On the Mordell-Weil groups of elliptic surfaces associated with Frey curves of degree two

Hayato Yagi

January 23, 2025

Abstract

We study a family of elliptic curves $y^2 = x(x - a^2)(x + b^2)$, where (a, b, c) are Pythagorean triples. This is the family of the Frey curves of degree 2. We can one-parameterize Pythagorean triples by rational numbers and consider the family as an elliptic curve over a function field.

$$E_{1,s} : y^2 = x(x - 4s^2)(x + (s^2 - 1)^2)$$

It is known that the generic rank of the Mordell-Weil group of $E_{1,s}$ over $\overline{\mathbb{Q}}(s)$ is 0. We found an infinite subfamily of $E_{1,s}$ whose Mordell-Weil rank over $\overline{\mathbb{Q}}(s)$ is 1, which means that there are infinitely many $s \in \overline{\mathbb{Q}}$ such that the Mordell-Weil group of $E_{1,s}$ has positive rank over $\overline{\mathbb{Q}}$.

We use the theory of elliptic surfaces to prove it. Each elliptic curve over a function field corresponds to an elliptic surface. The Shioda-Tate formula gives the relation between the Mordell-Weil rank and the Néron-Severi rank of elliptic surfaces. We compute the types of special fibers of the elliptic surfaces and consider an upper bound of the rank of the Néron-Severi group.

It is relatively easy to prove that the generic rank of the subfamily is less than 2. In order to prove that the generic rank is exactly 1, we calculate the characteristic polynomial of the action of the Frobenius automorphism on the second l-adic étale cohomology group to get the sharp upper bound of the rank of the Néron-Severi group.

1 Introduction

Let a, b, c be positive integers which satisfy the Fermat's equation

$$a^n + b^n = c^n.$$

for any integer $n \geq 3$ and consider the elliptic curve defined by the Weierstrass equation

$$y^2 = x(x - a^n)(x + b^n),$$

which is called the Frey curve. The Frey curve took an important role in the proof of Fermat's Last Theorem by Wiles. Wiles proved that the Frey curve cannot exist, which implies that the Fermat's equation has no nontrivial solution.

In this paper, we consider elliptic curves in the form of the Frey curves for $n = 2$. In other words, let (a, b, c) be a Pythagorean triple, i.e., $a^2 + b^2 = c^2$, and consider the elliptic curve defined by the Weierstrass equation

$$y^2 = x(x - a^2)(x + b^2),$$

which we call the Frey curve of degree 2. The Frey curves of degree 2 do exist infinitely unlike for $n \geq 3$.

For an elliptic curve E defined over a field K, the Mordell-Weil group $E(K)$ is a group consisting of all K-rational points on E. The Mordell-Weil group is an important object in the study of elliptic curves.

Theorem 1.1. (Mordell's Theorem) Let E be an elliptic curve defined over a number field K. Then the Mordell-Weil group $E(K)$ is a finitely generated abelian group.

By the structure theorem of finite abelian groups, the Mordell-Weil group can be decomposed into a free part and a torsion part:

$$E(K) \cong \mathbb{Z}^{\oplus r} \oplus E(K)_{\text{tors}}$$

where r is the rank of the Mordell-Weil group and $E(K)_{\text{tors}}$ is the torsion subgroup of $E(K)$.

We can one-parameterize Pythagorean triples by rational numbers and then the Frey curves of degree 2 are isomorphic to

$$E_{1,s} : y^2 = x(x - 4s^2)(x + (s^2 - 1)^2) \tag{1.1}$$

for some $s \in \mathbb{Q}$. We consider $E_{1,s}$ as an elliptic curve over a function field $\overline{\mathbb{Q}}(s)$.

For any elliptic curves E over a function field $k(C)$ of a smooth irreducible projective curve C over an algebraically closed field k, there is an elliptic surface $\pi : \mathcal{E} \to C$ with the generic fiber E called the Néron model, and we can use some theorems in the theory of surfaces. The elliptic surface $E/k(C)$ is called the generic fiber of the elliptic surface $\mathcal{E} \to C$. For $s \in \overline{\mathbb{Q}}$, $\mathcal{E}_t := \pi^{-1}(s)$ is called the special fiber at s. For all but finitely many $s \in \overline{\mathbb{Q}}$, the special fiber at s is non-singular, which means that is an elliptic curve.

The Mordell's Theorem also holds for elliptic curves over a function field.

Theorem 1.2. ([1, Theorem 6.1.]) Let $\mathcal{E} \to C$ be an elliptic surface defined over a field k and E be the corresponding elliptic curve over the function field $k(C)$. If $\mathcal{E} \to C$ does not split, then the Mordell-Weil group $E(k(C))$ is a finitely generated abelian group.

On the relation between the Mordell-Weil group of an elliptic curve over a function field and its special fibers, the following theorem is known.

Theorem 1.3. (Specialization Theorem, [1, Theorem 11.4.]) Let $\mathcal{E} \to C$ be a non-split elliptic surface defined over a number field k and E be the corresponding elliptic curve over the function field $k(C)$. Let $k' = k$ or $\overline{k}$. Then for all but finitely many $s \in C(k')$, a homomorphism

$$E(k(C)) \hookrightarrow \mathcal{E}_s(k'),$$

called the specialization homomorphism at s, is injective.

2 Main theorem

First, we determine the Mordell-Weil group of $E_{1,s}$ defined by (1.1).

Theorem 2.1. The Mordell-Weil group of $E_{1,s}$ over $\overline{\mathbb{Q}}(s)$ satisfies

$$E_{1,s}(\overline{\mathbb{Q}}(s)) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z},$$

especially the rank is 0. The torsion subgroup is generated by

$$\begin{aligned} T_1 &:= (2s(s+1)^2, 2s(s+1)^2(s^2+1)), \\ T_2 &:= (2\sqrt{-1}s(s^2-1), 2\sqrt{-1}s(s+\sqrt{-1})^2(s^2-1)). \end{aligned}$$

Corollary 2.2.

$$E_{1,s}(\mathbb{Q}(s)) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$$

is generated by T_1 and $2T_2 = (0, 0)$.

By Corollary 2.2 and the specialization theorem (Theorem 1.3), we have

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \hookrightarrow E_{1,s_0}(\mathbb{Q}) \tag{2.1}$$

for all but finitely many $s_0 \in \mathbb{Q}$. Actually, we can prove that the image of the specialization homomorphism is $E_{1,s_0}(\mathbb{Q})_{\mathrm{tors}}$ for all $s_0 \in \mathbb{Q}$ unless E_{1,s_0} is singular.

Theorem 2.3. For any $s_0 \in \mathbb{Q}\setminus\{0, \pm 1\}$, E_{1,s_0} is non-singular and the torsion subgroup satisfies

$$E_{1,s_0}(\mathbb{Q})_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

Inspite of the fact that the generic rank of $E_{1,s}$ is 0, Yoshida ([2, Corollary 4.7.]) showed that there are infinitely many $s \in \mathbb{Q}$ such that the Mordell-Weil group of $E_{1,s}$ has positive rank over $\mathbb{Q}$. However, the infinite family is not explicitly parameterized. We find the subset of $s \in \overline{\mathbb{Q}}$ with the positive rank of the Mordell-Weil group of $E_{1,s}$ parameterized by an rational function of one variable $t \in \overline{\mathbb{Q}}$. In order to prove it, by the specialization theorem (Theorem 1.3), it is enough to find a subfamily of $E_{1,s}$ whose generic rank is 1.

By substituting $s = \frac{2t}{t^2-3}$ into $E_{1,s}$, we get a new family of elliptic curves

$$E_{2,t} : y^2 = x\left(x - 4\left(\frac{2t}{t^2-3}\right)^2\right)\left(x + \left(\left(\frac{2t}{t^2-3}\right)^2 - 1\right)^2\right),$$

which is a subfamily of $E_{1,s}$.

The following is our main result.

Theorem 2.4. The Mordell-Weil group of $E_{2,t}$ over $\overline{\mathbb{Q}}(t)$ satisfies

$$E_{2,t}(\overline{\mathbb{Q}}(t)) \cong \mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z},$$

especially the rank is 1. We denote $s = \frac{2t}{t^2-3}$. The torsion subgroup is generated by T_1 and T_2 in Theorem 2.1 and the free part is generated by

$$\left(s^2 - 1, \sqrt{-1}s(s^2-1)\frac{t^2+3}{t^2-3}\right).$$

The important point is that we prove that the generic rank of $E_{2,t}$ is exactly 1, not only the existence of a point of infinite order. Our proof is based on the method of Naskręcki in [3].

3 Preliminaries

In order to get the lower bound of the rank of the Mordell-Weil group, finding points of infinite order is enough. It is quite difficult to get a good upper bound of the rank. The following theorem behaves a key role in the proof of the main theorem.

Theorem 3.1. (Shioda-Tate formula, [4, Corollary 5.3]) Let $R \subset C$ be the set of points where the special fiber of $\mathcal{E}$ is singular. For each $v \in R$, let m_v be the number of components of the special fiber of $\mathcal{E}$ at v. Let $\rho(\mathcal{E})$ denote the rank of the Néron-Severi group of $\mathcal{E}$. Then, we have

$$\rho(\mathcal{E}) = 2 + \sum_{v \in R}(m_v - 1) + \mathrm{rank}(E(k(C))).$$

We can calculate R and m_v by Tate's algorithm, but it is still difficult to determine $\rho(\mathcal{E})$. We have the following theorem to get an upper bound of $\rho(\mathcal{E})$.

Theorem 3.2.

$$\rho(\mathcal{E}) \leq \frac{5}{6} e(\tilde{S}),$$
$$e(\tilde{S}) := \sum_{v \in R} e(F_v).$$

where $e(\tilde{S})$ is the Euler number, $e(F_v)$ is the local Euler number of the special fiber of $\mathcal{E}$ at v for each $v \in R$ and

$$e(F_v) = \begin{cases} m_v & \text{if the fiber has multiplicative reduction,} \\ m_v + 1 & \text{if the fiber has additive reduction.} \end{cases}$$

Proof. TODO: Naskrencki の PhD の 2.2.19(ii), 2.2.9, 2.2.10 （やその引用元）を引用するオイラー数については [5, pp. 136-137 付録 2], [6, p.14 Table II] □

For the torsion subgroup of the Mordell-Weil group, we have the following theorem.

Theorem 3.3. ([3, Lem.3.5])

$$E(\overline{\mathbb{Q}}(s))_{\mathrm{tors}} \hookrightarrow \prod_{v \in R} G(F_v)$$

where $G(F_v)$ is the group generated by all simple components of the fiber at v. If F_v is of type I_n in Kodaira's symbol, then $G(F_v) \cong \mathbb{Z}/n\mathbb{Z}$.

Proof. TODO □

4 Proof of Theorem 2.1 and Theorem 2.3

Theorem 4.1. ([1, Exercise 3.9.]) j-invariant が const でなければ non-split

Proof of Theorem 2.1. Let $\mathcal{E}_{1,s} \to \mathbb{P}^1$ be the elliptic surface with the generic fiber $E_{1,s}$. The discriminant of $E_{1,s}$ is

$$\Delta_{E_{1,s}} = 256s^4(s+1)^4(s-1)^4(s^2+1)^4, \tag{4.1}$$

and by Tate's algorithm, we have the following table.

Table 1: Singular fibers of $E_{1,s}$

Place	Type	m_v
$s=0$	I_4	4
$s=\pm 1$	I_4	4
$s=\pm\sqrt{-1}$	I_4	4
$s=\infty$	I_4	4

Then $e(\mathcal{E}_{1,s}) = 24$ and by Theorem 3.2, we have $\rho(\mathcal{E}_{1,s}) \leq 20$. By Shioda-Tate formula (Theorem 3.1), we have

$$\mathrm{rank}(E_{1,s}) = 0$$

As for the torsion subgroup, we have

$$E_{1,s}(\overline{\mathbb{Q}}(s))[2] = \{\mathcal{O}, (0,0), (4s^2,0), (-(s^2-1)^2,0)\},$$

and we can check by calculation that

$$2T_1 = (4s^2, 0), \tag{4.2}$$
$$2T_2 = (0,0). \tag{4.3}$$

By Theorem 3.3, we have $E_{1,s}(\overline{\mathbb{Q}}(s))_{\mathrm{tors}} \hookrightarrow (\mathbb{Z}/4\mathbb{Z})^6$. Therefore, we have

$$E_{1,s}(\overline{\mathbb{Q}}(s))_{\mathrm{tors}} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

□

Theorem 4.2. (Mazur's Theorem) Let E be an elliptic curve defined over $\mathbb{Q}$. Then the torsion subgroup $E(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to one of the following groups.

(1) $\mathbb{Z}/n\mathbb{Z}$ $\quad (1 \leq n \leq 10 \text{ or } n = 12)$,
(2) $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ $\quad (1 \leq n \leq 4)$.

Proof of Theorem 2.3. The non-singularity of the special fibers of $\mathcal{E}_{1,s}$ at $s \in \mathbb{Q}\backslash\{0, \pm 1\}$ follows from the equation (4.1). By the equation (2.1) and Mazur's Theorem (Theorem 4.2), the only possibility of $E_{1,s_0}(\mathbb{Q})_{\mathrm{tors}}$ is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. For a point $P = (x, y) \in E_{1,s_0}(\mathbb{Q})$, we can calculate the x-coordinate of $2P$ as

$$x(2P) = \frac{16s^4(s^2-1)^4 + 8s^2(s^2-1)^2x^2 + x^4}{4x(x-4s^2)(x+(s^2-1)^2)}.$$

Assume that there is a rational point of order 8, then there is a point $P = (x, y) \in E_{1,s_0}(\mathbb{Q})$ such that $2P = T_1 = (2s(s+1)^2, 2s(s+1)^2(s^2+1))$. Then we have

$$\frac{16s^4(s^2-1)^4 + 8s^2(s^2-1)^2x^2 + x^4}{4x(x-4s^2)(x+(s^2-1)^2)} = 2s(s+1)^2.$$

Put $x' = x - 2s(s+1)^2$, then we have

$$\begin{aligned} x'^4 &= 8s(s^2+1)(s+1)^4(x' + 2s(s^2+1))^2, \\ x'^2 &= \pm\sqrt{8s(s^2+1)}(s+1)^2(x' + 2s(s^2+1)). \end{aligned}$$

Since $x', s \in \mathbb{Q}$, we have $\sqrt{8s(s^2+1)} \in \mathbb{Q}$. Then $(2s, \sqrt{8s(s^2+1)})$ is a rational point on the elliptic curve $y^2 = x^3 + 4x$. However, we know that the Mordell-Weil group of $y^2 = x^3 + 4x$ over $\mathbb{Q}$ is

$$\{\mathcal{O}, (0,0), (2, \pm 4)\}.$$

This contradicts the assumption that $s \in \mathbb{Q} \setminus \{0, \pm 1\}$. □

5 The Generic Rank of $E_{2,t}$

In order to prove Theorem 2.4, Theorem 3.2 is not enough to get the sharp upper bound of the ranks of the Néron-Severi group. Actually, the discriminant of $E_{2,t}$ is

$$\Delta_{E_{2,t}} = 4096t^4(t-1)^4(t+1)^4(t-3)^4(t+3)^4(t^2-3)^4(t^4-2t^2+9)^4,$$

and the types of the singular fibers of $E_{2,t}$ are calculated as in Table 2 below by Tate's algorithm. Then in a similar way to the proof of Theorem 2.1, we get $\operatorname{rank} E_{2,t}(\overline{\mathbb{Q}}(t)) \leq 2$. On the other hand, we have only one point of infinite order in $E_{2,t}(\overline{\mathbb{Q}}(t))$.

Lemma 5.1.

$$E_{2,t}(\overline{\mathbb{Q}}(t))_{\mathrm{tors}} \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

Table 2: Singular fibers of $E_{2,t}$

Place	Type	m_v
$t=0$	I_4	4
$t=\pm 1$	I_4	4
$t=\pm 3$	I_4	4
$t=\pm\sqrt{3}$	I_4	4
$t^4-2t^2+9=0$	I_4	4
$t=\infty$	I_4	4

Proof. By Theorem 3.3, we have

$$E_{2,t}(\overline{\mathbb{Q}}(t))_{\text{tors}} \hookrightarrow (\mathbb{Z}/4\mathbb{Z})^{12}.$$

Obviously, we have

$$E_{1,s}(\overline{\mathbb{Q}}(s))_{\text{tors}} \subset E_{2,t}(\overline{\mathbb{Q}}(t))_{\text{tors}}.$$

□

Lemma 5.2.

$$\operatorname{rank} E_{2,t}(\overline{\mathbb{Q}}(t)) \geq 1$$

Proof.

$$\left(s^2-1, \sqrt{-1}s(s^2-1)\frac{t^2+3}{t^2-3}\right) \in E_{2,t}(\overline{\mathbb{Q}}(t)) \setminus E_{2,t}(\overline{\mathbb{Q}}(t))_{\text{tors}}.$$

□

Now, our goal is to show the rank of $E_{2,t}(\overline{\mathbb{Q}}(t))$ is not greater than 1.

We use another method to estimate an upper bound of the rank of Néron-Severi group, which we will explain in Section 6. Beforehand, we express the rank of $E_{2,t}(\overline{\mathbb{Q}}(t))$ in terms of ranks of elliptic curves with lower order coefficients in the Weierstrass equations to make the later computation feasible.

Definition 5.3. Let C be a smooth curve over an algebraically closed field k. Let E be an elliptic curve over a function field $k(C)$ given by the Weierstrass equation

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6$$

where $a_2, a_4, a_6 \in k(C)$. For a fixed $u \in k(C)^*$, we denote

$$E^{(u)} : uy^2 = x^3 + a_2x^2 + a_4x + a_6$$

to be the quadratic twist of E by u.

Theorem 5.4. ([7, Exercise 10.16]) Let E be an elliptic curve over a function field $k(C)$ and $u \in k(C)^*$. Then, the following equation holds

$$\operatorname{rank} E(k(C)(\sqrt{u})) = \operatorname{rank} E(k(C)) + \operatorname{rank} E^{(u)}(k(C)).$$

Theorem 5.5. Let

$$E_{0,u} : y^2 = x(x-4u)(x+(u-1)^2)$$

be an elliptic curve over $\overline{\mathbb{Q}}(u)$. Then, we have

$$\operatorname{rank} E_{2,t}(\overline{\mathbb{Q}}(t)) = \operatorname{rank} E_{1,s}(\overline{\mathbb{Q}}(s)) + \operatorname{rank} E_{1,s}^{(1+3s^2)}(\overline{\mathbb{Q}}(s)), \tag{5.1}$$

$$\operatorname{rank} E_{1,s}^{(1+3s^2)}(\overline{\mathbb{Q}}(s)) = \operatorname{rank} E_{0,u}^{(1+3u)}(\overline{\mathbb{Q}}(u)) + \operatorname{rank} E_{0,u}^{(u(1+3u))}(\overline{\mathbb{Q}}(u)). \tag{5.2}$$

Therefore, we have

$$\operatorname{rank} E_{2,t}(\overline{\mathbb{Q}}(t)) = \operatorname{rank} E_{1,s}(\overline{\mathbb{Q}}(s)) + \operatorname{rank} E_{0,u}^{(1+3u)}(\overline{\mathbb{Q}}(u)) + \operatorname{rank} E_{0,u}^{(u(1+3u))}(\overline{\mathbb{Q}}(u)).$$

Proof. Since solving $s = \frac{2t}{t^2-3}$ for t yields $t = \frac{1\pm\sqrt{1+3s^2}}{s}$, we have

$$E_{2,t}(\overline{\mathbb{Q}}(t)) = E_{1,s}(\overline{\mathbb{Q}}(s)(\sqrt{1+3s^2}))$$

By Theorem 5.4, we get (5.1). Similarly, $E_{1,s}$ is obtained by substituting $u = s^2$ into $E_{0,u}$, so we have

$$E_{1,s}^{(1+3s^2)}(\overline{\mathbb{Q}}(s)) = E_{0,u}^{(1+3u)}(\overline{\mathbb{Q}}(u)(\sqrt{u})),$$

then we get (5.2). □

Theorem 5.6.

$$\operatorname{rank} E_{0,u}^{(u(1+3u))}(\overline{\mathbb{Q}}(u)) = 1$$

Proof. We have a point of infinite order

$$(u-1, \sqrt{-1}(u-1)) \in E_{0,u}^{(u(1+3u))}(\overline{\mathbb{Q}}(u))$$

and thus the rank is positive. The discriminant of $E_{0,u}^{(u(1+3u))}$ is

$$\Delta(E_{0,u}^{(u(1+3u))}) = 256u^8(u-1)^4(u+1)^4(3u+1)^6,$$

and the types of the singular fibers of $E_{0,u}^{(u(1+3u))}$ are calculated as in Table 3 below by Tate's algorithm. In the same way as the proof of Theorem 2.1, we have

$$\operatorname{rank} E_{0,u}^{(u(1+3u))}(\overline{\mathbb{Q}}(u)) \leq 1.$$

□

Table 3: Singular fibers of $E_{0,u}^{(u(1+3u))}$

Place	Type	m_v
$u = 0$	I_2^*	7
$u = \pm 1$	I_4	4
$u = -\frac{1}{3}$	I_0^*	5
$u = \infty$	I_2	2

6 Reductions

Let A be a discrete valuation ring of a number field K with maximal ideal $\mathfrak{m}$, whose residue field k has $q = p^r$ elements with p prime. Let S be an integral scheme with a morphism $S \to \operatorname{Spec} A$ that is projective and smooth of relative dimension 2. Then the projective surface $\overline{S} = S_{\overline{\mathbb{Q}}}$ and $\tilde{S} = S_{\overline{k}}$ are smooth over the algebraically closed field $\overline{\mathbb{Q}}$ and $\overline{k}$, respectively. We will assume that $\overline{S}$ and $\tilde{S}$ are integrals, i.e., they are irreducible, nonsingular, projective surfaces.

For $l \neq p$ be a prime number, we denote by $H^2_{\text{ét}}(\tilde{S}, \mathbb{Q}_l)$ the l-adic étale cohomology group of X and by $H^2_{\text{ét}}(\tilde{S}, \mathbb{Q}_l)(1)$ the Tate twist of it.

Theorem 6.1. ([8, Proposition 6.2.])
There are natural injective homomorphisms

$$\mathrm{NS}(\overline{S}) \otimes_{\mathbb{Z}} \mathbb{Q}_l \hookrightarrow \mathrm{NS}(\tilde{S}) \otimes_{\mathbb{Z}} \mathbb{Q}_l \hookrightarrow H^2_{\text{ét}}(\tilde{S}, \mathbb{Q}_l)(1)$$

of finite-dimensional vector spaces over $\mathbb{Q}_l$.

Let $F : S_k \to S_k$ denote the absolute Frobenius, which acts as the identity on the points and by $f \mapsto f^p$ on the structure sheaf. Set $\varphi := F^r$ and let $\varphi^{(i)}$ denote the automorphism on $H^i_{\text{ét}}(\tilde{S}, \mathbb{Q}_l)$ induced by $\varphi \times 1$ acting on $S_k \times_{\operatorname{Spec} k} \operatorname{Spec} \overline{k} \cong \tilde{S}$.

Corollary 6.2. ([8, Corollary 6.4.]) The ranks of $\mathrm{NS}(\overline{S})$ and $\mathrm{NS}(\tilde{S})$ are bounded from above by the number of eigenvalues λ of $\varphi^{(2)}$ for which λ/q is a root of unity, counted with multiplicity.

Remark 6.3. ([8, Remark 6.5.]) Tate's conjecture states that the upper bound mentioned in Corollary 6.2 is actually equal to the rank of $\mathrm{NS}(\tilde{S})$. Tate's conjecture has been proven for elliptic K3 surfaces.

Now we want to calculate the characteristic polynomial $\operatorname{char}(\varphi^{(2)})$. Beforehand, we recall the Lefschetz fixed point theorem.

Theorem 6.4.

$$\#\tilde{S}(\mathbb{F}_{q^m}) = \sum_{i=0}^{n} (-1)^i \operatorname{Tr}((\varphi^{(i)})^m)$$

Corollary 6.5.

$$\operatorname{Tr}((\varphi^{(2)})^m) = \#\tilde{S}(\mathbb{F}_{q^m}) - 1 - q^{2m}$$

Proof.

$$\dim H^1_{\text{ét}}(\tilde{S}, \mathbb{Q}_l) = \dim H^3_{\text{ét}}(\tilde{S}, \mathbb{Q}_l) = 0$$

and $\varphi^{(4)}$ acts on $H^4_{\text{ét}}(\tilde{S}, \mathbb{Q}_l) \cong \mathbb{Q}_l$ by multiplication by q^2. □

Let V be the linear subspace of $H^2_{\text{ét}}(\tilde{S}, \mathbb{Q}_l)$ generated by the components of the singular fibers and by the zero section and $W = H^2_{\text{ét}}(\tilde{S}, \mathbb{Q}_l)/V$, then

$$\dim V = \sum_{v \in R} (m_v - 1) + 2.$$

By the multiplicativity of the characteristic polynomial, we have

$$\operatorname{char}(\varphi^{(2)}) = \operatorname{char}(\varphi^{(2)}|V) \cdot \operatorname{char}(\varphi^{(2)}_W)$$

and

$$\operatorname{Tr}((\varphi^{(2)})^m) = \operatorname{Tr}((\varphi^{(2)}|V)^m) + \operatorname{Tr}((\varphi^{(2)}_W)^m) \tag{6.1}$$

for any $m \in \mathbb{Z}$, where $\varphi^{(2)}_W : W \to W$ is induced by $\varphi^{(2)}$. Since $\varphi^{(2)}$ acts on V by multiplication by q, we have

$$\operatorname{char}(\varphi^{(2)}|V) = (x - q)^{\dim V}.$$

As for the characteristic polynomial of $\varphi^{(2)}_W$, let $t_m := \operatorname{Tr}((\varphi^{(2)}_W)^m)$, then $\operatorname{char}(\varphi^{(2)}_W)$ is the polynomial part of

$$\frac{x^{\dim W}}{\exp\left(\sum_{m=1}^{\infty} \frac{t_m}{m} x^{-m}\right)} = x^{\dim W}\left(1 + t_1 x^{-1} + \frac{t_1^2 - t^2}{2} x^{-2} + \frac{-t_1^3 + 3t_1 t_2 - 2t_3}{6} x^{-3} + \cdots\right).$$

Here, by (6.1) and Corollary 6.5, we have

$$t_m = \#\tilde{S}(\mathbb{F}_{q^m}) - 1 - q^{2m} - \dim V \cdot q^m.$$

Lemma 6.6. ([9, Theorem 4, Part III]) If $\tilde{S}$ is a K3 surface, then the second Betti number of $\tilde{S}$ is 22.

Theorem 6.7.

$$\operatorname{rank} E_{0,u}^{(1+3u)}(\overline{\mathbb{Q}}(u)) = 0$$

Table 4: Singular fibers of $E_{0,u}^{(1+3u)}$

Place	Type	m_v
$u=0$	I_2	2
$u=\pm 1$	I_4	4
$u=-\frac{1}{3}$	I_0^*	5
$u=\infty$	I_2^*	7

Proof. We denote by $S=\mathcal{E}_{0,u}^{(1+3u)}\to\mathbb{P}^1$ the elliptic surface with the generic fiber $E_{0,u}^{(1+3u)}$.

Then S is a K3 surface and by Lemma 6.6, we have

$$\dim_{\mathbb{Q}_l} H^2_{\text{ét}}(\tilde{S},\mathbb{Q}_l)=22.$$

V is of rank 19, on which the Frobenius automorphism acts by multiplication by p.

$$\operatorname{char}(\varphi^{(2)}|V)=(x-5)^{19}$$

Note that all the multiplicative fibers are split in $\mathbb{F}_{5^m}$ for $m=1,2,3$.

$$t_m=\#\tilde{S}(\mathbb{F}_{5^m})-1-5^{2m}-19\cdot 5^m$$

m	1	2	3
$\#\tilde{S}(\mathbb{F}_{5^m})$	120	1080	18264
t_m	-1	-21	263

$$\operatorname{char}(\varphi_W^{(2)})=x^3+x^2+11x-77$$

If $\operatorname{char}(\varphi_W^{(2)})$ has a root of the form $x=5\zeta$ for some root of unity ζ, then ζ is a root of the polynomial

$$125x^3+25x^2+55x-77,$$

which is irreducible over $\mathbb{Q}$. It contradicts the fact that ζ is an algebraic integer. By Corollary 6.2, $\rho(\mathcal{E}_{0,u}^{(1+3u)})\le 19$. Then by Theorem 3.1, we have

$$\operatorname{rank} E_{0,u}^{(1+3u)}(\overline{\mathbb{Q}}(u))=0.$$

□

This concludes the proof of the main theorem.

Acknowledgments

I would like to express my deepest appreciation to my professor Masato Kurihara for his guidance and encouragement. I also could not have undertaken this journey without the support of Dr. Bartosz Naskręcki. He has politely answered my many emails with questions and given me valuable advice.

References

[1] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. eng. Graduate texts in mathematics ; 151. New York: Springer, 1994.

[2] T. Yoshida. *The relationship between face cuboids and elliptic curves*. 2024. arXiv: 2407.09825 [math.NT]. URL: https://arxiv.org/abs/2407.09825.

[3] B. Naskręcki. "Mordell-Weil ranks of families of elliptic curves associated to Pythagorean triples". eng. In: *Acta Arithmetica* 160.2 (2013), pp. 159–183. URL: http://eudml.org/doc/279803.

[4] T. Shioda. "On the Mordell-Weil Lattices". In: *Commentarii Mathematici Universitatis Sancti Pauli* 39 (1990).

[5] 徹. 塩田. *Mordell-Weil lattice* **の理論とその応用**. jpn. 東京大学数理科学セミナリーノート ; 1. 東京: Graduate school of mathematical sciences, 1993.

[6] K. Kodaira. "On Compact Analytic Surfaces, III". In: *Annals of Mathematics* 78.1 (1963), pp. 1–40. URL: http://www.jstor.org/stable/1970500 (visited on 2025-01-12).

[7] J. H. Silverman. *The arithmetic of elliptic curves*. eng. 2nd ed. Graduate texts in mathematics ; 106. New York: Springer, 2009.

[8] R. van Luijk. "An elliptic K3 surface associated to Heron triangles". In: *Journal of Number Theory* 123.1 (2007), pp. 92–119. DOI: https://doi.org/10.1016/j.jnt URL: https://www.sciencedirect.com/science/article/pii/S0022314X06001326.

[9] D. Mumford. *Selected papers on the classification of varieties and moduli spaces*. eng. New York: Springer, 2004.