ピタゴラス数に対するフライ曲線の Mordell-Weil 群について

八木 颯仁

慶應義塾大学 栗原研究室 修士 1 年

January 31, 2025

発表の内容と動機

フライ曲線とは楕円曲線の一種であり、フェルマーの最終定理の証明において重要な役割を果たした。フライ曲線はフェルマー方程式の解に対応して定まる「存在しない」曲線である。私はフライ曲線の方程式を少し変形し、ピタゴラス数に対して定まる「存在する」楕円曲線について研究し、その Mordell-Weil 群（後で定義を与える）の構造について**独自の結果を得た**。

- 楕円曲線とは
- フライ曲線とは
- Torsion subgroup
- ランク
- 具体例

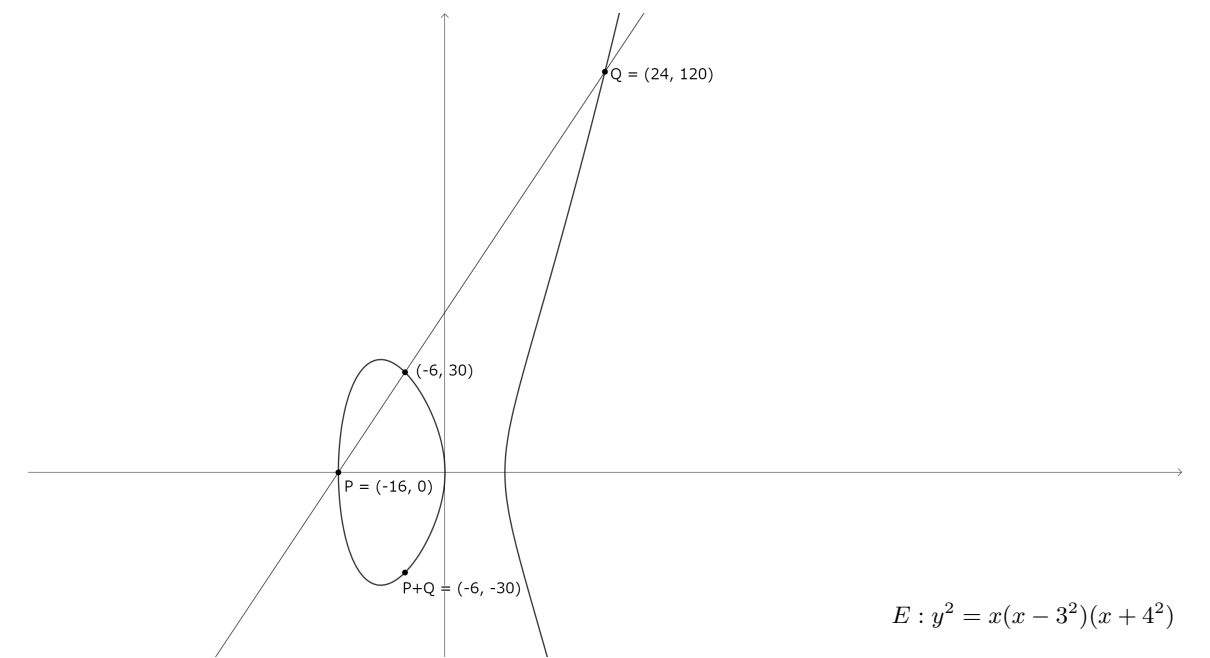
楕円曲線とは

$\mathbb{Q}$ 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。

$$E : y^2 = x^3 + ax^2 + bx + c \quad (a, b, c \in \mathbb{Q}). \tag{1}$$

ただし右辺は $\overline{\mathbb{Q}}$ において重根を持たないとする。

$P, Q \in E$ とし、L を P と Q を通る直線とするとき L と E は重複度を込めてちょうど 3 点で交わる。そこで L と E のもう 1 つの交点を R とし、R と x 軸について対称な点を $P + Q$ と定義する。
E 上の有理点全体に無限遠点 $\mathcal{O}$ を加えた集合を **Mordell-Weil 群**と呼び、$E(\mathbb{Q})$ と書く。$E(\mathbb{Q})$ は上の演算により $\mathcal{O}$ を単位元としてアーベル群をなす。



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

楕円曲線とは

Theorem 1 (Mordell)

$E(\mathbb{Q})$ は有限生成アーベル群であり, したがって次のように書ける。

$$E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E(\mathbb{Q})_{\mathrm{tors}}. \tag{2}$$

ただし $E(\mathbb{Q})_{\mathrm{tors}}$ は $E(\mathbb{Q})$ の元のうち位数が有限のもの全体の集合である。
r を $E(\mathbb{Q})$ の**ランク**、$E(\mathbb{Q})_{\mathrm{tors}}$ を **torsion subgroup** と呼ぶ。

Theorem 2 (Mazur)

$E(\mathbb{Q})_{tors}$ は次のいずれかに同型である。

$$\begin{aligned} &(1) \quad \mathbb{Z}/n\mathbb{Z} && (1 \leq n \leq 10 \text{ もしくは } n = 12), \\ &(2) \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} && (1 \leq n \leq 4). \end{aligned} \tag{3}$$

フライ曲線とは

フェルマー方程式

$$x^n + y^n = z^n, \quad xyz \neq 0, \quad n \geq 3 \tag{4}$$

の解 $(x, y, z) = (a, b, c)$ に対し、

$$y^2 = x(x - a^n)(x + b^n) \tag{5}$$

は楕円曲線を与える。これを**フライ曲線**と呼ぶ。

(a, b, c) を以下を満たす有理数の 3 つ組であるとする。

$$a^2 + b^2 = c^2, \quad abc \neq 0. \tag{6}$$

次の方程式で与えられる楕円曲線 $E/\mathbb{Q}$ を、**ピタゴラス数に対するフライ曲線**と呼ぶことにする。

$$E : y^2 = x(x - a^2)(x + b^2) = x^3 + (b^2 - a^2)x^2 - a^2b^2x. \tag{7}$$

フライ曲線とは

互いに素な正の整数 a_0, b_0, c_0 が $a_0^2 + b_0^2 = c_0^2$ を満たすとき、(a_0, b_0, c_0) を原始ピタゴラス数と呼ぶ。
(6) を満たす有理数の 3 つ組 (a, b, c) に対し、$s \in \mathbb{Q}^\times$ と原始ピタゴラス数 (a_0, b_0, c_0) が存在し、

$$(a, b, c) = (sa_0, sb_0, sc_0) \tag{8}$$

と書ける。$(x, y) \mapsto (s^{-2}x, s^{-3}y)$ という変換により $y^2 = x(x - a^2)(x + b^2)$ は

$$Y^2 = X(X - a_0^2)(X + b_0^2) \tag{9}$$

に $\mathbb{Q}$ 上同型である。したがってこの後の証明中では (a, b, c) が原始ピタゴラス数であると仮定して一般性を失わない。

Torsion subgroup

ピタゴラス数に対するフライ曲線について**独自に以下の結果を得た**。

Theorem 3

$E/\mathbb{Q}$ をピタゴラス数に対するフライ曲線とするとき以下が成り立つ。

$$\begin{aligned} E(\mathbb{Q})_{\mathrm{tors}} &= \{\mathcal{O}, (0,0), (a^2,0), (-b^2,0), (a^2+ac, \pm ac(a+c)), (a^2-ac, \pm ac(a-c))\} \\ &= \langle (0,0), (a^2+ac, ac(a+c)) \rangle \\ &\simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}. \end{aligned} \tag{10}$$

- 定義よりすぐに「$P = (x,y) \in E(\mathbb{Q})$の位数が2 $\iff$ $y = 0$」は分かる。
- 楕円曲線の演算は幾何的に定義したが、係数を使って具体的に書けることが知られており、

$$x(2P) = \frac{a^4b^4 + 2a^2b^2x^2 + x^4}{4x(x-a^2)(x+b^2)} = a^2 \tag{11}$$

という方程式を解くことで 4-torsion points も具体的に求めることができた。

Theorem 3 の証明

Theorem 2 (Mazur, 再掲)

$E(\mathbb{Q})_{\text{tors}}$ は次のいずれかに同型である。

$$\begin{aligned} &(1) \quad \mathbb{Z}/n\mathbb{Z} && (1 \leq n \leq 10 \text{ もしくは } n = 12), \\ &(2) \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} && (1 \leq n \leq 4). \end{aligned} \tag{12}$$

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \subset E(\mathbb{Q})_{\text{tors}}$ が分かった時点で、$E(\mathbb{Q})_{\text{tors}}$ の可能性は

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \quad \text{または} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \tag{13}$$

のいずれかに絞られる。したがってあとは 8-torsion points が存在しないことを示せばよい。

8-torsion points が存在すると仮定すると、以下の方程式が非自明な整数解を持つことが示せる。

$$x^4 + y^2 = z^4. \tag{14}$$

しかしこの方程式は非自明な整数解を持たないことが知られている [1]。

ランク

Theorem 4 $((a,b,c)=(3,4,5))$

次の楕円曲線

$$E: y^2 = x(x-3^2)(x+4^2) = x^3+7x^2-144x \tag{15}$$

の Mordell-Weil 群 $E(\mathbb{Q})$ は

$$E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \tag{16}$$

となる。特にランクは 0 である。

Theorem 5 $((a,b,c)=(15,8,17))$

次の楕円曲線

$$E: y^2 = x(x-15^2)(x+8^2) = x^3-161x^2-14400x \tag{17}$$

の Mordell-Weil 群 $E(\mathbb{Q})$ は

$$E(\mathbb{Q}) \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \tag{18}$$

となる。特にランクは 1 である。

ランク

- 一般的にランクを求めるのは難しい（アルゴリズムは知られていない）。
- いつでも使えるわけではないが Silverman の教科書 [2] で紹介されている手法を紹介する。

$\mathbb{Q}$ 上の楕円曲線 $E : y^2 = x^3 + Ax^2 + Bx$ に対し、

$$\begin{aligned} S &:= \{\infty, 2\} \cup \{p : \text{素数} \mid v_p(\Delta) \geq 1\}, \\ \mathbb{Q}(S,2) &:= \left\{ b \in \mathbb{Q}/\mathbb{Q}^{\times 2} \mid \forall p \notin S, v_p(b) \equiv 0 \pmod 2 \right\} \end{aligned} \tag{19}$$

とおき、

$$\phi : E \to E', \quad \hat{\phi} : E' \to E, \quad \hat{\phi} \circ \phi = [2] \quad (2 \text{ 倍写像}) \tag{20}$$

なる楕円曲線 $E'/\mathbb{Q}$ と ϕ : 2-isogeny（具体的な与え方は省略）を考えて

$$\begin{aligned} C_d &: dw^2 = d^2 - 2Adz^2 + (A^2 - 4B)z^4 : \quad \text{Homogeneous space} \\ S^{(\phi)}(E/\mathbb{Q}) &:= \{d \in \mathbb{Q}(S,2) \mid \forall v \in S, C_d(\mathbb{Q}_v) \neq \varnothing\} : \quad \text{Selmer 群} \end{aligned} \tag{21}$$

と定義する。

$$\#S < \infty, \quad \#\mathbb{Q}(S,2) < \infty \tag{22}$$

ランク

次の完全系列が存在する。

$$0 \to E'(\mathbb{Q})/\phi(E(\mathbb{Q})) \xrightarrow{\delta} S^{(\phi)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[\phi] \to 0 \tag{23}$$

$S^{(\phi)}(E/\mathbb{Q})$ が求まり、運良く δ が全射であれば $E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ が求まる。
$E'(\mathbb{Q})/\phi(E(\mathbb{Q}))$ と、E と E' を入れ替えて同様の計算をすることで $E(\mathbb{Q})/\hat{\phi}(E'(\mathbb{Q}))$ が求まったとする。このとき以下の完全系列

$$\frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} \xrightarrow{\hat{\phi}} \frac{E(\mathbb{Q})}{2E(\mathbb{Q})} \to \frac{E(\mathbb{Q})}{\hat{\phi}(E'(\mathbb{Q}))} \to 0. \tag{24}$$

より運が良ければ $E(\mathbb{Q})/2E(\mathbb{Q})$ が求まる。したがって $E(\mathbb{Q})$ の生成元の数が分かる。ピタゴラス数に対するフライ曲線の torsion subgroup の生成元の数は 2 であると分かっていたのでランクも求まる。

Theorem 4 の証明

$$S = \{\infty, 2, 3, 5\}, \quad \mathbb{Q}(S, 2) = \{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30\}, \tag{25}$$

$$S^{(\phi)}(E/\mathbb{Q}) \coloneqq \{d \in \mathbb{Q}(S, 2) \mid \forall v \in S, C_d(\mathbb{Q}_v) \neq \varnothing\}. \tag{26}$$

たとえば $d = 5$ に対して、

$$C_5 : w^2 = 5 - 14z^2 + 125z^4 \tag{27}$$

は $\mathbb{Q}_3$ 上で解を持たない（分母を払った上で $\bmod 3$ で解を持たないというのと同じような意味である）ので $5 \notin S^{(\phi)}(E/\mathbb{Q})$ である。実際 z の 3 進付値が負 (分母が 3 で割り切れる) とすると、分母を払って

$$1 \equiv w'^2 \equiv 125z'^4 \equiv 2 \pmod 3 \tag{28}$$

となり矛盾。一方 $z \in \mathbb{Z}$ のとき

$$\begin{aligned} z \equiv 0 \pmod 3 \quad &\Rightarrow \quad w^2 \equiv 5 \equiv 2 \pmod 3, \\ z \equiv \pm 1 \pmod 3 \quad &\Rightarrow \quad w^2 \equiv 5 - 14 + 125 \equiv 2 \pmod 3 \end{aligned} \tag{29}$$

でありやはり矛盾。
これをすべての $d \in \mathbb{Q}(S, 2)$ について計算し、さらに E と E' を入れ替えて同様の計算をする。

Theorem 5 の証明

$(a, b, c) = (15, 8, 17)$ のときは

$$
\begin{aligned}
S &= \{\infty, 2, 3, 5, 17\}, \\
\mathbb{Q}(S, 2) &= \{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 17, \pm 30, \pm 34, \pm 51, \pm 85, \pm 102, \pm 170, \pm 255, \pm 510\}\,,
\end{aligned} \tag{30}
$$

$$
S^{(\phi)}(E/\mathbb{Q}) \coloneqq \{d \in \mathbb{Q}(S, 2) \mid \forall v \in S, C_d(\mathbb{Q}_v) \neq \varnothing\}\,. \tag{31}
$$

とさらに d の候補が増えて、非常に多くの計算が必要になる。

今後の展望

- ピタゴラス数に対するフライ曲線でランクが 0 のものは無限個存在するか？
- ピタゴラス数に対するフライ曲線でランクが 1 のものは無限個存在するか？
- ピタゴラス数に対するフライ曲線でランクが 2 以上のものは存在するか？

30 個程の原始ピタゴラス数に対しデータベース [**?**] で確認した中では、ランクは 0 と 1 のものしか出てこなかった。

- ランクが 0 になる (a, b, c) の十分条件を与えることはできるか？
- 他のピタゴラス数に付随する楕円曲線の族についてはどうか？

たとえば

$$E : y^2 = x(x - a^2)(x - b^2) \tag{32}$$

のランクは常に 1 以上であることが知られている [3]。a, b に条件を付けることにより、ランクが 2 以上のものも無限個存在することが分かっている [4]。

参考文献

[1] J. H. Silverman.
The arithmetic of elliptic curves.
Graduate texts in mathematics ; 106. Springer, 2nd ed. edition, 2009.

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

[3] K. Kodaira.
On compact analytic surfaces, iii.
Annals of Mathematics, Vol. 78, No. 1, pp. 1–40, 1963.

[4] T. Yoshida.
The relationship between face cuboids and elliptic curves, 2024.