Compositio Math. 140 (2004) 567–580
DOI: 10.1112/S0010437X03000381

Arithmetic on elliptic threefolds

Rania Wazir

Abstract

In a recent paper, Rosen and Silverman showed that Tate's conjecture on algebraic cycles implies a formula of Nagao, which gives the rank of an elliptic surface in terms of a weighted average of fibral Frobenius trace values. In this article, we extend their result to the case of elliptic threefolds. The main ingredients of our argument are a Shioda–Tate-like formula for elliptic threefolds, and a relation between the 'average' number of rational points on singular fibers and the Galois action on those fibers.

1. Introduction

Let K be a function field of transcendence degree $n-1$ over $\mathbb{Q}$, and consider an elliptic curve E/K given by the Weierstrass equation

$$E : y^2 = x^3 + Ax + B, \quad \text{with } A, B \in K, \tag{1}$$

and with discriminant $\Delta := 4A^3+27B^2 \not\equiv 0$. A smooth n-dimensional variety $\mathcal{E} \to \mathbb{P}^{n-1}$ with generic fiber E is called an elliptic n-fold over $\mathbb{Q}$. By the Mordell–Weil theorem, the set $E(K)$ of rational points on E is a finitely-generated abelian group; its rank has been an object of intense study and speculation, yet many of its properties, and the relation to the underlying geometry of E, remain elusive. Some progress in this direction was made by Rosen and Silverman [RS98] in the case of elliptic surfaces (i.e. $n = 2$), based on a conjectural formula of Nagao [Nag97] relating the rank of an elliptic surface to an average of its fibral Frobenius trace values.

To be more specific, define, for each $t \in \mathbb{P}^{n-1}(\mathbb{F}_p)$ and each prime p,

$$a_p(\mathcal{E}_t) := \begin{cases} \mathrm{Trace}(\mathrm{Frob}_p | H^1_{\text{ét}}(\mathcal{E}_t/\bar{\mathbb{Q}}, \mathbb{Q}_l)) & \text{if } \mathcal{E}_t \text{ has good reduction at } p, \\ 0 & \text{otherwise,} \end{cases}$$

where Frob_p denotes the Frobenius morphism over $\mathbb{F}_p$, and let

$$A_p(\mathcal{E}) := \frac{1}{p^n} \sum_{t \in \mathbb{P}^{n-1}(\mathbb{F}_p)} a_p(\mathcal{E}_t).$$

Then in the case $n = 2$, Nagao [Nag97] conjectured that

$$\lim_{X\to\infty} \frac{1}{X} \sum_{p \leqslant X} -A_p(\mathcal{E}) \log p = \mathrm{rank}\, E(\mathbb{Q}(T)).$$

Assuming Tate's Conjecture for $\mathcal{E}$, Rosen and Silverman [RS98] were able to prove the following analytic version of Nagao's formula for non-split elliptic surfaces $\mathcal{E}$:

$$\operatorname*{res}_{s=1} \sum_p -A_p(\mathcal{E}) \frac{\log p}{p^s} = \mathrm{rank}\, E(\mathbb{Q}(T)).$$

Received 18 January 2002, accepted in final form 16 May 2003.
2000 Mathematics Subject Classification 11G05, 14D06.
Keywords: elliptic n-fold, Mordell–Weil group, Shioda–Tate formula, Nagao formula, Frobenius trace values.

The aim of this paper is to generalize this result to the case of elliptic threefolds.

Theorem 1.1. *Let k be a number field, $\mathfrak{p}$ a prime in k, and $q_{\mathfrak{p}}$ its norm. Let $\mathcal{E} \to \mathcal{S}$ be a non-split elliptic threefold with section σ, defined over k, and assume $\mathcal{E}(k) \neq \emptyset$. Then Tate's conjecture for $\mathcal{E}/k$ and $\mathcal{S}/k$ implies*

$$\operatorname*{res}_{s=1} \sum_{\mathfrak{p}} -A_{\mathfrak{p}}(\mathcal{E}) \frac{\log q_{\mathfrak{p}}}{q_{\mathfrak{p}}^s} = \operatorname{rank} \mathcal{E}(\mathcal{S}/k).$$

We refer the reader to § 2 for more precise definitions of elliptic n-folds, and their basic properties. Section 3 is dedicated to generalizing two important theorems from the theory of elliptic surfaces to non-split elliptic n-folds of arbitrary dimension: an isomorphism in cohomology $H^1_{\text{ét}}(\mathcal{S}/\bar{k}, \mathbb{Q}_l) \cong H^1_{\text{ét}}(\mathcal{E}/\bar{k}, \mathbb{Q}_l)$ and a Shioda–Tate-type isomorphism, describing the Galois-module decomposition of the Neron–Severi group of $\mathcal{E}$. In § 4, we find a geometric interpretation for the Galois action on the singular fibers of an elliptic threefold $\mathcal{E}$, and, in the final section, reinterpret our results in terms of L-series, which, together with Tate's conjecture, leads to a proof of Theorem 1.1.

2. Basic definitions and notation

Let k be a number field with ring of integers O_k, and for a prime $\mathfrak{p} \in O_k$, let $\mathbb{F}_{\mathfrak{p}}$ be its residue field and $q_{\mathfrak{p}}$ its norm. For a field F, let $\bar{F}$ denote its separable algebraic closure. If $\mathcal{X}$ and $\mathcal{Y}$ are varieties defined over k, we write morphism (respectively section, rational section) for maps $f : \mathcal{X} \to \mathcal{Y}$ defined over $\bar{k}$, and k-morphism (respectively k-section, rational k-section) for maps defined over k.

An elliptic n-fold defined over k is a smooth, projective variety $\mathcal{E}/k$ of dimension n, together with a proper, flat k-morphism $\pi : \mathcal{E} \to \mathcal{S}$ to a smooth projective $(n-1)$-dimensional variety $\mathcal{S}/k$, such that the generic fiber is a smooth elliptic curve E defined over $K := k(\mathcal{S})$, the function field of $\mathcal{S}/k$; let $\widehat{K} := \bar{k}(\mathcal{S})$. Furthermore, we take the elliptic n-fold $\mathcal{E}/k$ to be non-split, with k-section $\sigma : \mathcal{S} \to \mathcal{E}$. Denote by (O) the image of the section σ in $\mathcal{E}$, and by O the corresponding point on E. Assume also that $\mathcal{E}(k) \neq \emptyset$; because of the k-section σ, this is equivalent to $\mathcal{S}(k) \neq \emptyset$. This assumption is made in order to ensure that $\operatorname{Pic}^0_{\mathcal{E}}$ and $\operatorname{Pic}^0_{\mathcal{S}}$ are defined over k (see § 2).

The closed subset $\Delta := \{s \in S \mid \mathcal{E}_s \text{ is not regular}\}$ is called the discriminant locus of $\mathcal{E}$. Note that Δ is a divisor on $\mathcal{S}$, and is also defined over k.

We briefly observe some basic properties of the elliptic n-fold $\mathcal{E}$. Let $(\tau, \mathcal{B})$ be the $\widehat{K}/\bar{k}$-trace of the generic fiber E of $\mathcal{E}$ (see [Lan83, p. 138] for definitions and details). Then the requirement that $\mathcal{E}$ be non-split is equivalent to saying that $\mathcal{B}$ is trivial; this description will be particularly useful in proving the isomorphism of Picard varieties in § 3. Moreover, note that since π is proper and faithfully flat, with reduced, connected generic fiber, it follows that $\pi_*(\mathcal{O}_{\mathcal{E}})$ is isomorphic to $\mathcal{O}_{\mathcal{S}}$, and hence the fibers $\mathcal{E}_s$ are connected, by Stein factorization. Finally, [GD66, Proposition IV.15.4.2] implies that π is flat if and only if the dimension of the fibers is locally constant.

By the Mordell–Weil theorem for function fields [Lan83, Theorem 6.1], the group $E(K)$ of K-rational points on E is a finitely generated Abelian group; since there is a natural isomorphism between $E(K)$ and the group of rational k-sections $\mathcal{E}(\mathcal{S}/k)$ [Sil94, Proposition III.3.10], we will refer to either indiscriminately as the Mordell–Weil group of $\mathcal{E}$, and to their rank as the Mordell–Weil rank of $\mathcal{E}$. This defines one side of the equation in Theorem 1.1, so we now address the terms on the other side of the equation, and make our notion of 'average' of fibral Frobenius trace values more precise.

Let $R \subset O_k$ be a finite set of primes in the ring of integers of k, and let $O_R \subset O_k$ be the subring of R-integers. By [GD66, Section IV.8], all algebraic constructions over k can be made over O_R for R sufficiently large. In particular, we choose R such that there are proper, flat morphisms

https://doi.org/10.1112/S0010437X03000381 Published online by Cambridge University Press

$\pi_R : \mathcal{E}_R \to \mathcal{S}_R$ of smooth, projective O_R-schemes, which induce π by base change. All sums $\sum_{\mathfrak{p}}$, products $\prod_{\mathfrak{p}}$, and reductions mod $\mathfrak{p}$ will henceforth be taken with respect to prime ideals $\mathfrak{p} \subset O_R$, where we recall that, given any variety $\mathcal{V}/k$, and an integral model $\mathcal{V}_R \to \operatorname{Spec} O_R$, reduction mod $\mathfrak{p}$ for some $\mathfrak{p} \subset O_R$ means taking the fiber over $\mathfrak{p}$: $\tilde{\mathcal{V}} := \mathcal{V} \times_{O_R} \mathfrak{p}$. We denote by $\tilde{\mathcal{V}}/\bar{\mathbb{F}}_{\mathfrak{p}}$ the variety $\tilde{\mathcal{V}} \times_{\mathbb{F}_{\mathfrak{p}}} \bar{\mathbb{F}}_{\mathfrak{p}}$. In the following, we will have several occasions for enlarging R; this introduces ambiguity for finitely-many primes $\mathfrak{p}$, but will have no effect on the order of vanishing computation of the various L-series we are interested in.

Definition 2.1. For any smooth, projective variety $\mathcal{V}/k$ and any $\mathfrak{p} \subset O_R$, let

$$a_{\mathfrak{p}}(\mathcal{V}) := \operatorname{Trace}(\operatorname{Frob}_{\mathfrak{p}} | H^1_{\text{ét}}(\mathcal{V}/\bar{k}, \mathbb{Q}_l)),$$
$$b_{\mathfrak{p}}(\mathcal{V}) := \operatorname{Trace}(\operatorname{Frob}_{\mathfrak{p}} | H^2_{\text{ét}}(\mathcal{V}/\bar{k}, \mathbb{Q}_l)),$$
$$c_{\mathfrak{p}}(\mathcal{V}) := \operatorname{Trace}(\operatorname{Frob}_{\mathfrak{p}} | H^3_{\text{ét}}(\mathcal{V}/\bar{k}, \mathbb{Q}_l)),$$

where cohomology is taken with l-adic coefficients such that $\gcd(l, q_{\mathfrak{p}}) = 1$.

Returning to the case of our elliptic n-fold $\mathcal{E}$, we also define, for a given point $x \in \tilde{\mathcal{S}}(\mathbb{F}_{\mathfrak{p}})$,

$$a_{\mathfrak{p}}(\mathcal{E}_x) := 1 - \#\tilde{\mathcal{E}}_x(\mathbb{F}_{\mathfrak{p}}) + q_{\mathfrak{p}} m_x,$$

where m_x is the number of $\mathbb{F}_{\mathfrak{p}}$-rational components of the fiber $\tilde{\mathcal{E}}_x$. These $a_{\mathfrak{p}}(\mathcal{E}_x)$ will be called the fibral Frobenius trace values of $\tilde{\mathcal{E}}$. Note that by the Lefshetz fixed-point theorem, when the fiber $\tilde{\mathcal{E}}_x$ is smooth, this definition agrees with Definition 2.1. Finally, we define the 'average' of fibral Frobenius trace values $A_{\mathfrak{p}}(\mathcal{E})$, which is given by

$$A_{\mathfrak{p}}(\mathcal{E}) := \frac{1}{q_{\mathfrak{p}}^{(n-1)}} \sum_{x \in \tilde{\mathcal{S}}(\mathbb{F}_{\mathfrak{p}})} a_{\mathfrak{p}}(\tilde{\mathcal{E}}_x).$$

3. Picard varieties

The goal of this section is to generalize results from the geometric theory of elliptic surfaces, to the case of elliptic n-folds of arbitrary dimension. The two main theorems will be an isomorphism of the Picard varieties of $\mathcal{E}$ and $\mathcal{S}$, and a Shioda–Tate-type formula for elliptic n-folds. The proofs are based on the work of Shioda and Raynaud for elliptic surfaces [Shi99, Theorems 1 and 2].

Let F be a field, and X/F be a smooth projective variety. The Picard scheme Pic_X of X can be realized as the group scheme representing the Picard functor from the category of F-schemes to the category of Abelian groups. Its group of $\bar{F}$-points is $\operatorname{Pic}(X)$, the group of divisors on X modulo linear equivalence. Its identity component is an Abelian group scheme $\operatorname{Pic}^0_{\mathrm{X}}$, whose $\bar{F}$-points are the group of divisors on X algebraically equivalent to zero, modulo linear equivalence. Denote this group by $\operatorname{Pic}^0(X)$. When F is of characteristic zero, $\operatorname{Pic}^0_{\mathrm{X}}$ is an abelian variety, called the Picard variety of X. The Neron Severi group of X is defined by $\operatorname{NS}(X) = \operatorname{Pic}(X)/\operatorname{Pic}^0(X)$. We let $\operatorname{Pic}(X/F)$, $\operatorname{Pic}^0(X/F)$ and $\operatorname{NS}(X/F)$ denote the Galois-invariant subgroups of $\operatorname{Pic}(X)$, $\operatorname{Pic}^0(X)$ and $\operatorname{NS}(X)$, respectively. Note that if $X(F) \neq \emptyset$, then Pic_X and $\operatorname{Pic}^0_{\mathrm{X}}$ are defined over F. For a brief account of definitions and properties, see [Mum82, Section 0.d].

Definition 3.1. The trivial part of $\operatorname{NS}(\mathcal{E}) \otimes \mathbb{Q}$, denoted $\mathcal{T}$, is the subspace generated by the image of the zero section (O), and by all geometrically irreducible components of the fibral divisors. Let $\mathcal{F}$ be the subspace of $\mathcal{T}$ generated by the non-identity components of the fibral divisors, where the identity component of a fibral divisor is the component intersecting (O).

Note that $\mathcal{T}$ is generated by (O), $\pi^*\operatorname{NS}(\mathcal{S})$, and $\mathcal{F}$. Furthermore, for all but finitely many primes $\mathfrak{p}$, the trivial part of $\operatorname{NS}(\tilde{\mathcal{E}}/\bar{\mathbb{F}}_{\mathfrak{p}}) \otimes \mathbb{Q}$ is isomorphic to $\tilde{\mathcal{T}}$, the subspace obtained by taking the generators of $\mathcal{T}$ and reducing modulo $(\mathfrak{p})$. Thus, enlarging the set of bad primes R if necessary, we can assume that this holds for all $\mathfrak{p} \subset O_R$.

3.1 A non-degenerate pairing

In the case of an elliptic surface $\mathcal{E}$, the proof of the isomorphism between the Picard varieties of $\mathcal{E}$ and $\mathcal{S}$ relies on a non-degenerate bilinear pairing

$$\mathrm{Div}(\mathcal{E}) \times \mathrm{Div}(\mathcal{E}) \to \mathbb{Z}$$

given by intersection theory on surfaces [Sil94, Section III.8]. In the case of higher-dimensional varieties, it is no longer possible to get a pairing into $\mathbb{Z}$; however, we will show that it suffices to have a pairing with a notion of 'positivity'.

For the rest of § 3.1, assume that all varieties are smooth and projective over an algebraically closed field F. If Γ is a cycle on an n-dimensional variety X, then $\mathrm{cl}(\Gamma)$ denotes its cycle class modulo rational equivalence. The group of codimension-r cycles modulo rational equivalence is denoted $A^r(X)$, and $A(X) := \bigoplus_{r=0}^{n} A^r(X)$. Recall that the intersection pairing on X makes $A(X)$ into a commutative, associative graded ring, such that for any morphism $f : X \to W$, the induced map $f^* : A(W) \to A(X)$ is a ring homomorphism. Furthermore, if f is proper, $f_* : A(X) \to A(W)$ is a degree-shifting map of graded groups, and both f^* and f_* preserve algebraic equivalence [Ful80, Example 19.3.9 and Proposition 10.3]. Note also that if W is an $(n-1)$-dimensional variety and C, D are in $A^1(X)$, then the intersection $C.D$ has dimension $n-2$, and so by definition, $f_*(C.D) \in A^1(W)$. These observations allow us to define the following pairing on $\mathcal{E}$.

Definition 3.2. We have a symmetric, bilinear pairing

$$\langle \cdot, \cdot \rangle : \mathrm{Pic}(\mathcal{E}) \times \mathrm{Pic}(\mathcal{E}) \to \mathrm{Pic}(\mathcal{S})$$

given by

$$\langle \Lambda, \Upsilon \rangle := \pi_*(\Lambda.\Upsilon)$$

for any $\Lambda, \Upsilon \in \mathrm{Pic}(\mathcal{E})$. If C, D are divisors in $\mathrm{Div}(\mathcal{E})$, set $\langle C, D \rangle := \langle \mathrm{cl}(C), \mathrm{cl}(D) \rangle$.

Definition 3.3. We say an irreducible divisor C on $\mathcal{E}$ is fibral if $C \subset \pi^{-1}(G)$ for some $G \in \mathrm{Div}(\mathcal{S})$. A fibral divisor on $\mathcal{E}$ is a divisor D such that $D = \sum a_i C_i$, where the C_i are fibral. We say a divisor D is horizontal if $\pi(D) = \mathcal{S}$.

The following proposition shows that the pairing defined above has the same properties as the intersection pairing on elliptic surfaces. We sketch the proof below, and refer to [Sil94, Proposition III.8.2] for details. Recall first that a cycle class $\alpha \in A^r(X)$ is non-positive, written $\alpha \leqslant 0$, if there is a codimension-r cycle $\Gamma = \sum a_i [V_i]$ such that $a_i \leqslant 0$ for all i, and with $\mathrm{cl}(\Gamma) = \alpha$. Analogous definitions hold for $\alpha < 0$, $\alpha \geqslant 0$, and $\alpha > 0$.

Proposition 3.1. *Let $D \in \mathrm{Div}(\mathcal{E})$ be a fibral divisor, and $G \in \mathrm{Div}(\mathcal{S})$. Then:*

a) $\langle D, \pi^*(G) \rangle = 0$;

b) $\langle D, D \rangle \leqslant 0$;

c) *if* $\langle D, D \rangle = 0$, *then* $D \in \pi^*(\mathrm{Div}(\mathcal{S}))$.

Proof. a) This follows from the projection formula, once we note that $\pi_*(D) = 0$ for any fibral divisor D:

$$\langle D, \pi^*(G) \rangle = \pi_*(\mathrm{cl}(D).\,\mathrm{cl}(\pi^* G)) = \pi_*(D).G = 0.$$

b) Suppose that $D \subset \pi^{-1}(G)$, where G has irreducible decomposition $G = G_1 + G_2 + \cdots + G_m$. Then we can write

$$D = D_1 + D_2 + \cdots + D_m,$$

where $D_i \subset \pi^{-1}(G_i)$. Since $D_i \cap D_j \subset \pi^{-1}(G_i \cap G_j)$, $\dim(G_i \cap G_j) = 0$ and $\dim(D_i \cap D_j) = 1$, this implies that $\langle D_i, D_j \rangle = 0$ for $i \neq j$. Therefore,

$$\langle D, D \rangle = \langle D_1, D_1 \rangle + \langle D_2, D_2 \rangle + \cdots + \langle D_n, D_n \rangle.$$

Thus, it suffices to prove the theorem for each D_i separately, and we can assume that $D \subset \pi^* G$, for some irreducible $G \in \mathrm{Div}(\mathcal{S})$. Let

$$H := \pi^* G = \sum_{i=0}^{t} n_i \Gamma_i$$

be the irreducible decomposition of H. Note that $n_i \geqslant 0$ for all i, and (assuming Γ_0 is the component intersecting the k-section σ) $n_0 = 1$. Furthermore, since $D \subset H$, D can be written as

$$D = \sum_{i=0}^{t} a_i \Gamma_i = \sum_{i=0}^{t} \left(\frac{a_i}{n_i}\right) n_i \Gamma_i.$$

Define a second divisor by $D' = \sum_{i=0}^{t} (a_i/n_i)^2 n_i \Gamma_i$. Then $\langle D', H \rangle = 0$ by part a, and a simple computation on

$$\langle D, D \rangle = \langle D', H \rangle - 2\langle D, D \rangle + \langle H, D' \rangle$$

as in [Sil94] completes the proof.

c) By [Sil94], we have $a_i/n_i = a_0 \in \mathbb{Z}$ for all i. Plugging this into the irreducible decomposition of D gives

$$D = \sum_{i=0}^{t} \left(\frac{a_i}{n_i}\right) n_i \Gamma_i = \sum_{i=0}^{t} a_0 n_i \Gamma_i = a_0 H \in \pi^*(\mathrm{Div}(\mathcal{S})). \qquad \square$$

3.2 An isomorphism in cohomology

The cohomology of a smooth variety defined over k is intimately related to the Tate-module of its Picard variety. We recall that, given an abelian variety A/k, its l-adic Tate-module is defined as

$$T_l(A) := \varprojlim A[l^n]$$

where l is any prime in $\mathbb{Z}$, and $A[l^n] := \{a \in A(\bar{k}) \mid l^n a = 0\}$. The Tate module $T_l(A)$ has a natural structure as a $\mathrm{Gal}(\bar{k}/k)$-module. We prove that $\mathrm{Pic}^0_{\mathcal{E}} \cong \mathrm{Pic}^0_{\mathcal{S}}$ (Theorem 3.2 below) by first proving the isomorphism of Tate-modules, and this will follow quite easily from the following.

Theorem 3.1. *Let $(\tau, \mathcal{B})$ denote the $\widehat{K}/\bar{k}$-trace of E; then there is an exact sequence of abelian groups:*

$$0 \to \mathrm{Pic}^0(\mathcal{S}) \to \mathrm{Pic}^0(\mathcal{E}) \to \mathcal{B}(\bar{k}). \tag{2}$$

Proof. The morphism $\pi : \mathcal{E} \to \mathcal{S}$ induces a map $\pi^* : \mathrm{Pic}^0_{\mathcal{S}} \to \mathrm{Pic}^0_{\mathcal{E}}$. Furthermore, restriction to the generic fiber induces the morphism

$$\psi : \mathrm{Pic}^0_{\mathcal{E}} \times_{\mathcal{S}} \mathrm{Spec}(k(\mathcal{S})) \to \mathrm{Pic}^0_{\mathrm{E}} \cong E, \tag{3}$$

which, by the universal mapping property of the $\widehat{K}/\bar{k}$-trace $(\tau, \mathcal{B})$ of E, factors through $\mathcal{B}$, i.e. there is a unique homomorphism $\beta : \mathrm{Pic}^0_{\mathcal{E}} \to \mathcal{B}$ such that $\psi = \tau \circ \beta$. Thus, we have a sequence of morphisms

$$\mathrm{Pic}^0_{\mathcal{S}} \xrightarrow{\pi^*} \mathrm{Pic}^0_{\mathcal{E}} \xrightarrow{\beta} \mathcal{B}, \tag{4}$$

and it remains to show that, as maps on the $\bar{k}$-points, this is a short exact sequence of abelian groups:

$$0 \to \mathrm{Pic}^0(\mathcal{S}) \xrightarrow{\pi^*} \mathrm{Pic}^0(\mathcal{E}) \xrightarrow{\beta} \mathcal{B}(\bar{k}). \tag{5}$$

https://doi.org/10.1112/S0010437X03000381 Published online by Cambridge University Press

The injectivity of π^* follows from the existence of the global section $\sigma_0 : \mathcal{S} \to \mathcal{E}$. By definition, $\pi \circ \sigma = \mathrm{id}_{\mathcal{S}}$, so $\mathrm{id}_{\mathrm{Pic}(\mathcal{S})} = (\pi \circ \sigma)^* = \sigma^* \circ \pi^*$.

To show exactness at the middle, note first that $\psi \circ \pi^* = 0$ (because π^* sends $\mathrm{Pic}^0(\mathcal{S})$ to fibral divisors in $\mathrm{Pic}^0(\mathcal{E})$, and restriction to the generic fiber sends fibral divisors in $\mathrm{Pic}^0(\mathcal{E})$ to zero). By the injectivity of τ, $\beta \circ \pi^* = 0$ also and, therefore, $\mathrm{Im}(\pi^*) \subset \mathrm{Ker}(\beta)$. Finally, to show $\mathrm{Ker}(\beta) = \mathrm{Im}(\pi^*)$, take any $0 \neq \Gamma \in \mathrm{Ker}(\beta)$. Then $\Gamma = \mathrm{cl}(D)$ for some divisor D with $D|_E = 0$, and thus D must be a fibral divisor. Since $\mathrm{cl}(D) \in \mathrm{Pic}^0(\mathcal{E})$, it follows that $\langle D, F\rangle = 0$ for every divisor F on $\mathcal{E}$ and, in particular, $\langle D, D\rangle = 0$. By Proposition 3.1, part c, it follows that $D \in \pi^*(\mathrm{Div}(\mathcal{S}))$. Thus, we have $D = \pi^* C$ for some $C \in \mathrm{Div}(\mathcal{S})$. Since also $D \sim_{\mathrm{alg}} 0$, this implies

$$C = \sigma^* \circ \pi^* C = \sigma^* D \sim_{\mathrm{alg}} 0,$$

and, therefore, $\Gamma = \mathrm{cl}(D) \in \pi^*(\mathrm{Pic}^0(\mathcal{S}))$. □

Now we are ready to prove the isomorphism of Tate modules; in fact, we will prove the following stronger result.

THEOREM 3.2. *Let $\pi : \mathcal{E} \to \mathcal{S}$ be a non-split elliptic n-fold. Then $\mathrm{Pic}^0_{\mathcal{S}}$ and $\mathrm{Pic}^0_{\mathcal{E}}$ are isomorphic as abelian varieties over k.*

Proof. The elliptic n-fold $\mathcal{E}$ is non-split, so $\mathcal{B}$ must be trivial. From the exact sequence (2), it then follows that $\mathrm{Pic}^0(\mathcal{S})$ and $\mathrm{Pic}^0(\mathcal{E})$ are isomorphic as groups and, therefore, since π^* is defined over k, the Tate modules $T_l(\mathrm{Pic}^0_{\mathcal{E}})$ and $T_l(\mathrm{Pic}^0_{\mathcal{S}})$ are isomorphic as $\mathrm{Gal}(\bar{k}/k)$-modules. This implies that π^* is an isogeny, and since it is also injective, we have $\mathrm{Pic}^0_{\mathcal{E}} \cong \mathrm{Pic}^0_{\mathcal{S}}$ by [Mum70, Corollary III.10.1]. □

Let $\mathcal{V}$ be a smooth, projective variety defined over k, and define $V_\ell(\mathrm{Pic}^0_{\mathcal{V}}) := T_\ell(\mathrm{Pic}^0_{\mathcal{V}}) \otimes \mathbb{Q}_l$. Then the Galois-module isomorphism [Mil80, Corollary III.4.19]

$$V_\ell(\mathrm{Pic}^0_{\mathcal{V}})(-1) \cong H^1_{\text{ét}}(\mathcal{V}/\bar{k}, \mathbb{Q}_l),$$

together with Theorem 3.2 above, imply as an immediate corollary the following.

COROLLARY 3.1. *If $\pi : \mathcal{E} \to \mathcal{S}$ is a non-split elliptic n-fold, then*

$$H^1_{\text{ét}}(\mathcal{S}/\bar{k}, \mathbb{Q}_l) \cong H^1_{\text{ét}}(\mathcal{E}/\bar{k}, \mathbb{Q}_l).$$

as $\mathrm{Gal}(\bar{k}/k)$-modules and, in particular, $a_{\mathfrak{p}}(\mathcal{E}) = a_{\mathfrak{p}}(\mathcal{S})$.

3.3 A Shioda–Tate formula

In this section, we prove that $\mathrm{NS}(\mathcal{E}) \otimes \mathbb{Q}$ is generated by $\mathcal{T}$ and by the k-rational sections. In the case of elliptic surfaces, this is the main result of the Shioda–Tate formula [Shi72, Theorem 1.1]. In order to prove an analogous formula for elliptic n-folds, we need to take a closer look at restriction to the generic fiber at the level of geometric points.

To every divisor class $\mathrm{cl}(D)$ on $\mathcal{E}$, we associate the divisor $D|_E = D.E$ on the generic fiber E, and this defines a homomorphism

$$\mathrm{Pic}(\mathcal{E}) \to \mathrm{Pic}(E/\widehat{K}). \tag{6}$$

Then, using the given rational point $O \in E(K)$, adjust the image by sending $\mathrm{cl}(D)$ to $\mathrm{cl}(D')$, where $D' := D.E - (D.E)O$; the divisor D' is thus a degree zero divisor on E, and the homomorphism becomes

$$\phi : \mathrm{Pic}(\mathcal{E}) \to \mathrm{Pic}^0(E/\widehat{K}) \cong E(\widehat{K}). \tag{7}$$

We wish to determine the kernel of this map.

Lemma 3.1. *Let $\check{\mathcal{T}}$ be the subgroup of* $\mathrm{Pic}(\mathcal{E})$ *generated by the irreducible components of the fibral divisors, and by the zero-section* (O). *Then*

$$0 \to \check{\mathcal{T}} \xrightarrow{\eta} \mathrm{Pic}(\mathcal{E}) \xrightarrow{\phi} E(\widehat{K}) \to 0 \tag{8}$$

is a short exact sequence of abelian groups.

Proof. Note first that the morphism ϕ is surjective: given any $\widehat{K}$-rational divisor C on E, taking the schematic closure of its irreducible components gives a divisor $\bar{C}$ on $\mathcal{E}$ such that $\bar{C}.E = C$.

Furthermore, by construction, $\check{\mathcal{T}} \subset \ker(\phi)$. To show that $\check{\mathcal{T}} = \ker(\phi)$, consider $\Upsilon \in \ker(\phi)$. In this case, $\Upsilon = \mathrm{cl}(D)$, where $D|_E \sim 0$ on E, and so $D|_E = \mathrm{div}(h)$, where

$$h \in \widehat{K}(E) = \bar{k}(\mathcal{S})(E) = \bar{k}(\mathcal{E}).$$

Therefore, there exists $H \in \bar{k}(\mathcal{E})$ such that $(H)|_E = (h)$. If $D' := D - (H)$, then D' must be in some fiber, i.e. $D' \in \check{\mathcal{T}}$, and therefore $\Upsilon = \mathrm{cl}(D) = \mathrm{cl}(D') \in \check{\mathcal{T}}$. □

Theorem 3.3 (A Shioda–Tate formula for elliptic n-folds). *Embed* $\mathcal{E}(\mathcal{S}/\bar{k})$ *into* $\mathrm{NS}(\mathcal{E})$ *by sending a section* γ *to the divisor* $\overline{\gamma(\mathcal{S})} - \sigma(\mathcal{S})$ *(where* $\overline{\gamma(\mathcal{S})}$ *is the schematic closure of* $\gamma(\mathcal{S})$ *in* $\mathcal{E}$*). Then there is a decomposition of* $\mathrm{Gal}(\bar{k}/k)$*-modules,*

$$\mathrm{NS}(\mathcal{E}) \otimes \mathbb{Q} \cong (\mathcal{E}(\mathcal{S}/\bar{k}) \otimes \mathbb{Q}) \oplus \mathcal{T}.$$

Proof. Comparing the short exact sequences (2) and (8), we see that ψ maps $\mathrm{Pic}(\mathcal{E})$ surjectively onto $E(\widehat{K})$, while at the same time sending $\mathrm{Pic}^0(\mathcal{E})$ to $B(\bar{k}) = 0$. This implies that

$$\mathrm{NS}(\mathcal{E}) := \mathrm{Pic}(\mathcal{E}) / \mathrm{Pic}^0(\mathcal{E}) \twoheadrightarrow E(\widehat{K}), \tag{9}$$

with kernel $\mathcal{T}'$, the image of $\check{\mathcal{T}}$ in $\mathrm{NS}(\mathcal{E})$. Thus, we have an exact sequence

$$0 \to \mathcal{T}' \to \mathrm{NS}(\mathcal{E}) \to E(\widehat{K}) \to 0.$$

Since the action of Galois sends fibral divisors to fibral divisors, and horizontal to horizontal, this sequence splits as a Galois module after tensoring with $\mathbb{Q}$; noting that $\mathcal{T}' \otimes \mathbb{Q} = \mathcal{T}$ then gives the desired formula. □

Corollary 3.2. *With notation as above,*

$$\mathrm{rank}\,\mathrm{NS}(\mathcal{E}/k) = 1 + \mathrm{rank}\,\mathcal{E}(\mathcal{S}/k) + \mathrm{rank}\,\mathrm{NS}(\mathcal{S}/k) + \mathrm{rank}\,\mathcal{F}^{\mathrm{Gal}(\bar{k}/k)},$$

where $\mathcal{F}$ *is the vector space generated by the non-identity geometrically irreducible components of the fibral divisors.*

Proof. Recall that $\mathcal{T}$ is generated by (O), $\pi^*(\mathrm{NS}(\mathcal{S}))$ and $\mathcal{F}$, and the corollary follows by taking $\mathrm{Gal}(\bar{k}/k)$-invariants of the Shioda–Tate formula for elliptic n-folds. □

4. The singular fibers

The goal of this section is to prove Theorem 4.1 below, which establishes a geometric interpretation for the action of Frobenius on the singular fibers. Our main tools will be Tate's algorithm for determining the singularity type of a given fiber, and an effective version of the geometric Chebotarev density theorem, and this requires that we now restrict to the case of an *elliptic threefold* $\mathcal{E}/k$.

Theorem 4.1. *Let* $\mathcal{E}/k$ *be an elliptic threefold, with notation as before. Then*

$$\sum_{x \in \tilde{\Delta}(\mathbb{F}_{\mathfrak{p}})} (m_x - 1) = q_{\mathfrak{p}}\,\mathrm{Trace}(\mathrm{Frob}_{\mathfrak{p}} | \tilde{\mathcal{F}}) + O(\sqrt{q_{\mathfrak{p}}}),$$

where we recall that $\tilde{\mathcal{F}}$ *is the vector space generated by all non-identity components of* $\pi^{-1}(\tilde{\Delta})$ *(the identity component is the component intersecting* (O)*).*

Proof. Let $\Delta = \Delta_1 + \cdots + \Delta_r$ be the irreducible decomposition (over $\bar{k}$) of the discriminant Δ of $\pi : \mathcal{E} \to \mathcal{S}$; then, by enlarging the set of bad primes R if necessary, the discriminant locus of $\tilde{\pi} : \tilde{\mathcal{E}} \to \tilde{\mathcal{S}}$ is given by $\tilde{\Delta}$, the reduction of Δ mod$(\mathfrak{p})$, which has irreducible decomposition

$$\tilde{\Delta} = \tilde{\Delta}_1 + \cdots + \tilde{\Delta}_r.$$

(This is cheating a bit. The Δ_i are not all defined over k, hence it does not make sense to talk about reduction mod $\mathfrak{p}$. However, there is a finite Galois extension h of k, and a prime ideal $\mathfrak{B}|\mathfrak{p}$ in O_h such that $\tilde{\Delta}_i = \Delta_i \mod \mathfrak{B}$ for all i). Now assume that, for all $1 \leqslant j \leqslant r$,

$$\sum_{x \in \tilde{\Delta}_j(\mathbb{F}_\mathfrak{p})} (m_x - 1) = q_\mathfrak{p} \operatorname{Trace}(\operatorname{Frob}_\mathfrak{p} | \tilde{\mathcal{F}}_j) + O(\sqrt{q_\mathfrak{p}}),$$

where $\tilde{\mathcal{F}}_j$ is the vector space generated by the non-identity fibral divisors over $\tilde{\Delta}_j$. Letting J be the error term coming from overcounting the points $x \in \tilde{\Delta}_i \cap \tilde{\Delta}_j$, we have

$$\begin{aligned}\sum_{x \in \tilde{\Delta}(\mathbb{F}_\mathfrak{p})} (m_x - 1) &= \sum_{j=1}^{r} \sum_{x \in \tilde{\Delta}_j(\mathbb{F}_\mathfrak{p})} (m_x - 1) + J, \\ &= \sum_{j=1}^{r} q_\mathfrak{p} \operatorname{Trace}(\operatorname{Frob}_\mathfrak{p} | \tilde{\mathcal{F}}_j) + O(\sqrt{q_\mathfrak{p}}) + J, \\ &= q_\mathfrak{p} \operatorname{Trace}(\operatorname{Frob}_\mathfrak{p} | \tilde{\mathcal{F}}) + O(\sqrt{q_\mathfrak{p}}) + J.\end{aligned}$$

Thus, if we can show that J only enters into the error term, it will suffice to prove the theorem with Δ replaced by one of its irreducible components. As we will have several occasions to thus 'throw out' bad points, we will refer to this as the elimination principle.

Let P be a property such that, for every prime $\mathfrak{p} \subset O_R$, the set $S \subset \tilde{\Delta}(\bar{\mathbb{F}}_\mathfrak{p})$ of points having property P is finite, and, by enlarging R if necessary, $S = \tilde{V}$ for some finite set of points $V \subset \Delta(\bar{k})$. Then $\#S \leqslant \#V$ is bounded independently of $\mathfrak{p}$. Furthermore, for every $x \in V$, the number of geometrically irreducible components of $\tilde{\mathcal{E}}_x$ is the same as the number of irreducible components of $\mathcal{E}_x$, and since V is a finite set, this shows that there is an upper bound M on the number of irreducible components in a fiber, independent of x and $\mathfrak{p}$. Therefore,

$$J = \sum_{x \in S(\mathbb{F}_\mathfrak{p})} m_x \leqslant M(\#S) \leqslant M(\#V)$$

is bounded independently of x and $\mathfrak{p}$, and throwing out points with property P has no effect on our calculation.

In particular, it is clear that points $x \in \tilde{\Delta}_i \cap \tilde{\Delta}_j$ satisfy the elimination principle, so we can let $\tilde{\Delta} = \tilde{\Delta}_i$ and assume that $\tilde{\Delta}$ is irreducible. However, *a priori* we do not know whether $\tilde{\Delta}_i$ is defined over $\mathbb{F}_\mathfrak{p}$; but since in the case $\tilde{\Delta}_i$ is not defined over $\mathbb{F}_\mathfrak{p}$ the only rational points $x \in \tilde{\Delta}_i(\mathbb{F}_\mathfrak{p})$ must lie in $\tilde{\Delta}_i \cap \tilde{\Delta}_j$, we can also assume that $\tilde{\Delta}_i$ is defined over $\mathbb{F}_\mathfrak{p}$.

Denote by $\eta : \hat{\Delta} \to \Delta$ the normalization of Δ, and (again enlarging R if necessary) extend this to an integral model $\eta_R : \hat{\Delta}_R \to \Delta_R$. Then the set of singular points on $\tilde{\Delta}$ satisfy the elimination principle. Further, since in our application of Tate's algorithm we are only interested in $k(\tilde{\Delta})$, we can replace $\tilde{\Delta}$ by $\hat{\tilde{\Delta}}$, and assume that $\tilde{\Delta}$ is non-singular.

We next apply Tate's algorithm to the localization of $\tilde{\mathcal{E}}$ at $\tilde{\Delta}$ to determine the generic Kodaira type of the singular fibers over $\tilde{\Delta}$. Let $\mathcal{O}_{\tilde{\mathcal{S}},\tilde{\Delta}}$ be the local ring of $\tilde{\Delta}$ on $\tilde{\mathcal{S}}$. Then $\mathcal{O}_{\tilde{\mathcal{S}},\tilde{\Delta}}$ is a discrete valuation ring, with residue field $F := \mathbb{F}_\mathfrak{p}(\tilde{\Delta})$ and prime ideal $\mathfrak{m}$. Let

$$\tilde{\mathcal{E}}_{\tilde{\Delta}} := \tilde{\mathcal{E}} \times_{\mathcal{O}_{\tilde{\mathcal{S}}}} \mathcal{O}_{\tilde{\mathcal{S}},\tilde{\Delta}}$$

be the localization of $\tilde{\mathcal{E}}$ at $\tilde{\Delta}$, then a Weierstrass equation for $\tilde{\mathcal{E}}_{\tilde{\Delta}}$ is given by

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \quad a_i \in \mathcal{O}_{\tilde{\mathcal{S}},\tilde{\Delta}}. \tag{10}$$

Remark 4.1. Note that $\tilde{\mathcal{E}}_{\tilde{\Delta}}$ is an elliptic curve defined over the discrete valuation ring $\mathcal{O}_{\tilde{\mathcal{S}},\tilde{\Delta}}$, which has *non-perfect* residue field F, whereas Tate's algorithm is for elliptic curves over discrete valuation rings with *perfect* residue fields. However, the proof of Tate's algorithm works verbatim for any residue field with the property that all extensions of degree 2 or 3 are separable (see [Tat75] or [Sil94, § IV.9]). Thus, if R is expanded to include all primes $\mathfrak{p}$ such that $2|q_{\mathfrak{p}}$ or $3|q_{\mathfrak{p}}$, then Tate's algorithm can also be applied here.

We return to the proof of Theorem 4.1.

We note that localizing $\mathcal{E}$ over Δ gives an elliptic curve defined over the discrete valuation ring $\mathcal{O}_{\mathcal{S},\Delta}$, and the Weierstrass equation for $\tilde{\mathcal{E}}_{\tilde{\Delta}}$ can be taken to be the reduction mod $\mathfrak{p}$ of the Weierstrass equation for $\mathcal{E}_{\Delta}$. Furthermore, $\mathcal{O}_{\mathcal{S},\Delta}$ has perfect residue field $k(\Delta)$; hence, a straightforward application of Tate's algorithm shows that the Kodaira singularity type of $\mathcal{E}$ is generically constant over Δ. So in this case, the set of points $x \in \tilde{\Delta}$ which do not have the generic fiber type also satisfy the elimination principle, and we can assume that all fibers have the same Kodaira fiber type (call it K).

Consider now the irreducible components of $\tilde{\mathcal{E}}_{\tilde{\Delta}}$, and define $H(K)$ as the number of irreducible components over $\bar{F}$, and $h(K)$ as the number of irreducible components over $\bar{F}$ that are defined over F.

By Tate's algorithm, there exists an integer $H_{\min}(K, F') \in [1, H(K)]$, and a separable polynomial $P(T)$ defined over F, derived from the Weierstrass equation (10) and with $\deg(P(T)) \leqslant 3$, such that, if F' is its splitting field, then

$$h(K) = \begin{cases} H(K) & \text{if } F' = F, \\ H_{\min}(K, F') & \text{if } F' \neq F. \end{cases}$$

However, since we are considering the action of $\mathrm{Frob}_{\mathfrak{p}}$ on a subspace of $\mathrm{NS}(\tilde{\mathcal{E}}/\bar{\mathbb{F}}_{\mathfrak{p}})$, we must look at all components of $\tilde{\mathcal{E}}_{\tilde{\Delta}}$ that are irreducible over $\bar{\mathbb{F}}_{\mathfrak{p}}(\tilde{\Delta})$ (and not just over $\bar{F}$)! The Frobenius trace picks out from among these those that are defined over F. Denote the number of such components by $M(K)$. In particular, if F' is a constant field extension of F (i.e. $F' = L(\tilde{\Delta})$, where L is a finite extension of $\mathbb{F}_{\mathfrak{p}}$), then the $\bar{\mathbb{F}}_{\mathfrak{p}}(\tilde{\Delta})$-irreducible components are clearly not defined over F. Otherwise, F' is a geometric extension of F, and therefore all F-irreducible components are also irreducible over $\bar{\mathbb{F}}_{\mathfrak{p}}(\tilde{\Delta})$. Thus we have the following three cases.

$F' = F$. In this case $M(K) = H(K) = m_d$ for all $d \in \tilde{\Delta}$. Therefore,

$$\begin{aligned} \sum_{d \in \tilde{\Delta}(\mathbb{F}_{\mathfrak{p}})} (m_d - 1) &= \sum_{d \in \tilde{\Delta}(\mathbb{F}_{\mathfrak{p}})} (M - 1) \\ &= \#\tilde{\Delta}(\mathbb{F}_{\mathfrak{p}})(M - 1) \\ &= \#\tilde{\Delta}(\mathbb{F}_{\mathfrak{p}}) \operatorname{Trace}(\mathrm{Frob}_{\mathfrak{p}}|\tilde{\mathcal{F}}). \end{aligned} \tag{11}$$

This case always holds for fibers of type II, III, II^*, and III^*.

$F' = L(\tilde{\Delta})$. In this case $M(K) = H_{\min}(K, F') = m_d$ for all $d \in \tilde{\Delta}$, and $\sum_{d \in \tilde{\Delta}(\mathbb{F}_{\mathfrak{p}})}(m_d - 1) = \#\tilde{\Delta}(\mathbb{F}_{\mathfrak{p}}) \operatorname{Trace}(\mathrm{Frob}_{\mathfrak{p}}|\tilde{\mathcal{F}})$ as before.

$F' \neq L(\tilde{\Delta})$. Let $\mathcal{G} := \mathrm{Gal}(F'/F)$. Then $\mathcal{G}$ acts on the geometrically irreducible components of $\tilde{\mathcal{E}}_{\tilde{\Delta}}$, and $M(K)$ is the number of $\mathcal{G}$ orbits. Furthermore, every $d \in \tilde{\Delta}(\mathbb{F}_{\mathfrak{p}})$ determines a conjugacy class $C_d \subset \mathcal{G}$ such that the Frobenius action on the fiber $\tilde{\mathcal{E}}_d$ can be identified (up to conjugacy) with the action of some $\sigma_d \in C_d$ when restricted to $\tilde{\mathcal{E}}_d$. Under this identification, the number of

https://doi.org/10.1112/S0010437X03000381 Published online by Cambridge University Press

components m_d in $\tilde{\mathcal{E}}_d$ defined over $\mathbb{F}_\mathfrak{p}$ equals the number of components fixed by σ_d. Furthermore, since two elements of the same conjugacy class fix the same number of components, it makes sense to say $m_d = i(C_d)$, where $i(\sigma_d)$ is the number of components that remain fixed under the action of $\sigma_d \in C_d$, and $i(C_d) := i(\sigma_d)$. Therefore,

$$\begin{aligned}\sum_{d\in\tilde{\Delta}(\mathbb{F}_\mathfrak{p})} m_d &= \sum_{C\subset\mathcal{G}}\sum_{d:C_d=C} i(\sigma_d), \quad \text{where the first sum is over all conjugacy classes } C \text{ in } \mathcal{G}\\ &= \sum_C i(C)\#\{d:\sigma_d = C\},\\ &= \sum_C i(C)\frac{|C|}{|\mathcal{G}|}\#\tilde{\Delta}(\mathbb{F}_\mathfrak{p}) + O(\sqrt{q_\mathfrak{p}}), \quad \text{by the Chebotarev density theorem (see (13))}\\ &= \#\tilde{\Delta}(\mathbb{F}_\mathfrak{p})\frac{1}{|\mathcal{G}|}\sum_C i(C)|C| + O(\sqrt{q_\mathfrak{p}}),\\ &= \#\tilde{\Delta}(\mathbb{F}_\mathfrak{p})\frac{1}{|\mathcal{G}|}\sum_C\sum_{g\in C} i(g) + O(\sqrt{q_\mathfrak{p}}),\\ &= \#\tilde{\Delta}(\mathbb{F}_\mathfrak{p})\frac{1}{|\mathcal{G}|}\sum_{g\in\mathcal{G}} i(g) + O(\sqrt{q_\mathfrak{p}}),\\ &= \#\tilde{\Delta}(\mathbb{F}_\mathfrak{p})M + O(\sqrt{q_\mathfrak{p}}).\end{aligned}$$

Therefore,

$$\begin{aligned}\sum_{d\in\tilde{\Delta}(\mathbb{F}_\mathfrak{p})}(m_d - 1) &= \#\tilde{\Delta}(\mathbb{F}_\mathfrak{p})(M-1) + O(\sqrt{q_\mathfrak{p}})\\ &= \#\tilde{\Delta}(\mathbb{F}_\mathfrak{p})\,\mathrm{Trace}(\mathrm{Frob}_\mathfrak{p}|\tilde{\mathcal{F}}) + O(\sqrt{q_\mathfrak{p}}).\end{aligned}$$

To complete the proof of Theorem 4.1, we must show that

$$\#\tilde{\Delta}(\mathbb{F}_\mathfrak{p})\,\mathrm{Trace}(\mathrm{Frob}_\mathfrak{p}|\tilde{\mathcal{F}}) = q_\mathfrak{p}\,\mathrm{Trace}(\mathrm{Frob}_\mathfrak{p}|\tilde{\mathcal{F}}) + O(\sqrt{q}_\mathfrak{p}).$$

However, by Weil's estimate, we have

$$\#\tilde{\Delta}(\mathbb{F}_\mathfrak{p}) = 1 + a_\mathfrak{p}(\Delta) + q_\mathfrak{p},$$

where $|a_\mathfrak{p}(\Delta)| \leqslant \sqrt{q}_\mathfrak{p} g_\Delta$. Furthermore, for all but finitely many primes $\mathfrak{p}$, $\mathrm{Trace}(\mathrm{Frob}_\mathfrak{p}|\tilde{\mathcal{F}})$ is bounded by the number of geometrically irreducible components of $\pi^{-1}(\Delta)$, hence is bounded independently of $\mathfrak{p}$. ☐

In proving Theorem 4.1, we have used the following effective version of the geometric Chebotarev density theorem.

Theorem 4.2 [MS94]. *Suppose $X \to Y$ is a geometric covering of curves over $\mathbb{F}_\mathfrak{p}$ (i.e. Y is defined over $\mathbb{F}_\mathfrak{p}$, and $\mathbb{F}_\mathfrak{p}$ is the algebraic closure of itself in $\mathbb{F}_\mathfrak{p}(X)$). Let C be a conjugacy class in $G := \mathrm{Gal}(X/Y)$, and for $y \in Y$ unramified, let C_y be its Frobenius conjugacy class. Define*

$$\begin{aligned}\psi_C &= \#\{y\in Y \mid y \text{ unramified}, C_y = C\},\\ \psi &= \#\{y\in Y \mid y \text{ unramified}\},\\ D &= \text{the set of ramified points in } \bar{Y} := Y\times_{\mathbb{F}_\mathfrak{p}}\bar{\mathbb{F}}_\mathfrak{p}.\end{aligned}$$

Then, if we let $|S|$ denote the size of a set S, we have

$$\left|\psi_C - \frac{|C|}{|G|}\psi\right| \leqslant 2g_X\frac{|C|}{|G|}\sqrt{q}_\mathfrak{p} + |D|. \tag{12}$$

To apply this version of Chebotarev, we note that in our case, X is the curve defined by the polynomial $P(T)$ (hence can be considered the reduction mod $\mathfrak{p}$ of a curve defined over k), and $Y = \tilde{\Delta}$. Observing also that $\psi = \#\tilde{\Delta}(\mathbb{F}_\mathfrak{p}) - |D|$, gives

$$\psi_C = \frac{|C|}{|G|}\#\tilde{\Delta}(\mathbb{F}_\mathfrak{p}) + O(\sqrt{q}_\mathfrak{p}), \tag{13}$$

where the constant implicit in the big-O notation depends only on $|G|$, g_X, and $|\tilde{\Delta}|$. Since the set of ramification points on $\tilde{\Delta}$ satisfies the elimination principle, this is bounded independent of $\mathfrak{p}$.

5. *L*-series

We now have all the information necessary to prove Theorem 1.1. What remains is to run it through the L-series machinery, and apply Tate's conjecture. We briefly recall the relevant definitions below.

For a smooth variety $\mathcal{V}/k$, the Hasse–Weil L-series attached to $H^2_{\text{ét}}(\mathcal{V}/\bar{k})$, denoted $L_2(\mathcal{V}, s)$, is given by

$$L_2(\mathcal{V}, s) := \prod_{\mathfrak{p}} \det(1 - \mathrm{Frob}_\mathfrak{p}\, q_\mathfrak{p}^{-s} | H^2_{\text{ét}}(\mathcal{V}/\bar{k}; \mathbb{Q}_l))^{-1}.$$

If V is a finite-dimensional $\mathbb{Q}$-vector space, with an action of $G := \mathrm{Gal}(\bar{k}/k)$, then V defines a Galois representation of G, and the Artin L-series attached to V is

$$L(V, s) := \prod_{\mathfrak{p}} \det(1 - \mathrm{Frob}_\mathfrak{p}\, q_\mathfrak{p}^{-s} | V^G)^{-1}.$$

Remark 5.1. To be precise, since in this paper we are working over all primes $\mathfrak{p} \subset O_R$,

$$L_2(\mathcal{E}, s) \approx \prod_{\mathfrak{p} \in O_R} \det(1 - \mathrm{Frob}_\mathfrak{p}\, q_\mathfrak{p}^{-s} | H^2_{\text{ét}}(\mathcal{E}/\bar{k}; \mathbb{Q}_l))^{-1},$$

and similarly for $L_2(\mathcal{S}, s)$ and $L(\mathcal{F}, s)$. The symbol $\approx$ is used to indicate that the two sides agree up to finitely many Euler factors; this, however, has no effect on the residue computation.

Conjecture 5.1 (Tate's conjecture [Tat65, Conjecture 2]). *Let $\mathcal{V}$ be a smooth projective variety defined over k, and let $L_2(\mathcal{V}, s)$ be the Hasse–Weil L-function attached to $H^2_{\text{ét}}(\mathcal{V}/\bar{k}; \mathbb{Q}_l)$. Then $L_2(\mathcal{V}, s)$ has a meromorphic continuation to $\mathbb{C}$, and has a pole at $s = 2$ of order*

$$-\operatorname*{ord}_{s=2} L_2(\mathcal{V}, s) = \operatorname{rank} \mathrm{NS}(\mathcal{E}/k).$$

Finally, we are ready to prove the main theorem.

Proof of Theorem 1.1. We begin by counting the number of $\mathbb{F}_\mathfrak{p}$-rational points on $\tilde{\mathcal{E}}$. First, view $\tilde{\mathcal{E}}$ as a fibration of curves, and use the Lefschetz fixed-point theorem to count points fiber by fiber:

$$\begin{aligned}
\#\tilde{\mathcal{E}}(\mathbb{F}_\mathfrak{p}) &= \sum_{x \in \tilde{\mathcal{S}}(\mathbb{F}_\mathfrak{p})} \#\tilde{\mathcal{E}}_x(\mathbb{F}_\mathfrak{p}) \\
&= \sum_{x \in \tilde{\mathcal{S}}(\mathbb{F}_\mathfrak{p})} (1 - a_\mathfrak{p}(\tilde{\mathcal{E}}_x) + q_\mathfrak{p} + (m_x - 1)q_\mathfrak{p}) \\
&= (1 + q_\mathfrak{p})\#\tilde{\mathcal{S}}(\mathbb{F}_\mathfrak{p}) - q_\mathfrak{p}^2 A_\mathfrak{p}(\mathcal{E}) + \sum_{x \in \tilde{\Delta}(\mathbb{F}_\mathfrak{p})} (m_x - 1)q_\mathfrak{p} \\
&= (1 + q_\mathfrak{p})\#\tilde{\mathcal{S}}(\mathbb{F}_\mathfrak{p}) - q_\mathfrak{p}^2 A_\mathfrak{p}(\mathcal{E}) + q_\mathfrak{p}\, \mathrm{Trace}(\mathrm{Frob}_\mathfrak{p} | \tilde{\mathcal{F}}) q_\mathfrak{p} + O(\sqrt{q_\mathfrak{p}^3}) \quad \text{by Theorem 4.1.}
\end{aligned} \tag{14}$$

Since $\#\tilde{\mathcal{S}}(\mathbb{F}_\mathfrak{p})$ is given by

$$\#\tilde{\mathcal{S}}(\mathbb{F}_\mathfrak{p}) = 1 - a_\mathfrak{p}(\tilde{\mathcal{S}}) + b_\mathfrak{p}(\tilde{\mathcal{S}}) - q_\mathfrak{p} a_\mathfrak{p}(\tilde{\mathcal{S}}) + q_\mathfrak{p}^2, \tag{15}$$

https://doi.org/10.1112/S0010437X03000381 Published online by Cambridge University Press

we obtain the following expression for $\#\tilde{\mathcal{E}}(\mathbb{F}_{\mathfrak{p}})$:

$$\begin{aligned}\#\tilde{\mathcal{E}}(\mathbb{F}_{\mathfrak{p}}) = 1 + q_{\mathfrak{p}} + q_{\mathfrak{p}}^2 + q_{\mathfrak{p}}^3 - a_{\mathfrak{p}}(\tilde{\mathcal{S}}) - 2q_{\mathfrak{p}}a_{\mathfrak{p}}(\tilde{\mathcal{S}}) - q_{\mathfrak{p}}^2 a_{\mathfrak{p}}(\tilde{\mathcal{S}}) + b_{\mathfrak{p}}(\tilde{\mathcal{S}}) + q_{\mathfrak{p}}b_{\mathfrak{p}}(\tilde{\mathcal{S}})\\ - q_{\mathfrak{p}}^2 A_{\mathfrak{p}}(\mathcal{E}) + q_{\mathfrak{p}} \operatorname{Trace}(\operatorname{Frob}_{\mathfrak{p}}|\tilde{\mathcal{F}})q_{\mathfrak{p}} + O(\sqrt{q_{\mathfrak{p}}^3}).\end{aligned} \tag{16}$$

Note that, for any smooth, n-dimensional variety $\mathcal{V}/k$,

$$\operatorname{Trace}(\operatorname{Frob}_{\mathfrak{p}}|H^{2n-i}_{\text{ét}}(\mathcal{V},\mathbb{Q}_l)) = q_{\mathfrak{p}}^{n-i}\operatorname{Trace}(\operatorname{Frob}_{\mathfrak{p}}|H^{i}_{\text{ét}}(\mathcal{V},\mathbb{Q}_l))$$

is given by Poincaré duality.

Next, we view $\mathcal{E}$ as a threefold to obtain

$$\begin{aligned}\#\tilde{\mathcal{E}}(\mathbb{F}_{\mathfrak{p}}) &= 1 - a_{\mathfrak{p}}(\tilde{\mathcal{E}}) + b_{\mathfrak{p}}(\tilde{\mathcal{E}}) - c_{\mathfrak{p}}(\tilde{\mathcal{E}}) + q_{\mathfrak{p}}b_{\mathfrak{p}}(\tilde{\mathcal{E}}) - q_{\mathfrak{p}}^2 a_{\mathfrak{p}}(\tilde{\mathcal{E}}) + q_{\mathfrak{p}}^3\\ &= 1 - a_{\mathfrak{p}}(\tilde{\mathcal{S}}) + b_{\mathfrak{p}}(\tilde{\mathcal{E}}) - c_{\mathfrak{p}}(\tilde{\mathcal{E}}) + q_{\mathfrak{p}}b_{\mathfrak{p}}(\tilde{\mathcal{E}}) - q_{\mathfrak{p}}^2 a_{\mathfrak{p}}(\tilde{\mathcal{S}}) + q_{\mathfrak{p}}^3 \quad \text{by Corollary 3.1.}\end{aligned} \tag{17}$$

Finally, equating the two expressions for the number of rational points on $\tilde{\mathcal{E}}$ in Equations (17) and (16) gives an expression for $A_{\mathfrak{p}}(\mathcal{E})$:

$$\begin{aligned}q_{\mathfrak{p}}^2 A_{\mathfrak{p}}(\mathcal{E}) = q_{\mathfrak{p}} - 2q_{\mathfrak{p}}a_{\mathfrak{p}}(\tilde{\mathcal{S}}) + b_{\mathfrak{p}}(\tilde{\mathcal{S}}) + q_{\mathfrak{p}}b_{\mathfrak{p}}(\tilde{\mathcal{S}}) + c_{\mathfrak{p}}(\tilde{\mathcal{E}}) - b_{\mathfrak{p}}(\tilde{\mathcal{E}}) - q_{\mathfrak{p}}b_{\mathfrak{p}}(\tilde{\mathcal{E}})\\ + q_{\mathfrak{p}}^2 + q_{\mathfrak{p}} \operatorname{Trace}(\operatorname{Frob}_{\mathfrak{p}}|\tilde{\mathcal{F}})q_{\mathfrak{p}} + O(\sqrt{q_{\mathfrak{p}}^3}).\end{aligned} \tag{18}$$

By Deligne's theorem [Del74], we know, for every smooth projective variety $\mathcal{V}$ defined over k, that

$$|\operatorname{Trace}(\operatorname{Frob}_{\mathfrak{p}}|H^{i}_{\text{ét}}(\mathcal{V},\mathbb{Q}_l))| \leqslant B_i(\mathcal{V})q_{\mathfrak{p}}^{i/2},$$

where $B_i(\mathcal{V}) := \dim H^{i}_{\text{ét}}(\mathcal{V}/\bar{k},\mathbb{Q}_l)$ is independent of $\mathfrak{p}$. Thus, we can group all terms of order $\sqrt{q_{\mathfrak{p}}^3}$ or less together, and obtain

$$q_{\mathfrak{p}}^2 A_{\mathfrak{p}}(\mathcal{E}) = q_{\mathfrak{p}}^2 + q_{\mathfrak{p}}b_{\mathfrak{p}}(\tilde{\mathcal{S}}) - q_{\mathfrak{p}}b_{\mathfrak{p}}(\tilde{\mathcal{E}}) + \operatorname{Trace}(\operatorname{Frob}_{\mathfrak{p}}|\tilde{\mathcal{F}})q_{\mathfrak{p}}^2 + O(\sqrt{q_{\mathfrak{p}}^3}). \tag{19}$$

It now only remains to compute residues. For $\operatorname{Re}(s) > \frac{1}{2}$,

$$\begin{aligned}\frac{d}{ds}\log L(\mathcal{F},s) &= \frac{d}{ds}\sum_{\mathfrak{p}} -\log\det(1 - \operatorname{Frob}_{\mathfrak{p}} q_{\mathfrak{p}}^{-s}|\mathcal{F})\\ &= \sum_{\mathfrak{p}} -\operatorname{Trace}(\operatorname{Frob}_{\mathfrak{p}}|\mathcal{F})\frac{\log q_{\mathfrak{p}}}{q_{\mathfrak{p}}^s} + O(1).\end{aligned}$$

Therefore,

$$\begin{aligned}\operatorname*{res}_{s=1}\sum_{\mathfrak{p}}\operatorname{Trace}(\operatorname{Frob}_{\mathfrak{p}}|\tilde{\mathcal{F}})\frac{\log q_{\mathfrak{p}}}{q_{\mathfrak{p}}^s} &= -\operatorname*{res}_{s=1}\frac{d}{ds}\log L(\mathcal{F},s)\\ &= -\operatorname*{ord}_{s=1} L(\mathcal{F},s)\\ &= \operatorname{rank}(\mathcal{F}^{\operatorname{Gal}(\bar{k}/k)}),\end{aligned} \tag{20}$$

where this last equality follows from [RS98, Proposition 1.5.1].

Furthermore, for $\operatorname{Re}(s) > \frac{3}{2}$,

$$\begin{aligned}\frac{d}{ds}\log L_2(\mathcal{E},s) &= \frac{d}{ds}\sum_{\mathfrak{p}} -\log\det(1 - \operatorname{Frob}_{\mathfrak{p}} q_{\mathfrak{p}}^{-s}|H^2_{\text{ét}}(\mathcal{E}/\bar{k},\mathbb{Q}_l))\\ &= \sum_{\mathfrak{p}} -b_{\mathfrak{p}}(\mathcal{E})\frac{\log q_{\mathfrak{p}}}{q_{\mathfrak{p}}^s} + O(1).\end{aligned}$$

Therefore,

$$\begin{aligned}\operatorname*{res}_{s=2}\sum_{\mathfrak{p}} b_{\mathfrak{p}}(\mathcal{E})\frac{\log q_{\mathfrak{p}}}{q_{\mathfrak{p}}^s} &= -\operatorname*{res}_{s=1}\frac{d}{ds}\log L_2(\mathcal{E},s)\\ &= -\operatorname*{ord}_{s=2} L_2(\mathcal{E},s)\\ &= \operatorname{rank}\operatorname{NS}(\mathcal{E}/k)\quad \text{by Tate's conjecture,}\end{aligned}\tag{21}$$

and similarly

$$\begin{aligned}\operatorname*{res}_{s=2}\sum_{\mathfrak{p}} b_{\mathfrak{p}}(\mathcal{S})\frac{\log q_{\mathfrak{p}}}{q_{\mathfrak{p}}^s} &= -\operatorname*{ord}_{s=2} L_2(\mathcal{S},s)\\ &= \operatorname{rank}\operatorname{NS}(\mathcal{S}/k)\quad \text{by Tate's conjecture.}\end{aligned}\tag{22}$$

Combining the residue calculations with Equation (19), we have

$$\operatorname*{res}_{s=1}\sum_{\mathfrak{p}} -A_{\mathfrak{p}}(\mathcal{E})\frac{\log q_{\mathfrak{p}}}{q_{\mathfrak{p}}^s} = -1-\operatorname{rank}(\mathcal{F}^{\operatorname{Gal}(\bar{k}/k)}) - \operatorname{rank}\operatorname{NS}(\mathcal{S}/k)+\operatorname{rank}\operatorname{NS}(\mathcal{E}/k)$$

and the theorem follows by the Shioda–Tate formula for elliptic threefolds (Corollary 3.2). □

Acknowledgements

The results in this article formed the bulk of the author's PhD Thesis [Waz01], and the author would like to thank her advisor, Professor Joseph Silverman, for many illuminating discussions on the arithmetic of elliptic fibrations. She is indebted to Professor Siman Wong, for answering many questions, and raising many more. She is also grateful to Professors Michael Rosen and Stephen Lichtenbaum for their advice and suggestions.

References

Del74 P. Deligne, *La conjecture de Weil I*, Publ. Math. IHES **43** (1974), 273–307.

Ful80 W. Fulton, *Intersection theory*, Ergebnisse der Mathematik und Ihrer Grenzgebiete, vol. 3 (Springer, Berlin, 1980).

GD66 A. Grothendieck and J. Dieudonné, *Éléments de géométrie algébrique*, Publ. Math. IHES **28** (1966).

Lan83 S. Lang, *Fundamentals of diophantine geometry* (Springer, Berlin, 1983).

Mil80 J. S. Milne, *Etale cohomology* (Princeton University Press, Princeton, NJ, 1980).

MS94 K. Murty and J. Scherk, *Effective versions of the Chebotarev density theorem for function fields*, Comptes Rendus des Seances de l'Academie des Sciences, Serie I, Mathematique **319** (1994), 523–528.

Mum70 D. Mumford, *Abelian varieties*, Tata Institute of Fundamental Research Studies in Mathematics, vol. 5 (Oxford University Press, 1970).

Mum82 D. Mumford, *Geometric invariant theory*, second edition, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 34 (Springer, Berlin, 1982).

Nag97 K. Nagao, $\mathbb{Q}(t)$*-rank of elliptic curves and certain limits coming from the local points*, Manuscripta Math. **92** (1997), 13–32.

RS98 M. Rosen and J. Silverman, *On the rank of an elliptic surface*, Invent. Math. **133** (1998), 43–67.

Shi72 T. Shioda, *On elliptic modular surfaces*, J. Math. Soc. Japan **24** (1972), 20–59.

Shi99 T. Shioda, *Mordell–Weil lattices for higher genus fibration over a curve*, in *New trends in algebraic geometry (Warwick, 1996)*, London Mathematical Society Lecture Note Series, vol. 264 (Cambridge University Press, Cambridge, 1999), 359–373.

Sil94 J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151 (Springer, Berlin, 1994).

Tat65 J. Tate, *Algebraic cycles and poles of zeta functions*, in *Arithmetical Algebraic Geometry* (Harper and Row, New York, 1965), 93–110.

Tat75 J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in *Modular functions of one variable IV*, Lecture Notes in Mathematics, vol. 476 (Springer, Berlin, 1975).

Waz01 R. Wazir, *Arithmetic on elliptic threefolds*, PhD thesis, Brown University, May 2001.

Rania Wazir wazir@dm.unito.it
Dipartimento di Matematica, Università degli Studi di Torino, Via Carlo Alberto, 10, 10129 Torino, Italy