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

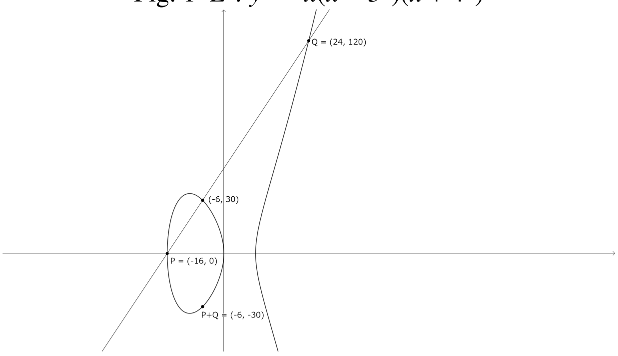
1 Introduction

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 elliptic curves. Especially, the rank of the Mordell-Weil group is important and difficult to determine.

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

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

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

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

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

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

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

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

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

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

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

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 Proof of Main Theorem

Lemma 3.1.

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

Proof.

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

□

The following theorem behaves a key role in the proof of the main theorem.

Theorem 3.2. (Shioda-Tate formula, [2, 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

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

Theorem 3.3. 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

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

Lemma 3.4.

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

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

It is relatively easy to prove Lemma 3.4. We can compute m_v and upper bounds of $\rho(\mathcal{E})$ in Theorem 3.2 by Tate's algorithm. 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.

Corollary 3.5. ([3, 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.

We apply Corollary 3.5 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 $\#\tilde{S}(\mathbb{F}_{5^m})$ and t_m

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

Then, we have

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

By Corollary 3.5, $\rho(\mathcal{E}_{0,u}^{(1+3u)}) \leq 19$. Then by Theorem 3.2, 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] T. Shioda. "On the Mordell-Weil Lattices". In: *Commentarii Mathematici Universitatis Sancti Pauli* 39 (1990).

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