

# 2次Frey曲線に付随する楕円曲面の Mordell-Weil 群について

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

八木 颯仁

慶應義塾大学 栗原研究室 修士 2 年

February 7, 2025

# 発表の概要と動機

## Fermat 方程式

$$x^n + y^n = z^n, \quad xyz \neq 0, \quad n \geq 2$$

の整数解  $(x, y, z) = (a, b, c)$  に対し、

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

は楕円曲線を与える。これを **Frey 曲線** と呼ぶ。

本研究では  $n = 2$  の場合の Frey 曲線の族について、それらをまとめて一つの楕円曲面と結び付けて扱うことで、Mordell-Weil 群の構造についていくつかの結果を得た。

- ランク 0 の 2 次 Frey 曲線はたくさん見つかるが、ランクが 1 の例もいくつか見つかっている。ランクが正の 2 次 Frey 曲線は無限個存在するのか？
- ランクが正の族を具体的にパラメトライズされた形で構成できないか？

## 1 Introduction

## 2 主定理

## 3 証明の概要

# 楕円曲線とは

体  $K$  (標数  $\neq 2$  とする) 上の楕円曲線  $E$  とは次のような形の方程式で表される曲線である。

$$E : y^2 = x^3 + Ax^2 + Bx + C \quad (A, B, C \in K)$$

ただし判別式  $\Delta = -4A^3C + A^2B^2 + 18ABC - 4B^3 - 27C^2$  は 0 でないとする。

楕円曲線上の  $K$ -有理点全体は群をなし、 $E(K)$  と書いて **Mordell-Weil 群** と呼ぶ。Mordell-Weil の定理によると、 $K$  に関する仮定の下で  $E(K)$  は有限生成アーベル群である。したがって

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

と書ける。ここで  $r$  は**ランク**、 $E(K)_{\text{tors}}$  は**振れ部分群** (torsion subgroup) と呼ばれる。

## 2次 Frey 曲線

本研究では Frey 曲線の 2 次の場合を扱う。

$(a, b, c)$  を以下を満たす正整数の 3 つ組とする。

$$a^2 + b^2 = c^2.$$

そのような  $(a, b, c)$  に対し、次の方程式で与えられる楕円曲線  $E/\mathbb{Q}$  を考える。

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

$(a, b, c)$  が互いに素でない場合は適当な変数変換によって原始ピタゴラス数の場合に帰着できる。原始ピタゴラス数  $(a, b, c)$  は 2 つの互いに素な正整数  $m > n$  によって

$$(a, b, c) = (2mn, m^2 - n^2, m^2 + n^2)$$

とパラメトライズされる。これを上の式に代入すると  $y^2 = x(x - 4m^2n^2)(x + (m^2 - n^2)^2)$  と書け、 $x, y$  を  $n^2x, n^3y$  で置き換えて  $s = m/n$  とおくと

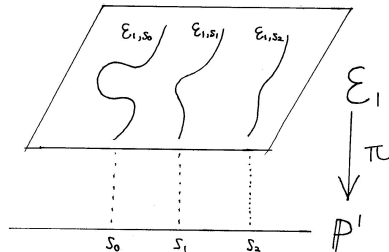
$$E_{1,s} : y^2 = x(x - 4s^2)(x + (s^2 - 1)^2)$$

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

本研究では、 $s$  に値を代入した個々の楕円曲線について考える代わりに、 $E_{1,s}$  を関数体  $\overline{\mathbb{Q}}(s)$  上の楕円曲線として考える。さらに  $E_{1,s}$  に対して

$$\mathcal{E}_1 = \{([X, Y, Z], s_0) \in \mathbb{P}^2 \times \mathbb{P}^1 \mid Y^2 Z = X(X - 4s_0^2 Z)(X + (s_0^2 - 1)^2 Z)\}$$

という  $\mathbb{P}^2 \times \mathbb{P}^1$  の 2 次元部分多様体を考えることで、 $E_{1,s}$  に対して楕円曲面  $\pi : \mathcal{E}_1 \rightarrow \mathbb{P}^1$  を対応させることができる。 $E_{1,s}$  を  $\mathcal{E}_1 \rightarrow \mathbb{P}^1$  の generic fiber と呼び、 $\mathcal{E}_{1,s_0} := \pi^{-1}(s_0)$  を special fiber と呼ぶ。有限個を除きすべての special fibers は非特異、すなわち楕円曲線である。



## Proposition 1 (Y.)

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

$E_{1,s}$  に  $s = \frac{2t}{t^2-3}$  を代入して

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

という  $E_{1,s}$  の部分族を考える。

## Theorem 1 (Y.)

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

ここでランクがちょうど 1 であることを示したということが重要である。

# Specialization Theorem

関数体上の Mordell-Weil 群と special fiber の Mordell-Weil 群の間には以下の関係がある。

## Theorem 2 (Specialization Theorem, [4])

- $\pi : \mathcal{E} \rightarrow \mathbb{P}^1$  を  $\mathbb{Q}$  上の *non-split* な楕円曲面
- $E$  を対応する  $\mathbb{Q}(\mathbb{P}^1)$  上の楕円曲線
- $\mathcal{E}_s := \pi^{-1}(s)$  を  $s$  での *special fiber*

とする。このとき有限個を除くすべての  $s \in \mathbb{P}^1(\overline{\mathbb{Q}})$  に対して *specialization homomorphism*

$$E(\overline{\mathbb{Q}}(\mathbb{P}^1)) \hookrightarrow \mathcal{E}_s(\overline{\mathbb{Q}})$$

が定義できて、これは**単射**である。

特に有限個の点を除き generic fiber のランクより special fiber のランクが小さくなることはない。したがって関数体上でランクの高い楕円曲線を見つけると、 $s$  に値を代入することで  $\overline{\mathbb{Q}}$  上ランクの高い楕円曲線を無限個見つけることができる。

# 証明の概要

- 捩れ部分群についての証明はランクに比べて簡単なのでここでは省略する。

- $E_{2,t}$  上の点

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

は無有限位数の点であることから  $E_{2,t}(\overline{\mathbb{Q}}(t))$  のランクは 1 以上であることが分かる。

- 重要なのは  $E_{1,s}(\overline{\mathbb{Q}}(s))$  のランクが 0 以下、 $E_{2,t}(\overline{\mathbb{Q}}(t))$  のランクが 1 以下であることを示すことである。

証明は大きく 2 つのステップに分けられる。

- ① Mordell-Weil 群のランクと Picard 数（後述）の関係を調べる。
- ② Picard 数を上から不等式で評価する。



## Theorem 3 (Shioda-Tate formula, [3])

- $\mathcal{E} \rightarrow \mathbb{P}^1$  を代数閉体  $k$  上で定義された楕円曲面
- $R \subset \mathbb{P}^1$  をその上の *special fiber* が特異となる点全体の集合
- 各  $v \in R$  に対し、 $m_v$  を  $v$  の上の *special fiber* の既約成分の数
- $\rho(\mathcal{E})$  を  $\mathcal{E}$  の Néron-Severi 群のランク ( Picard 数と呼ばれる )

とする。このとき

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

が成り立つ。

定理中に現れる  $R$  や  $m_v$  は Tate's algorithm によって計算できる。

## Proposition 2 ([2])

- $k$  と  $\mathcal{E} \rightarrow \mathbb{P}^1$  と  $R$  は先ほどの定理 (*Shioda-Tate formula*) と同じもの
- 各  $v \in R$  に対し、 $e(\mathcal{E}_v)$  を *special fiber*  $\mathcal{E}_v$  の *Euler 数*

とする。このとき

$$\rho(\mathcal{E}) \leq \frac{5}{6} \sum_{v \in R} e(\mathcal{E}_v)$$

が成り立つ。

$e(\mathcal{E}_v)$  も Tate's algorithm によって計算できる。

# $E_{1,s}(\overline{\mathbb{Q}}(s))$ のランク

実際 Tate's algorithm により各値は以下のように計算できる。

$E_{1,s}$  の特異ファイバー

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

したがって  $\rho(E_{1,s}) \leq 20$  であり、 $\text{rank}(E_{1,s}(\overline{\mathbb{Q}}(s))) \leq 0$  であることが分かる。

## $E_{2,t}(\overline{\mathbb{Q}}(t))$ のランク

ところが、同じ計算を  $E_{2,t}$  に対して行っても、ランクが 2 以下であることしか分からない。Picard 数の評価がゆるい。別の方法でより良い評価を得る必要がある。その準備として次の定理が必要である。

### Theorem 4 (Y.)

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

という  $\overline{\mathbb{Q}}(u)$  上の楕円曲線を新たに用意する。 $E^{(w)}$  で  $E$  の  $w$  での *quadratic twist* を表す。このとき

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

既に  $E_{1,s}$  のランクが 0 であることが分かっている。また  $E_{0,u}^{(u(1+3u))}$  のランクが 1 であることも同じ方法で分かる。残るは  $E_{0,u}^{(1+3u)}$  のランクを計算することである。 $E_{0,u}^{(1+3u)}$  は  $E_{2,t}$  より係数の次数が低く、また対応する楕円曲面が **K3 曲面**と呼ばれるよく研究された対象になることから、この後の計算が実行可能になる。

- $p$  を素数、 $q$  を  $p$  の冪とする。
- $S := \mathcal{E}_0^{(1+3u)} \rightarrow \mathbb{P}^1$  に対して  $\tilde{S} = S_{\overline{\mathbb{F}_q}} \rightarrow \mathbb{P}^1$  という reduction を考えることができる。
- $l$  を  $p$  と異なる素数として  $l$ -進 étale コホモロジーを  $H_{\text{ét}}^i(\tilde{S}, \mathbb{Q}_l)$  と書く。
- $H_{\text{ét}}^i(\tilde{S}, \mathbb{Q}_l)$  に作用する Frobenius 自己同型を  $\varphi^{(i)}$  と書く。

このとき  $\tilde{S}$  に関するいくつかの仮定の下で以下の定理が成り立つ。

### Theorem 5 ([1])

$S$  や  $\tilde{S}$  の Néron-Severi 群のランクは、 $\varphi^{(2)}$  の固有値  $\lambda$  で  $\lambda/q$  が 1 のべき根であるようなものの重複度を込めた個数以下である。

$\varphi^{(2)}$  の固有多項式を求めるには、今の場合  $m = 1, 2, 3$  に対して  $\text{Tr}((\varphi^{(2)})^m)$  を計算すればよい。

### Theorem 6 (Lefschetz の不動点定理)

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

$q = 5$  として実際に計算すると

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

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

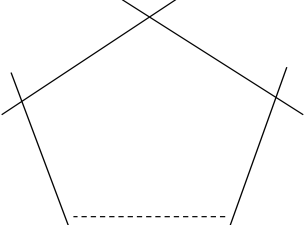
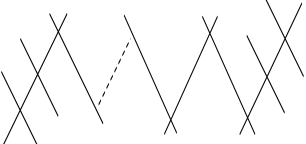
$m$	1	2	3
$\#\tilde{S}(\mathbb{F}_{5^m})$	120	1080	18264

これらの計算により固有多項式は

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

と計算でき、 $\rho(\mathcal{E}_{0,u}^{(1+3u)}) \leq 19$  と分かる。Shioda-Tate formula により  $\text{rank } E_{0,u}^{(1+3u)}(\overline{\mathbb{Q}}(u)) \leq 0$  が従い、主定理のランク部分である  $\text{rank } E_{2,t}(\overline{\mathbb{Q}}(t)) = 1$  が得られる。

# Number of points on each singular fiber over a finite field

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

- [1] R. van Luijk.  
An elliptic K3 surface associated to Heron triangles.  
*Journal of Number Theory*, Vol. 123, No. 1, pp. 92–119, 2007.
- [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.  
*Commentarii Mathematici Universitatis Sancti Pauli*, Vol. 39, No. 2, pp. 211–240, 1990.
- [4] J. H. Silverman.  
*Advanced topics in the arithmetic of elliptic curves*.  
Graduate texts in mathematics ; 151. Springer, 1994.