrm{Fix}(\beta, N_1) \subset \mathrm{Fix}(\beta, N_2)$ whenever $N_1 | N_2$.

2. $\mathrm{Fix}(\beta, N)$ is the elements contained in a β-orbit with cardinality dividing N.

3. When $a \in \sigma(\mathrm{Aut}(G)) \subset \mathrm{Aff}(G)$, $\mathrm{Fix}(a, N)$ is a subgroup of G.

4. When $\psi = \tau_h a$ for $a \in \sigma(\mathrm{Aut}(G))$, $\mathrm{Fix}(\psi, N)$ is either empty or is a principal homogeneous space for $\mathrm{Fix}(a, N)$. In particular, either $O(\psi, N) = 0$ or $O(\psi, N) = O(a, N)$.

We verify the last assertion: Take $g_1, g_2 \in \mathrm{Fix}(\psi, N)$ and $g \in \mathrm{Fix}(a, N)$, so that $g = a^N g$ and $g_i = \psi^N(g_i), i = 1, 2$. Since $\psi^N = (\tau_h a)^N = \tau_{h'} a^N$ for some $h' \in G$, we have $g_1 = \tau_{h'} a^N(g_1)$, $\tau_{h'} a^N(g_1 g) = \tau_{h'} a^N(g_1) a^N(g) = g_1 g$, and $g_1 g \in \mathrm{Fix}(\psi, N)$. Furthermore,

$$a^N(g_1^{-1} g_2) = a^N(g_1)^{-1} a^N(g_2) = (\tau_{h'}^{-1} g_1)^{-1} \tau_{h'}^{-1} g_2 = g_1^{-1} g_2$$

so that $g_1^{-1} g_2 \in \mathrm{Fix}(a, N)$.

Let $o(\beta, d)$ denote the number of β-orbits of G with cardinality d, so that

$$\begin{aligned} O(\beta, N) &= \sum_{d|N} o(\beta, d) d \\ o(\beta, d) &= 1/d \sum_{j|d} O(\beta, d/j) \mu(j) \end{aligned}$$

where μ is the Mobius function. Then the total number of β-orbits is

$$\begin{aligned} \#\ \mathrm{orbits}(\beta) &= \sum_{d|\ \mathrm{order}(\beta)} o(\beta, d) = \sum_{d} 1/d \sum_{j|d} O(\beta, d/j) \mu(j) \\ &= \sum_{j|\ \mathrm{order}(\beta)} O(\beta, j)/j \sum_{k|\ \mathrm{order}(\beta)/j} \mu(k)/k \\ &= \sum_{j|\ \mathrm{order}(\beta)} O(\beta, j)/j \prod_{\ell \text{ prime } |\ \mathrm{order}(\beta)/j} (\ell - 1)/\ell. \end{aligned}$$

This is a positive linear combination of the $O(\beta, j)$. We have seen that $O(\psi, j) \leq O(a, j)$ for each j, hence

$$\#\ \mathrm{orbits}(\psi) \leq \#\ \mathrm{orbits}(a).$$

If equality holds then $O(\psi, j) = O(a, j)$ for each j so, in particular, $O(\psi, 1) \neq 0$. If ψ fixes an element $g \in G$ then $\tau_g^{-1} \psi \tau_g$ fixes the identity. However, any element of $\mathrm{Aff}(G)$ fixing the identity is in $\sigma(\mathrm{Aut}(G))$ and

$$q(\tau_g^{-1} \psi \tau_g) = q(\psi) = q(a),$$

hence $\psi = \tau_g a \tau_g^{-1}$. □

9.3 Genus of the p-torsion

We organize our computation by the Kodaira type of the degenerate fiber (see [Kod] §9, Table 1 or [BPV] pp. 159).

Theorem 9.3 *Let $\overline{J} \to B$ be a relatively minimal Jacobian elliptic fibration with generic fiber J_F. Suppose there are n_0 degenerate fibers of type I_0^*, n_1' degenerate fibers of type $I_a, a > 0$, n_1'' degenerate fibers of type $I_a^*, a > 0$, n_2 fibers of type II or II^*, n_3 fibers of type III or III^*, and n_4 fibers of type IV or IV^*.*

If p is a sufficiently large prime number then

$$\begin{aligned} 2g(J_F[p]) - 2 &= p^2(2g(B)-2) + n_1'(p-1)^2 + n_1''(p^2-p) \\ &\quad +(p^2-1)(1/2n_0 + 5/6n_2 + 3/4n_3 + 2/3n_4) \\ 2g(J_F[p] - \{0\}) - 2 &= n_1'(p-1)^2 + n_1''(p^2-p) + (p^2-1)(2g(B)-2 \\ &\quad +1/2n_0 + 5/6n_2 + 3/4n_3 + 2/3n_4). \end{aligned}$$

Remark 9.4 $J_F[p]$ does not generally extend to a group scheme finite and flat over B. Any such group scheme would be smooth over B, but the proof of the theorem shows the existence of ramification at singular fibers.

Corollary 9.5 Retain the notation and assumptions of Theorem 9.3. Suppose $B = \mathbb{P}^1$ and assume

$$c(\overline{J}) := 1/2n_0 + n_1' + n_1'' + 5/6n_2 + 3/4n_3 + 2/3n_4 - 2 > 0.$$

Then for $p \gg 0$ both $J_F[p]$ and $J_F[p] - \{0\}$ have positive genus, as does any $J_F[p]$-principal homogeneous space.

The last assertion follows from Theorem 9.1.
Proof of theorem: To compute the full torsion we take $M_F = J_F[p]$, so the resulting morphism $f : M \to B$ has degree p^2.

In order to apply the Riemann Hurwitz formula as in §9.1, we record the local monodromy $\rho(\gamma_b) \in \mathrm{SL}_2(\mathbb{Z})$, the number of orbits of $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$ under $\rho(\gamma_b)$, and the contribution to the total ramification. In the table below we assume that $p \neq 2, 3$, so that for fibers of types I_0^*,II,II^*, III,III^*,IV,IV^* the mod p reduction of $\rho(\gamma_b)$ is semisimple and fixes only the origin. If there are fibers of type I_a (resp. I_a^*) we also assume $(p, a) = 1$, so the mod p reduction is conjugate to

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \left(\text{resp.} \quad -\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right).$$

Table 1: Ramification contributions at degenerate fibers

Kodaira type	monodromy matrix $\rho(\gamma_b)$	# orbits mod p $r(b)$	ramification $\sum_{m\in f^{-1}(b)} e_m$
I_0	$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$	p^2	0
I_0^*	$-\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$	$1/2(p^2+1)$	$1/2(p^2-1)$
I_a	$\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}$	$2p-1$	$(p-1)^2$
I_a^*	$-\begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}$	p	p^2-p
II	$\begin{pmatrix}1 & 1\\ -1 & 0\end{pmatrix}$	$1/6(p^2+5)$	$5/6(p^2-1)$
II^*	$\begin{pmatrix}0 & -1\\ 1 & 1\end{pmatrix}$	$1/6(p^2+5)$	$5/6(p^2-1)$
III	$\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$	$1/4(p^2+3)$	$3/4(p^2-1)$
III^*	$\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$	$1/4(p^2+3)$	$3/4(p^2-1)$
IV	$\begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}$	$1/3(p^2+2)$	$2/3(p^2-1)$
IV^*	$\begin{pmatrix}-1 & -1\\ 1 & 0\end{pmatrix}$	$1/3(p^2+2)$	$2/3(p^2-1)$

To compute the nonzero torsion we take $M_F = J_F[p] - \{0\}$, so the resulting morphism $f : M \to B$ has degree $p^2 - 1$. On the other hand, removing the origin involves eliminating an orbit of size one, which does not change the ramification contribution. □

We classify the K3 surfaces where Corollary 9.5 *fails* to apply:

Proposition 9.6 *Let $X \to \mathbb{P}^1$ be an elliptic K3 surface, with Jacobian $\overline{J} \to \mathbb{P}^1$ and generic fiber J_F. If $c(\overline{J}) \leq 0$ (cf. Corollary 9.5) then X is isotrivial and takes one of the following forms*

1. *four degenerate fibers of type* I_0^**, and rank NS*$(X) = 18, 19, 20$*;*

2. *three degenerate fibers of types* I_0^*, II^*, IV^**, and rank NS*$(X) = 20$*;*

3. *one degenerate fiber of type* I_0^**, two of type* III^**, and rank NS*$(X) = 20$*;*

4. *three degenerate fibers of type* IV^**, and rank NS*$(X) = 20$.

Proof: Retain the notation of Theorem 9.3 and §7.4. If $c(\overline{J}) \leq 0$ then

$$2n_0 + 4n_1' + 4n_1'' + 10/3n_2 + 3n_3 + 8/3n_4 \leq 8$$

and subtracting from the formula of Corollary 7.15

$$\text{rank NS}(X) + n_1' + 2(n_0 + n_1'' + n_2 + n_3 + n_4) = 26 + r(J_F)$$

gives

$$\text{rank NS}(X) \geq 18 + r(J_F) + 3n_1' + 2n_1'' + 4/3n_2 + n_3 + 2/3n_4.$$

Since rank NS$(X) \leq 20$, it follows that $n_1' = 0$.

The expressions above admit the following solutions:

	n_0	n_1'	n_1''	n_2	n_3	n_4	rank NS(X)	$r(J)$
1	4	0	0	0	0	0	18, 19, 20	2, 1, 0
2	3	0	0	0	0	0	20	0
3	2	0	1	0	0	0	20	0
4	2	0	0	1	0	0	20	0
5	2	0	0	0	1	0	20	0
6	2	0	0	0	0	1	20	0
7	1	0	0	1	0	1	20	0
8	1	0	0	0	2	0	20	0
9	1	0	0	0	1	1	20	0
10	1	0	0	0	0	2	20	0
11	0	0	0	0	0	3	20	0

Several of these can be excluded. Solutions 2,4,5,6,9, and 10 are inconsistent with the Euler characteristic computation of Proposition 7.14. As for solution 3, suppose $X \to \mathbb{P}^1$ is an elliptic surface with one fiber of type I_a^* for $a > 0$ and two fibers of type I_0^*. Such a fiber has one rational curve with multiplicity two, intersected transversally by four rational curves with

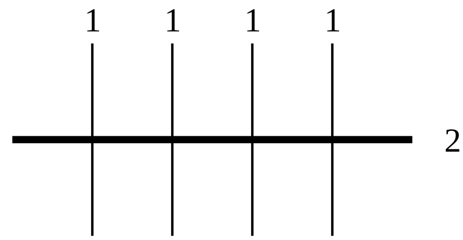

Figure 1: Degenerate fiber of type I_0^*

multiplicity two (see Figure 1). Let $B' \to \mathbb{P}^1$ be a double cover branched at the two points $b_1, b_2 \in \mathbb{P}^1$ with fibers of type I_0^*. The fiber product $X \times_{\mathbb{P}^1} B'$ is non-normal along the preimages of the rational curves with multiplicty two. Let Y be the normalization and $\psi : Y \to B'$ the induced elliptic fibration. The fibers $\psi^{-1}(b_i)$ consist of a smooth elliptic curve, along with four (-1)-curves intersecting it transversally, i.e., the preimages of the rational curves of multiplicity one. Thus ψ is not relatively minimal over the points b_1, b_2, so we blown down the eight (-1)-curves. Let $\psi' : Y' \to B'$ be the resulting fibration, which has only two degenerate fibers, both with potentially multiplicative reduction, i.e., j-invariant infinity (see [Kod], Part II, pp. 604). We obtain a nonisotrivial elliptic fibration with abelian monodromy, an impossibility (see Lemma 8.5.)

The remaining solutions are consistent with Proposition 7.14 and are enumerated above. These correspond to isotrivial elliptic fibrations because there are no fibers of potentially multiplicative reduction.□

Remark 9.7 Ad hoc arguments give potential density for the degenerate cases enumerated in Proposition 9.6. The first case is a Kummer surface: Suppose that $X \to \mathbb{P}^1$ is an elliptic K3 surface with type I_0^* degenerate fibers at the points $b_1, b_2, b_3, b_4 \in \mathbb{P}^1$. The local and global monodromy is multiplication by -1. Let $E \to \mathbb{P}^1$ be the ramified double cover branched over b_1, b_2, b_3, b_4, an elliptic curve. Let $\psi' : Y' \to E$ be the minimal elliptic fibration obtained from $X \times_{\mathbb{P}^1} E \to E$, which is now smooth and has trivial monodromy. Such fibrations are classified (see [BPV] §V.5): ψ' is isotrivial with constant fiber C, is classified by the induced representation $\pi_1(E)$ into the torsion subgroup of C, and Y' is an abelian surface. By Proposition 4.2, Y' has potentially dense rational points. Since Y' dominates X, it also has potentially dense rational points.

The remaining cases have rank twenty, and thus have infinite automorphism group [SI] Theorem 5. Potential density follows from Theorem 6.3.

9.4 Second proof of Theorem 8.8

In light of Remark 8.11, it suffices to establish:

Proposition 9.8 *Let $X \to \mathbb{P}^1$ be a nonisotrivial elliptic K3 surface, with Jacobian $\overline{J}$ and generic fiber J_F. Then there exists an elliptic K3 surface $X' \to \mathbb{P}^1$ with Jacobian $\overline{J}$, a dominant rational map $X' \dashrightarrow X$ over $\mathbb{P}^1$, and a nontorsion rational multisection $M' \subset X'$.*

Proof: We retain the notation of the proof of Theorem 8.7, so that X' is an order-p twist of X. If M' has order N then the image of M' under the multiplication map

$$\mu_N : X' \dashrightarrow J^N(X')$$

is a section of $J^N(X') \to \mathbb{P}^1$. Since X' has order divisible by p, Proposition 7.5 implies $p|N$. Write $N = pn$ and let $Y = J^n(X')$, an elliptic K3 surface with Jacobian J_F, so that $[Y] = n[X']$. We have a factorization of μ_N

$$X' \overset{\mu_n}{\dashrightarrow} Y \overset{\mu_p}{\dashrightarrow} J^N(X') = J^p(Y).$$

The image $M := \mu_n(M')$ is a *rational* multisection in Y of order exactly p and $\Sigma := \mu_p(M)$ is a section in $J^p(Y)$, with $M \subset \mu_p^{-1}(\Sigma)$. Furthermore, $P_F := \mu_p^{-1}(\Sigma)_F$ is a principal homogeneous space for $J_F[p]$.

If $P_F \simeq J_F[p]$ then $M_F \simeq J_F[p] - \{0\}$ because Theorem 8.3 implies $J_F[p]-\{0\}$ is irreducible when $p \gg 0$. It has positive genus by Proposition 9.6 and Corollary 9.5. As our family is nonisotrivial, this can also be extracted from standard computations of the genera of modular curves (e.g., [Miy] §4.2).

If P_F is nontrivial then Theorem 8.3 guarantees it is irreducible for $p \gg 0$. Then $M = \mu_p^{-1}(\Sigma)$ and Corollary 9.5 implies M has positive genus when $p \gg 0$, a contradiction. □

9.5 Completing Theorem 6.4: the isotrivial case

After Theorem 8.8 and Remark 9.7, the only case where potential density remains open is isotrivial elliptic K3 surfaces with $c(\overline{J}) > 0$. Can the argument of §9.4 be applied in this situation? The main complication is that

$J_F[p]-\{0\}$, and even nontrivial $J_F[p]$-principal homogeneous spaces, may fail to be irreducible. Indeed, the monodromy group is a subgroup of the automorphism group of the geometric generic fiber; the irreducible components of $J_F[p]$ correspond to orbits of p-torsion points under these automorphisms. Unfortunately, Theorems 9.3 and 9.1 shed little light on the genus of an *irreducible component* of a principal homogeneous space.

With some extra bookkeeping, one can still prove the following:

Theorem 9.9 *Let $\overline{J} \to \mathbb{P}^1$ be an isotrivial Jacobian elliptic surface, with generic fiber J_F. Suppose that $c(\overline{J}) > 0$. For prime numbers $p \gg 0$, each irreducible component of $J_F[p]-\{0\}$ has positive genus. If P_F is a nontrivial $J_F[p]$-principal homogeneous space then each irreducible component of P_F has positive genus.*

Repeating the argument for Proposition 9.8, we obtain

Proposition 9.10 *Let $X \to \mathbb{P}^1$ be an isotrivial elliptic K3 surface, with Jacobian $\overline{J} \to \mathbb{P}^1$ and generic fiber J_F, so that $c(\overline{J}) > 0$. Then there exists an elliptic K3 surface $X' \to \mathbb{P}^1$ with Jacobian $\overline{J}$, a dominant rational map $X' \dashrightarrow X$ over $\mathbb{P}^1$, and a nontorsion rational multisection $M' \subset X'$.*

Given this, the argument of §9.4 gives potential density for isotrivial elliptic K3 surfaces with $c(\overline{J}) > 0$.

Before establishing Theorem 9.9, we generalize Proposition 8.1 to classify the irreducible components of principal homogeneous spaces for the p-torsion of an isotrivial elliptic fibration. We use the notation of the Appendix, in particular, the exact sequence

$$1 \to (\mathbb{Z}/p\mathbb{Z})^{\oplus 2} \to \mathrm{AffSL}_2(\mathbb{Z}/p\mathbb{Z}) \xrightarrow{q} \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}) \to 1, \qquad (2)$$

with canonical splitting σ.

Proposition 9.11 *Let $T \in \mathrm{SL}_2(\mathbb{Z})$ be an element of finite order n generating a subgroup H, $p \neq 2,3$ a prime, and $H' \subset \mathrm{AffSL}_2(\mathbb{Z}/p\mathbb{Z})$ so that $q(H') = H$. Then there is a split exact sequence*

$$1 \to V \to H' \to H \to 1, \quad V := H' \cap (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}. \qquad (3)$$

For each splitting σ', $\sigma'(H)$ is conjugate to a subgroup of $\sigma(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}))$, where σ is the canonical splitting of exact sequence 2.

The orbit decomposition of $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$ under the action of H' is one of the following:

1. *If* $\dim_{\mathbb{Z}/p\mathbb{Z}}(V) = 0$*,* H' *has one fixed point and* $(p^2-1)/n$ *orbits with* n *elements.*

2. *If* $\dim_{\mathbb{Z}/p\mathbb{Z}}(V) = 1$*,* H' *has one orbit with* p *elements (the subspace* V*) and* $(p-1)/n$ *orbits with* pn *elements.*

3. *If* $\dim_{\mathbb{Z}/p\mathbb{Z}}(V) = 2$*,* H' *has one orbit with* p^2 *elements.*

Proof: If $T \in \mathrm{SL}_2(\mathbb{Z})$ has finite order n, it is semisimple and its eigenvalues are primitive nth roots of unity. The characteristic polynomial of T is quadratic, so $n = 2, 3, 4$, or 6. As $p \neq 2, 3$, the reduction of $T(\bmod\ p)$ still has eigenvalues which are nth roots of unity, and $T(\bmod\ p)$ has order n.

The exact sequence 3 is clearly induced from exact sequence 2; it is split because $|V|$ is prime to $n = |H|$. Now $\sigma'(H)$ is conjugate to a subgroup of $\sigma(\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z}))$, provided $\sigma'(T)$ fixes some point $v \in (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$: Consider the action of $\sigma'(T)$ on polynomials over $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$ of degree ≤ 1

$$c_0 + c_1 x_1 + c_2 x_2, \quad c_0, c_1, c_2 \in \mathbb{Z}/p\mathbb{Z}.$$

We know $\sigma'(T)$ fixes the constants c_0 and has order prime to p, so its action decomposes as a direct sum of irreducibles

$$\langle 1 \rangle \oplus \langle x_1 - v_1, x_2 - v_2 \rangle ,$$

and the induced action on the second factor is semisimple. The fixed point is $v = (v_1, v_2)$; the orbit analysis in the next paragraph will show that $v \in V$.

It remains to analyze the orbit decomposition. In each case, we first conjugate so that $\sigma'(H) \subset \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. If $V = 0$, $H' \subset \mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, generated by a semisimple matrix $\sigma'(T)$ of order $n > 1$. The fixed point is the origin and every other orbit has n elements. If $V = (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$ then H' contains the full translation group, so the action is transitive. Now assume V is one dimensional. Of course, V is an eigenspace for $\sigma'(T)$. The group H' is generated by translations by elements of V and the action of $\sigma'(T)$. Again, the only fixed point under the action of $\sigma'(T)$ is the origin, so any orbit not containing the origin has order divisible by n. No element of $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$ is fixed under translation by V, so each orbit has order divisible by p. The description of the orbits follows. □

Proof of Theorem 9.9: Let M denote a component of the normalization of $\mathbb{P}^1$ in $J_F[p] - \{0\}$ or P_F, corresponding to an orbit of H' on $(\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$. In the first case of Proposition 9.11, M corresponds to an H'-orbit with n elements and Riemann-Hurwitz takes the form

$$2g(M) - 2 = c(\overline{J})n > 0.$$

In the last case of Proposition 9.11 P_F is irreducible, so Theorems 9.3 and 9.1 apply as in the nonisotrivial case.

For the remaining cases, we analyze more closely the behavior at fibers of additive reduction:

Lemma 9.12 Let $\hat{F} = \mathbb{C}((t))$ with absolute Galois group $\hat{\Gamma}$, and $J_{\hat{F}}$ an elliptic curve over $\hat{F}$. Assume that the closed fiber is not of type I_a. For primes $p > 3$, $H^1(\hat{\Gamma}, J_{\hat{F}}[p]) = 0$.

Proof of lemma: Take the associated Néron/relatively minimal model $\overline{J}$ over $\mathbb{C}[[t]]$. The locus where the fibers of $\overline{J}$ are smooth and reduced is called the 'group-like' part. In the case of additive reduction, the identity component of the group-like part is the additive group, which has no torsion. Hence, the order of the torsion group is equal to the number of connected components of the group-like part. The Kodaira classification ([Kod] §9, Table 1 or Figure 2 of §10) gives

Kodaira type	I_a^*	II	II^*	III	III^*	IV	IV^*
torsion order	4	0	0	2	2	3	3

By Proposition 7.2, in these cases any local $J_{\hat{F}}[p]$-principal homogeneous space (with $p > 3$) is trivial. □

We complete the proof of Theorem 9.9. Only the second case of Proposition 9.11 remains. Lemma 9.12 says that at each point $b \in \mathbb{P}^1$ of additive reduction, the local monodromy $\phi(\gamma_b) \in H'$ has a fixed point (see Proposition A.2.) If M corresponds to an H'-orbit with p elements then one of the elements is fixed at each point of additive reduction, and Riemann-Hurwitz takes the form

$$2g(M) - 2 \geq -2p + (1/2n_0 + 5/6n_2 + 3/4n_3 + 2/3n_4)(p-1) = (p-1)c(\overline{J}) - 2.$$

We have inequality because $f : M \to \mathbb{P}^1$ may ramify at smooth fibers. If M corresponds to an orbit with pn elements then none of the elements is fixed and

$$2g(M) - 2 \geq -2pn + (1/2n_0 + 5/6n_2 + 3/4n_3 + 2/3n_4)(np) = npc(\overline{J}).$$

This completes the proof.□

10 Approach III: elliptic multisections (based on correspondence with J. Kollár)

10.1 Cubical curves

Definition 10.1 A *cubical curve* C is a reduced curve which may be imbedded as a plane cubic $C \subset \mathbb{P}^2$, with at most two irreducible components.

Example 10.2

1. an elliptic curve is cubical;
2. an irreducible rational curve with a single node is cubical with equation $y^2z = x^2z + x^3$, and is called the 'nodal cubic';
3. an irreducible rational curve with a single cusp is cubical with equation $y^2z = x^3$, and is called the 'cuspidal cubic';
4. a curve with two smooth rational components intersecting in two nodes is cubical with equation $x(x^2 - yz) = 0$, and is called the 'secant cubic';
5. a curve with two smooth rational components intersecting in one point tangentially is cubical with equation $z(x^2 - yz) = 0$, and is called the 'tangential cubic'.

Proposition 10.3

1. *Cubical curves are connected of arithmetic genus one and admit flat deformations to smooth curves.*
2. *Any isomorphism $C_1^\nu \to C_2^\nu$ between the normalizations of cubical curves that respects their conductors descends to an isomorphism $C_1 \to C_2$ of the cubical curves.*
3. *Let R be a projective integral singular rational curve. Then there exists a cubical curve C and birational morphism $f : C \to R$.*
4. *Let R be a projective connected curve with two rational irreducible components, at least one of which is smooth. Assume that the smooth component intersects the second component in at least two distinct points, or intersects a smooth branch of the second component with multiplicity greater than one. Then there exists a cubical curve C and birational morphism $f : C \to R$.*

Proof: We leave the proof of the first part to the reader. One way to establish the isomorphism assertion is to observe that Example 10.2 gives a complete classification of cubical curves.

For the remaining claims, consider the *seminormalization* $\sigma : R^\sigma \to R$ [Kol2] I.7.2. This is a finite, birational, *bijective* morphism, and is maximal with these properties; it is obtained from the normalization R^ν by identifying points which are identified by $\nu : R^\nu \to R$.

For the third assertion, $R^\nu \simeq \mathbb{P}^1$ and either $R^\nu \to R^\sigma$ or $R^\sigma \to R$ fails to be an isomorphism, because R is singular. If $R^\nu \to R^\sigma$ fails to be an isomorphism then there exist distinct $r_1, r_2 \in R^\nu$ that are identified in R. Let C_0 be the nodal cubic obtained from R^ν by identifying r_1 and r_2. The induced $C_0 \to R$ is the desired morphism from a cubical curve. Otherwise, $R^\sigma \simeq \mathbb{P}^1$ and we choose $r \in R^\sigma$ at which σ is not an isomorphism. Consider the local rings $\mathcal{O}_{R,\sigma(r)} \subset \mathcal{O}_{R^\sigma,r}$, a finite extension of $\mathcal{O}_{R^\sigma,r}$-modules. If $t \in \mathfrak{m}_{R^\sigma,r}$ is a local uniformizer then $t^n \in \mathfrak{m}_{R,\sigma(r)}$ for $n \gg 0$ but not $n = 1$. The intermediate ring

$$\mathcal{O}_{R,\sigma(r)} \subset \mathcal{O}_{R,\sigma(r)}[t^2, t^3, t^4, \ldots] \subset \mathcal{O}_{R^\sigma,r}$$

corresponds to a factorization $R^\sigma \to C \to R$ through a cuspidal curve C.

For the last assertion, we have $R^\nu = R_1^\nu \cup R_2^\nu \simeq \mathbb{P}^1 \cup \mathbb{P}^1$ with R_1^ν mapped isomorphically onto its image in R. Suppose we have distinct $r_1, r_1' \in R_1^\nu$ and $r_2, r_2' \in R_2^\nu$ so that $\nu(r_1) = \nu(r_2)$ and $\nu(r_1') = \nu(r_2')$. Let C be the curve obtained by gluing the R_i^ν so that r_1 and r_2 (resp. r_1' and r_2') are identified. This is a 'secant cubic' and we obtain a factorization $R^\nu \to C \to R$. Now suppose we have $r_i \in R_i^\nu$ so that $\nu(r_1) = \nu(r_2) = r$, and ν maps an open neighborhood of r_2 isomorphically onto its image, which intersects $\nu(R_1^\nu)$ with multiplicity at least two at r. Algebraically, $\mathcal{O}_{R,r}$ is contained in the subring of elements $(f_1, f_2) \in \mathcal{O}_{R_1^\nu,r_1} \times \mathcal{O}_{R_2^\nu,r_2}$ with $f_1(r_1) = f_2(r_2)$ and $f_1 \in \mathfrak{m}^2_{R_1^\nu,r_1}$ if and only if $f_2 \in \mathfrak{m}^2_{R_2^\nu,r_2}$. This is the ring of functions of a curve C of arithmetic genus one consisting of two smooth rational components meeting tangentially at a single point, i.e., a tangential cubic. Thus we get the desired factorization $R^\nu \to C \to R$. $\square$

10.2 Production of cubical curves

Proposition 10.4 *Let $\eta : X \to \mathbb{P}^1$ be an elliptic K3 surface with Jacobian fibration $\overline{J} \to \mathbb{P}^1$ and generic fiber J_F. There exist the following*

1. *an elliptic K3 surface $\eta' : X' \to \mathbb{P}^1$ with Jacobian $\overline{J} \to \mathbb{P}^1$;*

2. *a dominant rational map $X' \dashrightarrow X$;*

3. *a morphism $f_0 : C_0 \to X'$ from a cubical curve that is birational onto its image; this image is not contained in any fiber of η'.*

Proof: Corollary 7.13 yields an elliptic K3 surface $X' \to \mathbb{P}^1$ with Jacobian $\overline{J}$ so that

$$\text{order } [X'_F] = p \cdot \text{order } [X_F] \text{ and } p[X'_F] = [X_F]$$

as well as a dominant rational map

$$\mu_p : X' \dashrightarrow J^p(X') = X.$$

Let $M' \subset X'$ be the rational multisection of degree $p \cdot \text{order } [X_F]$ guaranteed by Proposition 7.12. If M' is singular then we obtain the desired map directly from the third part of Proposition 10.3. If M' is nonsingular, we apply the fourth part of Proposition 10.3 to the union of M' and a suitable irreducible component of a degenerate fiber. It remains to show there exists a component satisfying the hypotheses of Proposition 10.3 provided M' has sufficiently large degree:

Lemma 10.5 Let $\eta' : X' \to \mathbb{P}^1$ be an elliptic K3 surface and M' a nonsingular multisection of degree $d \geq 35$. Then M' intersects some irreducible component of a degenerate fiber in at least two points, or intersects one smooth reduced branch of the degenerate fiber with multiplicity greater than one.

Proof of Lemma: Recall the multiplicities of irreducible components of degenerate fibers in the Kodaira classification [BPV], pp. 150, displayed in Figure 2.

First consider the fibers where all the reduced irreducible components are nonsingular. We choose d so that it is greater than the sum of the multiplicities over all the components:

type	$I_a, a > 1$	III	IV	I_a^*	II^*	III^*	IV^*
sum of multiplicities	a	2	3	$2a+6$	30	18	12

Then M' intersects some component twice, or perhaps at one point with multiplicity greater than one. Proposition 7.14 implies that an elliptic K3

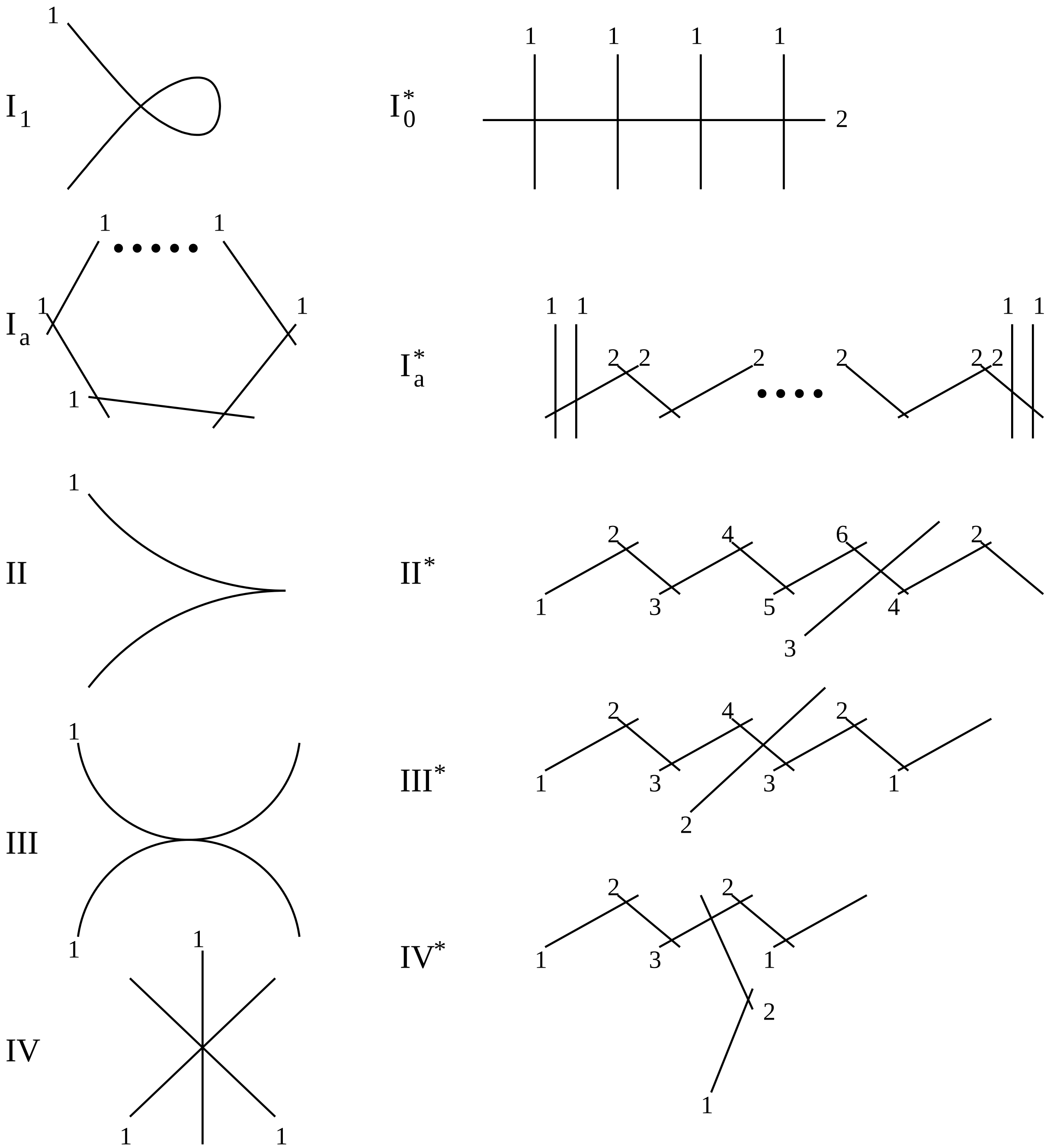

Figure 2: Multiplicities of degenerate fibers

can only have fibers of type I_a (resp. I_a^*) for $a \leq 19$ (resp. $a \leq 14$). Thus it suffices to take $d \geq 35$.

Now consider the remaining fibers. For fibers of type I_1, any smooth curve intersecting the nodal point with multiplicity ≥ 3 intersects one of the branches with multiplicity ≥ 2. It suffices that $d \geq 3$. In case II, any smooth curve intersects the cuspidal point in at most multiplicity three, so it suffices that $d \geq 4$. $\square$

10.3 Production of elliptic curves

Proposition 10.6 *Let X be a K3 surface, C_0 a cubical curve, and $f_0 : C_0 \to X$ a morphism birational onto its image. Then $\{f_0 : C_0 \to X\}$ deforms to a morphism $\{f : C \to X\}$, where C is a smooth elliptic curve. The resulting family of elliptic curves dominates X.*

Proof: Let $v : \mathcal{C} \to S$ be a versal deformation of C_0, with C_0 the fiber over the distinguished point $s_0 \in S$. This can be realized as a linear series of plane cubic curves containing C_0 (cf. the first part of Proposition 10.3). The generic fiber is a smooth elliptic curve and $\dim(S) = \dim \mathrm{Aut}(C_0)$ [Kol2] II.1.11.

Consider the functor of morphisms of flat S-schemes

$$Hom(\mathcal{C}, X \times S)(T) = \{T - \text{ morphisms } g : \mathcal{C} \times_S T \to (X \times S) \times_S T\},$$

where T is an S-scheme. Assigning to each morphism its graph, we may represent this functor by an S-scheme $\mathrm{Hom}(\mathcal{C}, X \times S)$, an open subset of the relative Hilbert scheme of $\mathcal{C} \times_S (X \times S)$. The morphism f_0 yields a point of $\mathrm{Hom}(\mathcal{C}, X \times S)$ over the basepoint s_0.

Our next task is to bound the dimension of $\mathrm{Hom}(\mathcal{C}, X \times S)$ at f_0 from below. General theory [Kol2] I.2.17, II.1.13 guarantees that

$$\begin{aligned}
\dim_{[f_0]} \mathrm{Hom}(\mathcal{C}, X \times S) \quad &\geq \quad \dim \mathrm{Hom}(f_0^*\Omega_X^1, \mathcal{O}_{C_0}) \\
&\qquad - \dim \mathrm{Ext}^1(f_0^*\Omega_X^1, \mathcal{O}_{C_0}) + \dim_{s_0} S \\
&= \quad -K_X \cdot C_0 + (\dim(X) - 3)\chi(\mathcal{O}_{C_0}) + \dim \mathrm{Aut}(C_0) \\
&= \quad \dim \mathrm{Aut}(C_0).
\end{aligned}$$

In our particular situation this can be improved (cf. [Kol2] II.1.13.1 and [Ra]): We claim that

$$\dim_{[f_0]} \mathrm{Hom}(\mathcal{C}, X \times S) \geq \dim \mathrm{Aut}(C_0) + 1.$$

Let $\mathcal{X} \to \Delta$ be a one-parameter complex-analytic deformation of X, so that the generic fiber contains no algebraic curves. This can be achieved using the Local Torelli Theorem [LP], by choosing a deformation for which none of the classes in $H^2(X, \mathbb{Z})$ remains of type $(1,1)$. Now consider the new mapping functor over $S \times \Delta$

$$\mathrm{Hom}(\mathcal{C} \times \Delta, \mathcal{X} \times S)$$

at the point

$$g_0 : C_0 \stackrel{f_0}{\to} X \hookrightarrow \mathcal{X}.$$

The general theory now gives

$$\begin{aligned} \dim_{[g_0]} \mathrm{Hom}(\mathcal{C} \times \Delta, \mathcal{X} \times S) &\geq \dim \mathrm{Hom}(g_0^* \Omega^1_{\mathcal{X}}, \mathcal{O}_{C_0}) \\ &\qquad - \dim \mathrm{Ext}^1(g_0^* \Omega^1_{\mathcal{X}}, \mathcal{O}_{C_0}) + \dim_{(s_0,0)}(S \times \Delta) \\ &= \dim \mathrm{Aut}(C_0) + 1. \end{aligned}$$

The generic fiber of $\mathcal{X}$ contains no algebraic curves, so the family $\mathrm{Hom}(\mathcal{C} \times \Delta, \mathcal{X} \times S)$ must parametrize curves contained in X.

Consequently, there are deformations $\{f : C \to X\}$ of $\{f_0 : C_0 \to X\}$ that are not obtained by composing f_0 with an automorphism of C_0. We claim that $f(C) \not\subset f_0(C_0)$. Indeed, suppose that $f(C) = f_0(C_0)$. Since f_0 and f are birational onto their images and normalizations are unique, the composed morphisms

$$C^\nu \to C \to f(C) \quad C_0^\nu \to C_0 \to f_0(C_0)$$

agree up to an isomorphism $C^\nu \to C_0^\nu$ which preserves conductors. By part two of Proposition 10.3, this descends to an isomorphism $C \to C_0$, a contradiction. Thus the images $f(C)$ dominate X, and since X is not ruled we conclude that the generic domain curve C is elliptic. □

10.4 Proof of Theorem 6.4

As in our previous approaches to Theorem 6.4, the key point is that each elliptic K3 surface $X \to \mathbb{P}^1$ is dominated by an elliptic K3 surface $X' \to \mathbb{P}^1$ admitting a nontorsion multisection with dense rational points, so that Proposition 4.13 applies. What is new here is that the multisection is an elliptic rather than a rational curve:

Theorem 10.7 *Let $\eta : X \to \mathbb{P}^1$ be an elliptic K3 surface with Jacobian fibration $\overline{J} \to \mathbb{P}^1$ and generic fiber J_F. There exist the following*

1. *an elliptic K3 surface $\eta' : X' \to \mathbb{P}^1$ with Jacobian $\overline{J} \to \mathbb{P}^1$;*
2. *a dominant rational map $X' \dashrightarrow X$;*
3. *a nontorsion elliptic multisection $\hat{M} \subset X'$.*

Furthermore, if X is defined over a number field then X' and $\hat{M}$ can be chosen so they are defined over a finite extension of that field.

This is an immediate consequence of Proposition 10.4 and the following:

Proposition 10.8 *Let $\eta' : X' \to \mathbb{P}^1$ be an elliptic K3 surface. Assume there exists a cubical curve C_0 and a morphism $f_0 : C_0 \to X'$ birational onto its image, so that $f_0(C_0)$ is not contained in any fiber of η' Then η' admits an elliptic multisection of infinite order. If X' is defined over a number field then the multisection can be defined over a finite extension of that field.*

In particular, any elliptic multisection deforms to a nontorsion elliptic multisection.
Proof of Proposition 10.8: Proposition 10.6 implies there exists a smooth projective elliptic surface $S \to B$, and a surjective morphism $g : S \to X'$ so that the generic fiber is mapped birationally onto its image. Under our assumptions, this image is not contained in a fiber of η'. Moreover, since X' is a K3 surface the images of any two fibers are linearly equivalent

$$[C] \equiv g_*[S_b] \text{ for each } b \in B.$$

We distinguish some special fibers of $S \to B$. We have the singular fibers and the fibers that fail to be mapped birationally onto their image. The image of these fibers maps to a closed subset $Z \subset X'$.

Choose a smooth fiber $X'_p = {\eta'}^{-1}(p)$ not lying in Z, defined over a number field if X' is. After passage to a larger number field L, we can find a point $x \in X'_p(L)$, $x \notin Z$, so that $t_x = -\deg(C.X'_p)x + [C]|_{X'_p} \in J(X'_p)$ has infinite order in the Jacobian (by the arithmetic result, Proposition 4.2). Let S_b be a fiber of $S \to B$ so that $x \in g(S_b)$, which by assumption is smooth and maps birationally onto its image $\hat{M} := g(S_b)$. As S_b maps birationally onto $\hat{M}$, $[\hat{M}] = [g_* S_b] = [C]$. Now t_x has infinite order in $J(X'_p)$ and coincides with the restriction of $\tau_{\hat{M}}$ to X'_p. Hence $\tau_{\hat{M}}$ itself has infinite order and the multisection $\hat{M}$ is nontorsion. $\square$

Corollary 10.9 Every elliptic K3 surface admits a nontorsion elliptic multisection.

Proof: Retain the notation of Theorem 10.7. The proof above yields an elliptic multisection $\hat{M}$ for η' through the generic point of X'. Its image $M \subset X$ is a multisection for η through the generic point of X; M has positive genus because X is not ruled and thus is elliptic. Proposition 10.8 shows M deforms to a nontorsion elliptic multisection. □

11 Symmetric products of K3 surfaces

11.1 Do generic K3 surfaces have potentially dense rational points?

In the previous sections, we have seen many special examples of K3 surfaces with potentially dense rational points. However, we know very little about the density of rational points on generic K3 surfaces. Indeed, all the K3 surfaces considered up to this point are very special in moduli:

Proposition 11.1 *A K3 surface X admits an elliptic fibration if and only if there exists a class $D \in \mathrm{NS}(X)$ with $D.D = 0$. If a K3 surface admits an elliptic fibration or an infinite automorphism group, then rank* $\mathrm{NS}(X) \geq 2$.

Proof: If X admits an elliptic fibration $\eta : X \to \mathbb{P}$, then the generic fiber $[\eta^{-1}(b)] \in \mathrm{NS}(X)$ has self-intersection zero. The class of the fiber is independent from the polarization of X, so rank $\mathrm{NS}(X) \geq 2$. Conversely, suppose X admits a class $[D] \in \mathrm{NS}(X)$ with $D.D = 0$. By Riemann Roch, either D or $-D$ is effective. Since the effective cone is the union of images of the nef cone under reflections by (-2)-curves ([LP] §2), we may asssume D is nef. Basic results on linear series on K3 surfaces [SD] imply that $|D|$ is basepoint free and defines an elliptic fibration on X.

If X has Néron-Severi rank one, then the polarization generates the Néron-Severi group and every automorphism fixes the polarization, so the automorphism group is finite (cf. the proof of Lemma 6.9). □

Question 11.2 Does there exist any K3 surface X over a number field with rank $\mathrm{NS}(X) = 1$ and dense rational points?

11.2 Symmetric powers of surfaces

To obtain potential density theorems for generic K3 surfaces, we consider auxilliary varieties, the *symmetric powers.* We refer the reader to [HT] for further details. The n-fold symmetric power of a surface X is the quotient

$$X^{(n)} = \underbrace{X \times X \times \ldots \times X}_{n \text{ times}} / \mathfrak{S}_n.$$

This variety admits a natural desingularization by the Hilbert scheme of length-n, zero-dimensional subschemes of X

$$\sigma : X^{[n]} \to X^{(n)}.$$

For a curve C, the behavior of rational points on the symmetric products $C^{(n)}$ bears little resemblance to the behavior of rational points on C. Indeed, for $n > 2g(C) - 2$, $C^{(n)}$ is a projective bundle over $J^n(C)$, and thus always has potentially dense rational points. For a surface X, the rational points on $X^{(n)}$ might very well behave similarly to rational points on X. There is a simple formula relating the Kodaira dimension of a surface and its symmetric product

$$\kappa(X^{(n)}) = n\kappa(X).$$

Moreover, the quotient morphism $q : X^n \to X^{(n)}$ is almost étale; it is unramified away from a codimension-two subset, the diagonal. If q *were* étale then the Chevalley-Weil Theorem (Proposition 3.4) would apply: potential density of rational points on $X^{(n)}$ implies potential density of rational points on X^n, and thus on X.

11.3 Main Theorem

Theorem 11.3 *Let X be a K3 surface defined over a number field. Assume that X admits a polarization f of degree $2N - 2$. Then rational points on $X^{(n)}$ are potentially dense for some $n \leq N$.*

The proof of Theorem 11.3 divides into cases, depending on the geometry of the elliptic curves contained in X. We first need a geometric result:

Proposition 11.4 *Let X be a K3 surface and f a divisor with $h^0(X, f) > 1$. Then there exists an irreducible, possibly singular, curve of genus one $C \subset X$ so that $f - [C]$ is effective.*

This is proved in detail in §4 of [HT]. The main ingredient is [MM], where it is shown that for a generic polarized K3 surface there is a one-parameter family of singular curves of genus one in the polarizing class. As in Lemma 6.10, these specialize to the desired curves.

We apply Proposition 11.4 to the polarization class f. The resulting genus-one curve C has self-intersection

$$C.C \leq f.f.$$

If $C.C > 0$ then $[C]$ is big by Riemann-Roch and Theorem 11.3 follows from:

Proposition 11.5 *Let X be a K3 surface defined over a number field, and g the class of a big line bundle of degree $2(n-1)$. Assume there is an irreducible, possibly singular, curve of genus one $C \subset X$ with $[C] = g$. Then rational points on $X^{(n)}$ are potentially dense.*

Sketch Proof: Again, we only give the main ideas of the argument; see [HT] for more details. The linear series $|g|$ contains an irreducible curve and so is basepoint free. Indeed, linear series on a K3 surface have no isolated fixed points, only fixed components [SD]§2. It follows that g is numerically effective and has no higher cohomology, and thus defines a morphism $j : X \to \mathbb{P}^n$. Consider the incidence correspondence

$$\begin{array}{ccccc} & & \mathcal{H} := \{(x, H) : j(x) \in H\} & \subset & X \times \check{\mathbb{P}}^n \\ & \swarrow^{\pi_1} & & \searrow^{\pi_2} & \\ X & & & & \check{\mathbb{P}}^n \end{array}$$

where $\check{\mathbb{P}}^n$ is the dual projective space. Over an open subset $V \subset \check{\mathbb{P}}^n$, the fibers of π_2 are smooth curves of genus n.

Consider the degree n component of the relative Albanese

$$\eta : J^n(\mathcal{H})_V \to V.$$

The Jacobi inversion formula says that the degree n component of the Albanese of a smooth projective curve C of genus n is birational to the symmetric product $C^{(n)}$. Globalizing, we find that $J^n(\mathcal{H})_V$ is birational to the symmetric product $X^{(n)}$. Indeed, for any generic $x_1 + \ldots + x_n \in X^{(n)}$, there is a unique hyperplane $H \supset \{j(x_1), \ldots, j(x_n)\}$, and we obtain an element $\mathcal{O}_{j^{-1}(H)}(x_1 + \ldots + x_n) \in J^n(j^{-1}(H))$.

By Proposition 4.13, it suffices to find a nondegenerate multisection M of η, defined over a number field, with dense rational points. Suppose we have n distinct irreducible curves $C_1, \ldots, C_n$ in $|g|$. Then we can map the product

$$C_1 \times C_2 \times \ldots \times C_n \dashrightarrow X^{(n)}$$

and let $C_1 * \ldots * C_n \subset X^{(n)}$ denote the closed image. The induced morphism $M = C_1 * \ldots * C_n \to V$ is generically finite: There are a finite number of points in the product supported in a generic hyperplane section of X.

The remainder of the argument follows Proposition 10.8. As before, there exists an elliptic fibration $S \to B$ and a surjective morphism $S \to X$ so that the generic fiber is mapped birationally onto a genus-one curve with class g. Pick a smooth fiber $A = \eta^{-1}(H)$ of $J^n(\mathcal{H})_V \to V$ and a point $\alpha \in A(K)$, where K is some number field, so that $-\deg(M/V)\alpha + [M]|_A$ is nondegenerate (see Proposition 4.2.) Using Jacobi inversion, we can express

$$\alpha = x_1 + \ldots + x_n, \quad x_1, \ldots, x_n \in X, \quad j(x_i) \in H.$$

After perhaps choosing a more general α, we may assume that each $x_i \in S_{b_i}$, where the S_{b_i} are distinct, irreducible fibers of $S \to B$, mapped birationally onto their image in X, and defined over a number field. It follows that α lies in the multisection $S_{b_1} * \ldots * S_{b_n}$, which is necessarily nondegenerate. $\square$

It remains to deal with the case $C.C \leq 0$. Since C is irreducible, adjunction implies C is smooth and $C.C = 0$. In particular, the linear series $|C|$ yields an elliptic fibration $\eta : X \to \mathbb{P}^1$. Then rational points on X are potentially dense by Theorem 6.4. $\square$

A Appendix: Galois cohomology and principal homogeneous spaces

Let G and Γ be groups and let $\mathrm{Aut}(G)$ denote the automorphism group of G. When G and Γ admit topological structures, all the maps described below are tacitly assumed to be continuous with respect to the relevant topologies.

Let G' be a twisted form of G with respect to Γ. This means we have an action

$$\begin{array}{rcl} \Gamma \times G & \to & G \\ (\gamma, g) & \to & \gamma(g), \end{array}$$

respecting the group structure, i.e., a homomorphism

$$\alpha : \Gamma \to \mathrm{Aut}(G).$$

Remark A.1 In applications, Γ is often the Galois group $\mathrm{Gal}(F^a/F)$ of the algebraic closure of a field of characteristic zero, G the group of F^a-points of a group scheme over F, and G' the associated Galois module. In this context, we will use the same notation for G' and the group scheme. We are mainly interested in the case where G' is an abelian variety or its N-torsion subgroup. The relation between Galois cohomology and principal homogeneous spaces in this context is developed in [LT].

The zeroth cohomology group of G' is the subgroup of invariant elements

$$H^0(\Gamma, G') = \{g \in G' : \gamma(g) = g \text{ for each } \gamma \in \Gamma\}.$$

A cocycle with values in G' is a map

$$\begin{array}{rcl} \xi : \Gamma & \to & G' \\ \gamma & \to & \xi(\gamma) \end{array}$$

satisfying the cocycle condition

$$\xi(\gamma\gamma') = \xi(\gamma)\gamma(\xi(\gamma')).$$

Two cocycles ξ and θ are cohomologous if there exists a $g \in G'$ so that

$$g\theta(\gamma) = \xi(\gamma)\gamma(g), \text{ for each } \gamma \in \Gamma.$$

The first cohomology set $H^1(\Gamma, G')$ is the set of equivalence classes of cocycles under the cohomology relation. If G' is abelian then $H^1(\Gamma, G')$ is an abelian group.

If the Γ-action on G' is trivial, we have

$$H^1(\Gamma, G') = \mathrm{Hom}(\Gamma, G),$$

the group homomorphisms from Γ to G. In particular, a twisted form of G is governed by an element $\alpha \in H^1(\Gamma, \mathrm{Aut}(G))$.

A G'-principal homogeneous space is a set P with two actions

$$\begin{array}{rcl} \Gamma \times P & \to & P \\ (\gamma, p) & \to & \gamma(p) \\ P \times G' & \to & P \\ (p, g) & \to & p \cdot g \end{array}$$

satisfying

1. the action of G' is compatible with the Γ-action

$$\gamma(p \cdot g) = \gamma(p) \cdot \gamma(g);$$

2. for each $p_1, p_2 \in P$, there is a unique $g \in G'$ with $p_1 \cdot g = p_2$.

G' acts on itself by multiplication: This is called the *trivial* principal homogeneous space.

Choose $p \in P$. For each $\gamma \in \Gamma$ there exists a unique $\xi(\gamma) \in G'$ so that $\gamma(p) = p \cdot \xi(\gamma)$. We have

$$\begin{aligned} \gamma(\gamma'(p)) &= \gamma(p \cdot \xi(\gamma')) = \gamma(p) \cdot \gamma(\xi(\gamma')) = p \cdot \xi(\gamma)\gamma(\xi(\gamma')) \\ (\gamma\gamma')p &= p \cdot \xi(\gamma\gamma') \end{aligned}$$

so $\xi(\gamma\gamma') = \xi(\gamma)\gamma(\xi(\gamma'))$ and ξ is a cocycle for G'. Changing the basepoint p, we may write

$$\gamma(p \cdot g) = (p \cdot g)\theta(\gamma)$$

where $g\theta(\gamma) = \xi(\gamma)\gamma(g)$, so θ is cohomologous to ξ. Thus every G'-principal homogeneous space determines an element of $H^1(\Gamma, G')$ and conversely.

Now let G be a group and $\mathrm{Aff}(G)$ the semidirect product of G by $\mathrm{Aut}(G)$, so we have an exact sequence

$$1 \to G \to \mathrm{Aff}(G) \xrightarrow{q} \mathrm{Aut}(G) \to 1 \tag{4}$$

admitting a splitting $\sigma : \mathrm{Aut}(G) \hookrightarrow \mathrm{Aff}(G)$. We interpret $\mathrm{Aff}(G)$ as the permutations of G generated by left translations

$$\tau_g : x \to gx \quad g \in G$$

and automorphisms $a \in \mathrm{Aut}(G)$. Given $g_1, g_2 \in G$ and $a_1, a_2 \in \mathrm{Aut}(G)$, we have

$$\tau_{g_1} a_1 \tau_{g_2} a_2 = \tau_{g_1}(a_1 \tau_{g_2} a_1^{-1}) a_1 a_2 = \tau_{g_1} \tau_{a_1(g_2)} a_1 a_2.$$

Proposition A.2 *Let G' be a Γ-twisted form of a group G, with classifying cocycle $\alpha \in H^1(\Gamma, \mathrm{Aut}(G)) = \mathrm{Hom}(\Gamma, \mathrm{Aut}(G))$. Then $H^1(\Gamma, G')$ corresponds to G-conjugacy classes of homomorphisms*

$$\phi : \Gamma \to \mathrm{Aff}(G), \ \textit{with} \quad q \circ \phi = \alpha.$$

The trivial element corresponds to $\sigma \circ \alpha$.

Proof: Given a cocycle $\xi(\gamma)$, we define $\phi(\gamma) = \tau_{\xi(\gamma)}\alpha(\gamma)$ so that

$$\begin{aligned}
\phi(\gamma\gamma') &= \tau_{\xi(\gamma\gamma')}\alpha(\gamma\gamma') \\
&= \tau_{\xi(\gamma)}\tau_{\gamma(\xi(\gamma'))}\alpha(\gamma)\alpha(\gamma') \\
&= \tau_{\xi(\gamma)}\alpha(\gamma)\tau_{\xi(\gamma')}\alpha(\gamma') \\
&= \phi(\gamma)\phi(\gamma').
\end{aligned}$$

Conversely, each homomorphism $\phi : \Gamma \to \mathrm{Aff}(G)$ with $q \circ \phi = \alpha$ yields a cocycle $\xi(\gamma)$. Now suppose that θ and ξ are cohomologous, so that $\theta(\gamma) = g^{-1}\xi(\gamma)\gamma(g)$ for some $g \in G'$, and let ϕ_θ and ϕ_ξ be the corresponding homomorphisms. Then we have

$$\begin{aligned}
\phi_\theta(\gamma) &= \tau_{g^{-1}\xi(\gamma)\gamma(g)}\alpha(\gamma) = \tau_g^{-1}\tau_{\xi(\gamma)}\tau_{\gamma(g)}\alpha(\gamma) \\
&= \tau_g^{-1}\tau_{\xi(\gamma)}\alpha(\gamma)\tau_g = \tau_g^{-1}\phi_\xi(\gamma)\tau_g,
\end{aligned}$$

and the homomorphisms are conjugate. □

Remark A.3 For each normal subgroup $H \subset \mathrm{Aut}(G)$, the split exact sequence (4) restricts to a split exact sequence

$$1 \to G \to \mathrm{Aff}H(G) \stackrel{q}{\to} H \to 1.$$

Assume that G' is governed by a coycle with values in H,

$$\alpha \in H^1(\Gamma, H) \simeq \mathrm{Hom}(\Gamma, H).$$

Then $H^1(\Gamma, G')$ corresponds to homomorphisms

$$\phi : \Gamma \to \mathrm{Aff}H(G), \text{ with } \quad q \circ \phi = \alpha.$$

References

[Am] S. A. Amitsur, Generic splitting fields of central simple algebras, *Ann. of Math. (2)* **62** (1955), 8–43.

[BPV] W. Barth, C. Peters, A. Van de Ven, *Compact complex surfaces*, Springer-Verlag, Berlin, 1984.

[BT1] F. Bogomolov and Y. Tschinkel, Density of rational points on Enriques surfaces, *Math. Res. Letters* **5** (1998), 623–628.

[BT2] F. Bogomolov and Y. Tschinkel, On the density of rational points on elliptic fibrations, *J. Reine Angew. Math.* **511** (1999), 87–93.

[BT3] F. Bogomolov and Y. Tschinkel, Density of rational points on elliptic K3 surfaces, *Asian Journ. of Math.* **4** (2000), no. 2, 351–368.

[Ca] F. Campana, Remarques sur le revêtement universel des variétés kählériennes compactes, *Bulletin de la Société mathématique de France* **122** (1994), 255–284.

[Ca2] F. Campana, Special varieties and classification theory, math.AG/0110051.

[CSS] J.L. Colliot-Thélène, A.N. Skorobogatov, P. Swinnerton-Dyer, Double fibres and double covers: paucity of rational points, *Acta Arith.* **79** (1997), no. 2, 113–135.

[CPR] A. Corti, A. Pukhlikov, M. Reid, Fano 3-fold hypersurfaces, in: *Explicit birational geometry of 3-folds*, 175–258, London Math. Soc. Lecture Note Ser., **281**, Cambridge Univ. Press, Cambridge, 2000.

[De] O. Debarre, Fano varieties, Lecture notes from the instructional conference 'Higher-Dimensional Varieties and Rational Points', at the Alfréd Rényi Institute of Mathematics, Budapest.

[Fa1] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), no. 3, 349–366; Erratum: *Invent. Math.* **75** (1984), no. 2, 381.

[Fa2] G. Faltings, Diophantine approximation on abelian varieties, *Ann. of Math. (2)* **133** (1991), no. 3, 549–576.

[FJ] G. Frey and M. Jarden, Approximation theory and the rank of Abelian varieties over large algebraic fields, *Proc. London Math. Soc.* **28** (1974), 112–128.

[GM1] G. Grant and E. Manduchi, Root numbers and algebraic points on elliptic surfaces with base P^1, *Duke Math. J.* **89** (1997), no. 3, 413–422.

[GM2] G. Grant and E. Manduchi, Root numbers and algebraic points on elliptic surfaces with elliptic base, *Duke Math. J.* **93** (1998), no. 3, 479–486.

[EGAIV] A. Grothendieck, Éléments de géométrie algébrique IV: Étude locale des schémas et des morphismes de schémas IV, *Inst. Hautes Études Sci. Publ. Math. No. 32*, 1967, 361 pages.

[HarT] J. Harris and Y. Tschinkel, Rational points on quartics, *Duke Math. Journ.*, **104** (2000), no. 3, 477–500.

[HT] B. Hassett and Y. Tschinkel, Abelian fibrations and rational points on symmetric products, *Internat. J. of Math.* **11** (2000), no. 9, 1163–1176

[HT2] B. Hassett and Y. Tschinkel, Density of integral points on algebraic varieties, in: *Rational Points on Algebraic Varieties*, (Points rationnels des variétés algébriques, Luminy, 1999), 165–197, Progress in mathematics **199**, Birkhhäuser, Boston, 2001

[IP] V.A. Iskovskikh and Yu. G. Prokhorov, *Fano varieties: Algebraic geometry V*, 1–247, Encyclopaedia Math. Sci., 47, Springer, Berlin, 1999.

[Kod] K. Kodaira, On compact analytic surfaces I,II,II, *Ann. of Math. (2)* **71** (1960), 111–152; **77** (1963), 563–626; **78** (1963), 1–40.

[Kol1] J. Kollár, Higher direct images of dualizing sheaves II, *Ann. of Math. (2)* **124** (1986), no. 1, 171–202.

[Kol2] J. Kollár, *Rational curves on algebraic varieties,* Springer-Verlag, Berlin, 1996.

[Ko] S. J. Kovács, The cone of curves of a $K3$ surface, *Math. Ann.* **300** (1994), no. 4, 681–691.

[La] S. Lang, *Abelian Varieties,* Interscience Tracts in Pure and Applied Mathematics, Number 7, 1959.

[LT] S. Lang and J. Tate, Principal homogeneous spaces over abelian varieties, *Amer. J. Math.* **80** (1958), 659–684.

[LP] E. Looijenga and C. Peters, Torelli theorems for Kähler $K3$ surfaces, *Compositio Math.* **42** (1980/81), no. 2, 145–186.

[Miy] T. Miyake, *Modular forms*, Springer-Verlag, Berlin, 1989.

[MM] S. Mori and S. Mukai, The uniruledness of the moduli space of curves of genus 11, in: *Algebraic geometry (Tokyo/Kyoto, 1982)*, 334–353, Lecture Notes in Math., 1016, Springer, Berlin, 1983.

[Mu] S. Mukai, On the moduli space of bundles on $K3$ surfaces I, in: *Vector bundles on algebraic varieties (Bombay, 1984)*, 341–413, Tata Inst. Fund. Res. Stud. Math., 11, Tata Inst. Fund. Res., Bombay, 1987.

[Ogg] A. P. Ogg, Cohomology of abelian varieties over function fields, *Ann. of Math. (2)* **76** (1962), 185–212.

[Ra] Z. Ran, Hodge theory and deformations of maps, *Compositio Math.* **97** (1995), no. 3, 309–328.

[Ro] P. Roquette, On the Galois cohomology of the projective linear group and its applications to the construction of generic splitting fields of algebras, *Math. Ann.* **150** (1963), 411–439.

[SD] B. Saint-Donat, Projective models of K3 surfaces, *Amer. J. Math.* **96** (1974), 602–639.

[Se1] J.P. Serre, *A course in arithmetic,* Springer-Verlag, New York-Heidelberg, 1973.

[Se2] J.P. Serre, *Lectures on the Mordell-Weil Theorem,* 2nd edition, Vieweg, Braunschweig, 1990.

[Shaf1] I.R. Shafarevich, Principal homogeneous spaces defined over a function field (Russian) *Trudy Mat. Inst. Steklov.* **64** (1961), 316–346; *Amer. Math. Soc. Transl. (2)* **37** (1964), 85–114.

[Shaf2] I.R. Shafarevich, Algebraic surfaces: By the members of the seminar of I. R. Šafarevič, *Proceedings of the Steklov Institute of Mathematics, No. 75* (1965) American Mathematical Society, Providence, R.I. 1965.

[Shi] T. Shioda, On elliptic modular surfaces, *J. Math. Soc. Japan* **24** (1972), 20–59.

[SI] T. Shioda and H. Inose, On singular $K3$ surfaces, in: *Complex analysis and algebraic geometry*, 119–136, Iwanami Shoten, Tokyo, 1977.

[Si] J. Silverman, Rational points on $K3$ surfaces: a new canonical height, *Invent. Math.* **105** (1991), no. 2, 347–373.

[St] H. Sterk, Finiteness results for algebraic $K3$ surfaces, *Math. Z.* **189** (1985), no. 4, 507–513.

[We] A. Weil, Arithmétique et géométrie sur les variétés algébriques, in: *Actualités Sci. Indust.* **206**, Hermann, Paris, 1936, 3–16; reprinted in: *Oeuvres Scientifiques* Vol. I, Springer-Verlag 1980, 87–100.

Department of Mathematics
Rice University, MS 136
6100 South Main Street
Houston, Texas 77005-1892
USA
hassett@math.rice.edu