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

指導教員：栗原将人教授
学籍番号：82313206　氏名：八木颯仁

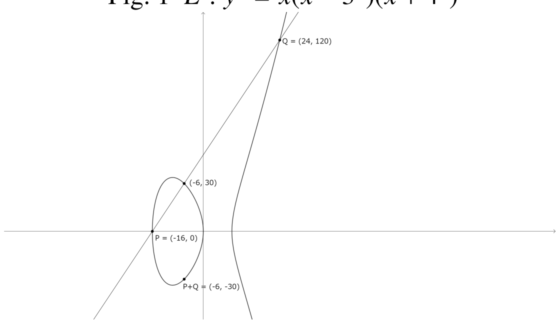
## 1 Introduction

An elliptic curve defined over a field $K$ is a curve defined by a Weierstrass equation

$$E : y^2 = x^3 + Ax^2 + Bx + C$$

where $A, B, C \in K$ and the discriminant $\Delta = -4A^3C + A^2B^2 + 18ABC - 4B^3 - 27C^2$ is nonzero. On points on an elliptic curve defined over $\mathbb{Q}$, we can define an addition law geometrically. For two points $P, Q$ on $E$, the point $-(P + Q)$ is defined as the third point of intersection of the line passing through $P$ and $Q$ with the curve. The sum $P + Q$ is the point symmetric to $-(P + Q)$ with respect to the $x$-axis.

Fig. 1 $E : y^2 = x(x - 3^2)(x + 4^2)$




The definition can be extended to any field $K$. The set of points on an elliptic curve forms an abelian group with the identity element being the point at infinity. 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 the arithmetic of elliptic curves. Especially, the rank of the Mordell-Weil group is important and difficult to determine in general.

Let $(a, b, c) \in \mathbb{Z}^3$ be a Pythagorean triple, namely integers satisfies $a^2 + b^2 = c^2$, and consider the elliptic curve defined by the Weierstrass equation

$$y^2 = x(x - a^2)(x + b^2). \tag{1}$$

This is the $n = 2$ case of the Frey curve.

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) 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

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

We consider $E_{1,s}$ as an elliptic curve over a function field $\overline{\mathbb{Q}}(s)$. We associate an elliptic surface $\mathcal{E}_{1,s} \to \mathbb{P}^1$ to $E_{1,s}$.

## 2 Main Theorem

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

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

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

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

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 [1].

## 3 Sketch of proof

First, we compute types of singular fibers of elliptic surfaces by Tate's algorithm. The number of components $m_v$ and the local Euler number $e(\mathcal{E}_v)$ of each special fiber at $v$ are computed. The torsion subgroups are determined using these data. We know that there is a point of infinite order $\left(s^2 - 1, \sqrt{-1}s(s^2 - 1)\frac{t^2+3}{t^2-3}\right)$ on $E_{2,t}(\overline{\mathbb{Q}}(t))$. This implies that the rank of $E_{2,t}(\overline{\mathbb{Q}}(t))$ is at least 1. The following theorem plays a key role in the proof of the main theorem.

**Theorem 3.1.** (Shioda-Tate formula, [3, Corollary 5.3]) Let $\mathcal{E} \to C$ 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

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

Now, we are interested in the upper bounds of the rank of the Néron-Severi groups. To make the later computation feasible, we decompose the rank of $E_{2,t}(\overline{\mathbb{Q}}(t))$ into the ranks of elliptic curves with lower order coefficients in the Weierstrass equations.

**Theorem 3.2.** 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

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

We have an estimation that $\rho(\mathcal{E}) \leq \frac{5}{6} \sum_{v \in R} e(\mathcal{E}_v)$ by [2], which gives

$$\operatorname{rank} E_{1,s}(\overline{\mathbb{Q}}(s)) = 0,$$

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

However, the upper bound computed in the same way for $E_{0,u}^{(1+3u)}$ is not sharp. We need a more sophisticated method to estimate the rank of $E_{0,u}^{(1+3u)}$, which we will explain below.

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 $S \to \operatorname{Spec} A$ 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. For a prime number $l \neq p$, we denote by $H^2_{\text{ét}}(\tilde{S}, \mathbb{Q}_l)$ the $l$-adic étale cohomology group of $X$ and by $H^2_{\text{ét}}(\tilde{S}, \mathbb{Q}_l)(1)$ its Tate twist. Let $\varphi^(i)$ be the Frobenius automorphism acting on $H^i_{\text{ét}}(\tilde{S}, \mathbb{Q}_l)$. Under some assumptions, we have the following theorem.

**Theorem 3.3.** ([4, Corollary 6.4.]) The ranks of $\mathrm{NS}(\overline{S})$ and $\mathrm{NS}(\tilde{S})$ are bounded from above by the number of eigenvalues $\lambda$ of $\varphi^{(2)}$ for which $\lambda/q$ is a root of unity, counted with multiplicity.

We apply Theorem 3.3 with $A = \mathbb{Z}_{(5)}$ and $S = \mathcal{E}_{0,u}^{(1+3u)} \to \mathbb{P}^1$. The characteristic polynomial of $\varphi^{(2)}$ can be calculated if we know the traces of $(\varphi^{(2)})^m$ for $m = 1, 2, 3$. The traces can be calculated by the Lefschetz fixed point theorem:

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

Tate's algorithm gives the types of singular fibers of $\mathcal{E}_{0,u}^{(1+3u)}$ as shown in Table 1, and the number of points on $\tilde{S}(\mathbb{F}_{5^m})$ are calculated as shown in Table 2.

Tab. 1 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 |

Tab. 2 $\#\tilde{S}(\mathbb{F}_{5^m})$

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

Using the computation above, we obtain

$$\operatorname{char}(\varphi^{(2)}) = (x - 5)^{19}(x^3 + x^2 + 11x - 77).$$

By Corollary 3.3, $\rho(\mathcal{E}_{0,u}^{(1+3u)}) \leq 19$. Then by Theorem 3.1, we have $\operatorname{rank} E_{0,u}^{(1+3u)}(\overline{\mathbb{Q}}(u)) \leq 0$.

## References


[1] B. Naskręcki. "Mordell-Weil ranks of families of elliptic curves associated to Pythagorean triples". eng. In: *Acta Arithmetica* 160.2 (2013), pp. 159–183.

[2] B. Naskręcki. "Rangi w rodzinach krzywych eliptycznych i formy modularne". PhD thesis. Adam Mickiewicz University, 2014.

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

[4] R. van Luijk. "An elliptic K3 surface associated to Heron triangles". In: *Journal of Number Theory* 123.1 (2007), pp. 92–119.