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 3, 2025

発表の概要と動機

Frey 曲線とは楕円曲線の一種であり、Fermat の最終定理の証明において重要な役割を果たした。Frey 曲線は Fermat 方程式の解に対応して定まり、$n \geq 3$ に対しては**存在しない**曲線である。
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。Generic fiber のランクは 0 であるが、ランクが正の 2 次 Frey 曲線も無限個存在することが知られている。部分族で generic ランクが 1 のものを発見した。

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

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

と書ける。ここで r は**ランク**、$E(K)_{\mathrm{tors}}$ は**捩れ部分群** (torsion subgroup) である。

Frey 曲線とは

Fermat 方程式

$$x^n + y^n = z^n, \quad xyz \neq 0, \quad n \geq 2 \tag{1}$$

の解 $(x, y, z) = (a, b, c)$ に対し、

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

は楕円曲線を与える。これを ***Frey* 曲線**と呼ぶ。

$n \geq 3$ のとき、Frey 曲線は存在しないことが知られている。本研究では Frey 曲線の 2 次の場合を扱う。

原始ピタゴラス数 (a, b, c) を以下を満たす正整数の 3 つ組で互いに素なものとする。

$$a^2 + b^2 = c^2. \tag{3}$$

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。

$$E : y^2 = x(x - a^2)(x + b^2) \tag{4}$$

原始ピタゴラス数は無限に存在する。

Frey 曲線とは

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。これを先ほどの式に代入すると $y^2 = x(x - 4m^2n^2)(x + (m^2 - n^2)^2)$ と書け、x, y を n^2x, n^3y で置き換えて $s = m/n$ とおくと

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

という方程式を得る。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。$E_{1,s}$ に対して

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

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 $\pi : \mathcal{E}_{1,s} \to \mathbb{P}^1$ を対応させることができる。$E_{1,s}$ を $\mathcal{E}_{1,s} \to \mathbb{P}^1$ 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。

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 1 (Specialization Theorem, [?])

$\pi : \mathcal{E} \to \mathbb{P}^1$ 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*

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

が定義できて、これは単射である。ただし $\mathcal{E}_s := \pi^{-1}(s)$ 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。

主定理

Proposition 1

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

$E_{1,s}$ 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 2 (主定理)

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

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。

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。また、$E_{2,t}$ 上の点

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

は無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。

Shioda-Tate formula

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

$\mathcal{E} \to \mathbb{P}^1$ を代数閉体 k 上で定義された楕円曲面とする。$R \subset \mathbb{P}^1$ を、その上の *special fiber* が特異となる点全体の集合とする。各 $v \in R$ に対し、m_v を v の上の *special fiber* の既約成分の数とする。$\rho(\mathcal{E})$ で $\mathcal{E}$ の *Néron-Severi* 群のランクを表し、*Picard* 数と呼ぶ。このとき

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

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。

Picard 数の評価

Proposition 2

k と $\mathcal{E} \to \mathbb{P}^1$ と R は先ほどの定理 *(Shioda-Tate formula)* と同じものとする。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、$\mathrm{rank}(E_{1,s}) \leq 0$ 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

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

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

$$\begin{aligned} \operatorname{rank} E_{2,t}(\overline{\mathbb{Q}}(t)) &= \operatorname{rank} E_{1,s}(\overline{\mathbb{Q}}(s)) \\ &\quad + \operatorname{rank} E_{0,u}^{(1+3u)}(\overline{\mathbb{Q}}(u)) \\ &\quad + \operatorname{rank} E_{0,u}^{(u(1+3u))}(\overline{\mathbb{Q}}(u)). \end{aligned} \tag{5}$$

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。

$S := \mathcal{E}_{0,u}^{(1+3u)} \to \mathbb{P}^1$ に対して $\tilde{S} = S_{\overline{\mathbb{F}_5}} \to \mathbb{P}^1$ という曲面が定義できる。l を 5 と異なる素数として l-進 étale コホモロジーを $H^i_{\text{ét}}(\tilde{S}, \mathbb{Q}_l)$、その Tate twist を $H^i_{\text{ét}}(\tilde{S}, \mathbb{Q}_l)(1)$ と書く。また $H^i_{\text{ét}}(\tilde{S}, \mathbb{Q}_l)$ に作用する Frobenius 自己同型を $\varphi^{(i)}$ と書く。このとき以下の定理が成り立つ。

Theorem 5 ([?])

S や $\tilde{S}$ の *Néron-Severi* 群のランクは、$\varphi^{(2)}$ の固有値 λ で $\lambda/5$ 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 $\mathrm{Tr}((\varphi^{(2)})^m)$ を計算すればよい。

Theorem 6 (Lefschetz の不動点定理)

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

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

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

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

参考文献