

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

Hayato Yagi

(Student ID No.: 82313206)

Advisor Professor Masato Kurihara

March 2025

Keio University
Graduate School of Science and Technology
School of Fundamental Science and Technology

論文要旨

楕円曲線とは、種数 1 の滑らかな射影曲線のことである。楕円曲線上の点に対して加法を定義することができ、これにより楕円曲線上の点全体は、無限遠点を単位元とするアーベル群となる。体 K 上に定義された楕円曲線 E に対して、Mordell-Weil 群 $E(K)$ は E 上の K 有理点全体からなる群である。Mordell-Weil の定理によると、Mordell-Weil 群が有限生成アーベル群である。Mordell-Weil 群は楕円曲線の研究において重要な対象であり、特にそのランクは決定が難しい。

本研究では、ピタゴラス数 $(a, b, c) \in \mathbb{Z}^3$ に対して、楕円曲線 $y^2 = x(x - a^2)(x + b^2)$ の族について考察する。これは Wiles によるフェルマーの最終定理の証明の鍵となった Frey 曲線の、 $n = 2$ の場合である。ピタゴラス数 (a, b, c) は、有理数 $m, n \in \mathbb{Q}$ で $(m, n) = 1$ を満たすものにより、 $(a, b, c) = (2mn, m^2 - n^2, m^2 + n^2)$ とパラメータ表示される。 $s = m/n$ とおけば、2 次 Frey 曲線の族は関数体 $\overline{\mathbb{Q}}(s)$ 上の楕円曲線

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

として扱うことができる。この楕円曲線の $\overline{\mathbb{Q}}(s)$ 上の Mordell-Weil 群のランクは 0 であることが知られている。本研究では、この楕円曲線の無限部分族で、その Mordell-Weil 群のランクが 1 であるものを発見した。これは、 $\overline{\mathbb{Q}}$ で $E_{1,s}$ の Mordell-Weil のランクが正となるような $s \in \overline{\mathbb{Q}}$ が無限に存在することを意味する。

証明には楕円曲面の理論を用いた。一般に関数体上の楕円曲線は楕円曲面に対応し、Shioda-Tate の公式は楕円曲面の Néron-Severi 群のランクと Mordell-Weil 群のランクの関係を与える。

Tate のアルゴリズムにより、楕円曲面の特異繊維の型と Néron-Severi 群のランクの上限を決定することで、無限部分族のランクが 2 以下であることを示すことができる。しかしながら、この上限は最適ではない。無限部分族のランクがちょうど 1 であることを示すために、Lefschetz の不動点定理を用いて l -進エタールコホモロジー に作用する Frobenius 自己同型の特性多項式を計算し、Néron-Severi 群のランクのより良い上界を得た。

Thesis Abstract

An elliptic curve is a smooth projective curve of genus 1. For points on an elliptic curve we can define an addition law, which makes the set of points on an elliptic curve into an abelian group with the identity element being the point at infinity. 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 theorem states that the Mordell-Weil group is a finitely generated abelian group. The Mordell-Weil group is an important object in the study of elliptic curves. Especially, the rank of the Mordell-Weil group is important and difficult to determine.

For Pythagorean triples $(a, b, c) \in \mathbb{Z}^3$, we study a family of elliptic curves $y^2 = x(x - a^2)(x + b^2)$. This is the $n = 2$ case of the Frey curve, the key curve used in the proof of Fermat's last theorem by Wiles. Using the parameterization of Pythagorean triples $(a, b, c) = (2mn, m^2 - n^2, m^2 + n^2)$ by $m, n \in \mathbb{Q}$ with $(m, n) = 1$ and putting $s = m/n$, we can one-parameterize Frey curves of degree two, and consider the family as an elliptic curve

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

over a function field $\overline{\mathbb{Q}}(s)$. 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 determine the types of special fibers of the elliptic surfaces and an upper bound of the rank of the Néron-Severi group by Tate's algorithm. Using this we can prove that the generic rank of the subfamily is no more than 2. However, the upper bound is not sharp. 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 using Lefschetz fixed point theorem and get the sharp upper bound of the rank of the Néron-Severi group.

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

Hayato Yagi

January 28, 2025

1 Introduction

An elliptic curve is a smooth projective curve of genus 1. For points on an elliptic curve we can define an addition law, which makes the set of points on an elliptic curve into an abelian group with the identity element being the point at infinity. 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 .

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 $E(K)$. The Mordell-Weil group is an important object in the study of elliptic curves. Especially, the rank of the Mordell-Weil group is important and difficult to determine.

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 $(a, b, c) \in \mathbb{Z}^3$ be a Pythagorean triple and consider the elliptic curve defined by the Weierstrass equation

$$y^2 = x(x - a^2)(x + b^2), \quad (1.1)$$

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

We can parameterize Pythagorean triples (a, b, c) by $m, n \in \mathbb{Z}$ with $(m, n) = 1$ as $(a, b, c) = (2mn, m^2 - n^2, m^2 + n^2)$. Then the equation (1.1) can be written as $y^2 = x(x - 4m^2n^2)(x + (m^2 - n^2)^2)$. We replace x, y by n^2x, n^3y and put $s = m/n$. Then we get an elliptic curve

$$E_{1,s} : y^2 = x(x - 4s^2)(x + (s^2 - 1)^2). \quad (1.2)$$

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 $\pi : \mathcal{E} \rightarrow C$ with the generic fiber E called the Néron model. We can use tools in the theory of surfaces by associating an elliptic surface $\mathcal{E}_{1,s} \rightarrow \mathbb{P}^1$ to $E_{1,s}$.

The elliptic surface $E/k(C)$ is called the generic fiber of the elliptic surface $\mathcal{E} \rightarrow C$. For $s \in \overline{\mathbb{Q}}$, $\mathcal{E}_s := \pi^{-1}(s)$ 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. ([7, Theorem 6.1.]) Let $\mathcal{E} \rightarrow C$ be an elliptic surface defined over a field k and E be the corresponding elliptic curve over the function field $k(C)$. If $\mathcal{E} \rightarrow C$ 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, [7, Theorem 11.4.]) Let $\mathcal{E} \rightarrow C$ 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 \bar{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.

Lemma 1.4. ([7, Exercise 3.9.(a)]) Let \mathcal{E} be an elliptic surface over k , and let $j_{\mathcal{E}} : C \rightarrow \mathbb{P}^1$ be a morphism such that $j_{\mathcal{E}}(v)$ gives the j -invariant for any non-singular fibers \mathcal{E}_v . If \mathcal{E} splits over k , then $j_{\mathcal{E}}$ is a constant map.

Remark 1.5. We can easily check that all elliptic surfaces in this paper have non-constant j -invariants, therefore, they do not split. Thus we can apply the Specialization Theorem (Theorem 1.3).

2 Main theorem

First, we determine the Mordell-Weil group of $E_{1,s}$ defined by (1.2).

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 $E_{1,s_0}(\mathbb{Q})_{\text{tors}}$ 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

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

In spite of the fact that the generic rank of $E_{1,s}$ is 0, Yoshida ([10, 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 a 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, [5, Corollary 5.3]) Let $\mathcal{E} \rightarrow C$ be an elliptic surface over a smooth projective curve C over an algebraically closed field k . 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

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

We have the following theorem giving an upper bound of the Picard number $\rho(\mathcal{E})$.

Theorem 3.2. ([4, Twierdzenie 2.2.9, 2.2.10, 2.2.19]) Let \mathcal{E} and R be as in Theorem 3.1. Let $\chi(\mathcal{E})$ be the arithmetic genus of \mathcal{E} , $e(\mathcal{E}_v)$ be the local Euler number of the special fiber at v , and $g(C)$ be the genus of C . Assume $\text{ch } k = 0$. Then

$$12\chi(\mathcal{E}) = e(\mathcal{E}) := \sum_{v \in R} e(\mathcal{E}_v),$$

$$\rho(\mathcal{E}) \leq 10\chi(\mathcal{E}) + 2g(C).$$

If $\chi(\mathcal{E}) = 1$, the elliptic surface \mathcal{E} is called rational. If $\chi(\mathcal{E}) = 2$, the elliptic surface \mathcal{E} is called an elliptic K3 surface.

We can compute types of each special fibers denoted by Kodaira's symbols by Tate's algorithm ([7, IV §9]). The following table shows the correspondence between Kodaira's symbols and the values of m_v and $e(\mathcal{E}_v)$ appearing in the two theorems above.

Table 1: Kodaira's symbols ([6, pp.136-137 付録 2])

Kodaira's symbol	m_v	$e(\mathcal{E}_v)$
I_n	n	n
II	1	2
III	2	3
IV	3	4
I_n^*	$n + 5$	$n + 6$
II^*	9	10
III^*	8	9
IV^*	7	8

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

Theorem 3.3. ([3, Lem.3.5]) Let \mathcal{E} and R be as in Theorem 3.1. Let E be the generic fiber of \mathcal{E} . Then we have

$$E(\overline{\mathbb{Q}}(s))_{\text{tors}} \hookrightarrow \prod_{v \in R} G(\mathcal{E}_v),$$

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

4 Proof of Theorem 2.1 and Theorem 2.3

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

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

and the j -invariant is

$$j_{\mathcal{E}_{1,s}} = \frac{16(s^4 - 2s^3 + 2s^2 + 2s + 1)^3(s^4 + 2s^3 + 2s^2 - 2s + 1)^3}{s^4(s+1)^4(s-1)^4(s^2+1)^4}.$$

By Tate's algorithm, we have the following table.

Table 2: Singular fibers of $E_{1,s}$

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

Then $e(\mathcal{E}_{1,s}) = 4 \times 6 = 24$ and we have $\rho(\mathcal{E}_{1,s}) \leq 20$ by Theorem 3.2. By Shioda-Tate formula (Theorem 3.1), we have

$$\text{rank}(E_{1,s}) \leq 20 - (2 + (4 - 1) \times 6) = 0$$

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

$$2T_1 = (4s^2, 0), \quad (4.2)$$

$$2T_2 = (0, 0). \quad (4.3)$$

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

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

□

Theorem 4.1. (Mazur's Theorem) Let E be an elliptic curve defined over \mathbb{Q} . Then the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following groups.

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

Proof of Theorem 2.3. The non-singularity of the special fibers of $\mathcal{E}_{1,s}$ at $s \in \mathbb{Q} \setminus \{0, \pm 1\}$ follows from the equation (4.1). By the equation (2.1) and Mazur's Theorem (Theorem 4.1), the only possibility of $E_{1,s_0}(\mathbb{Q})_{\text{tors}}$ 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, the study of this elliptic curve goes back to Fetmat, and it is well known 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 3 below by Tate's algorithm. Then in a similar way to the proof of Theorem 2.1, we get $\text{rank } E_{2,t}(\overline{\mathbb{Q}}(t)) \leq 2$. On the other hand, we have only one point of infinite order in $E_{2,t}(\overline{\mathbb{Q}}(t))$.

Lemma 5.1.

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

Table 3: Singular fibers of $E_{2,t}$

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

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

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. ([8, 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

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

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

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

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

Therefore, we have

$$\begin{aligned} \text{rank } E_{2,t}(\overline{\mathbb{Q}}(t)) &= \text{rank } E_{1,s}(\overline{\mathbb{Q}}(s)) \\ &\quad + \text{rank } E_{0,u}^{(1+3u)}(\overline{\mathbb{Q}}(u)) \\ &\quad + \text{rank } E_{0,u}^{(u(1+3u))}(\overline{\mathbb{Q}}(u)). \end{aligned} \quad (5.3)$$

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). □

We already know that the rank of $E_{1,s}(\overline{\mathbb{Q}})$ is 0. The rank of $E_{0,u}^{(u(1+3u))}(\overline{\mathbb{Q}}(u))$ in the equation (5.3) can also be calculated easily as follows.

Theorem 5.6.

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

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

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

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

Place	Type	m_v	e
$u = 0$	I_2^*	7	8
$u = \pm 1$	I_4	4	4
$u = -\frac{1}{3}$	I_0^*	5	6
$u = \infty$	I_2	2	2

and the types of the singular fibers of $E_{0,u}^{(u(1+3u))}$ are calculated as in Table 4 below by Tate's algorithm. In the same way as the proof of Theorem 2.1, we have $e(\mathcal{E}_{0,u}^{(u(1+3u))}) = 8 + 4 \times 2 + 6 + 2 = 24$ and

$$\text{rank } E_{0,u}^{(u(1+3u))}(\overline{\mathbb{Q}}(u)) \leq 20 - (2 + (7 - 1) + (4 - 1) \times 2 + (5 - 1) + (2 - 1)) = 1.$$

□

The remaining task is to calculate the rank of $E_{0,u}^{(1+3u)}(\overline{\mathbb{Q}}(u))$. Theorem 3.2 gives the rank is not greater than 1, which is not sharp. We will show the rank is 0 in the next section.

6 Reductions

Let A be a discrete valuation ring with maximal ideal \mathfrak{m} and fraction field K . Assume that the residue field $k = A/\mathfrak{m}$ has $q = p^r$ elements with p prime. Let S be an integral scheme with a morphism $S \rightarrow \text{Spec } A$ 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 a prime number $l \neq p$, we denote by $H_{\text{ét}}^2(\tilde{S}, \mathbb{Q}_l)$ the l -adic étale cohomology group of X and by $H_{\text{ét}}^2(\tilde{S}, \mathbb{Q}_l)(1)$ its Tate twist.

Theorem 6.1. ([9, Proposition 6.2.]) There are natural injective homomorphisms

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

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

Let $F : S_k \rightarrow S_k$ 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 $H_{\text{ét}}^i(\tilde{S}, \mathbb{Q}_l)$ induced by $\varphi \times 1$ acting on $S_k \times_{\text{Spec } k} \text{Spec } \overline{k} \cong \tilde{S}$.

Corollary 6.2. ([9, Corollary 6.4.]) The ranks of $\text{NS}(\bar{S})$ and $\text{NS}(\tilde{S})$ 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. ([9, Remark 6.5.]) Tate's conjecture states that the upper bound mentioned in Corollary 6.2 is actually equal to the rank of $\text{NS}(\tilde{S})$. Tate's conjecture has been proven for elliptic K3 surfaces by Artin and Swinnerton-Dyer [1].

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

Theorem 6.4.

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

Corollary 6.5.

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

Proof.

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

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

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

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

By the multiplicativity of the characteristic polynomial, we have

$$\text{char}(\varphi^{(2)}) = \text{char}(\varphi^{(2)}|V) \cdot \text{char}(\varphi_W^{(2)})$$

and

$$\text{Tr}((\varphi^{(2)})^m) = \text{Tr}((\varphi^{(2)}|V)^m) + \text{Tr}((\varphi_W^{(2)})^m) \quad (6.1)$$

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

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

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

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

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

Theorem 6.7.

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

Proof. We denote by $S = \mathcal{E}_{0,u}^{(1+3u)} \rightarrow \mathbb{P}^1$ the elliptic surface with the generic fiber $E_{0,u}^{(1+3u)}$. Put $\mathfrak{p} = (5) \in \text{Spec } \mathbb{Z}$ and $A = \mathbb{Z}_{\mathfrak{p}}$. The residue field $k = A/\mathfrak{p} \cong \mathbb{F}_5$. S defines an elliptic surface $\tilde{S} = S_{\overline{\mathbb{F}_5}} \rightarrow \mathbb{P}^1$. We can check that \tilde{S} has exactly the same types of singular fibers as S .

Table 5: Singular fibers of $E_{0,u}^{(1+3u)}$

Place	Type	m_v	e
$u = 0$	I_2	2	2
$u = \pm 1$	I_4	4	4
$u = -\frac{1}{3}$	I_0^*	5	6
$u = \infty$	I_2^*	7	8

Then since $e(\tilde{S}) = 2 + 4 \times 2 + 6 + 8 = 24$, \tilde{S} is a K3 surface and by Lemma 6.6, we have

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

V is of rank 19, on which the Frobenius automorphism acts by multiplication by 5. Thus

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

In order to calculate the characteristic polynomial of $\varphi_W^{(2)}$, we need to compute the number of points on \tilde{S} over finite fields \mathbb{F}_{5^m} . Note that all the multiplicative fibers are split in \mathbb{F}_{5^m} for $m = 1, 2, 3$. We count the number of points on each special fibers. For non-singular fibers, the Schoof-Elkies-Atkin (SEA) algorithm, which calculates the number of points on an elliptic curve over a finite field, is known and can be used. For each singular fiber, the number of points is determined by the type of the fiber. Singular fibers' configurations are as shown in Table 1 where each component is \mathbb{P}^1 (TODO: 絵を貼る). We get Table 6 by subtracting from $m_v \times \#\mathbb{P}^1(\mathbb{F}_{q^m}) = m_v(q^m + 1)$ the number of points that are counted twice or more.

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

Table 6: Number of points on each singular fiber over a finite field
(TODO: I_n と I_n^* しか使わないが他も書くか?)

Type	Configuration	$\mathcal{E}_v(\mathbb{F}_{q^m})$
I_n	x	nq^m
II	x	x
III	x	x
IV	x	x
I_n^*	x	$(n+5)q^m + 1$
II^*	x	x
III^*	x	x
IV^*	x	x

These calculations result in Table 7.

Therefore, we have

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

If $\text{char}(\varphi_W^{(2)})$ 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, $\rho(\mathcal{E}_{0,u}^{(1+3u)}) \leq 19$. Then by Theorem 3.1, we have

$$\text{rank } E_{0,u}^{(1+3u)}(\overline{\mathbb{Q}}(u)) \leq 19 - (2 + (2-1) + (4-1) \times 2 + (5-1) + (7-1)) = 0.$$

□

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.

Table 7: $\#\tilde{S}(\mathbb{F}_{5^m})$ and t_m

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

References

- [1] M. Artin and H. P. F. Swinnerton-Dyer. “The Shafarevich-Tate Conjecture for Pencils of Elliptic Curves on K3 Surfaces.” In: *Inventiones mathematicae* 20 (1973), pp. 249–266.
- [2] D. Mumford. *Selected papers on the classification of varieties and moduli spaces*. eng. New York: Springer, 2004.
- [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.
- [4] B. Naskręcki. “Rangi w rodzinach krzywych eliptycznych i formy modularne”. PhD thesis. Adam Mickiewicz University, 2014.
- [5] T. Shioda. “On the Mordell-Weil Lattices”. In: *Commentarii Mathematici Universitatis Sancti Pauli* 39 (1990).
- [6] T. Shioda. *Mordell-Weil lattice の理論とその応用*. jpn. 東京大学数理学科学セミナーノート ; 1. 東京: Graduate school of mathematical sciences, 1993.
- [7] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. eng. Graduate texts in mathematics ; 151. New York: Springer, 1994.
- [8] J. H. Silverman. *The arithmetic of elliptic curves*. eng. 2nd ed. Graduate texts in mathematics ; 106. New York: Springer, 2009.
- [9] R. van Luijk. “An elliptic K3 surface associated to Heron triangles”. In: *Journal of Number Theory* 123.1 (2007), pp. 92–119.
- [10] T. Yoshida. *The relationship between face cuboids and elliptic curves*. 2024. arXiv: 2407.09825 [math.NT].