A unique pair of triangles

慶應義塾大学大学院 理工学研究科 基礎理工学専攻
松村英樹 (Hideki Matsumura)

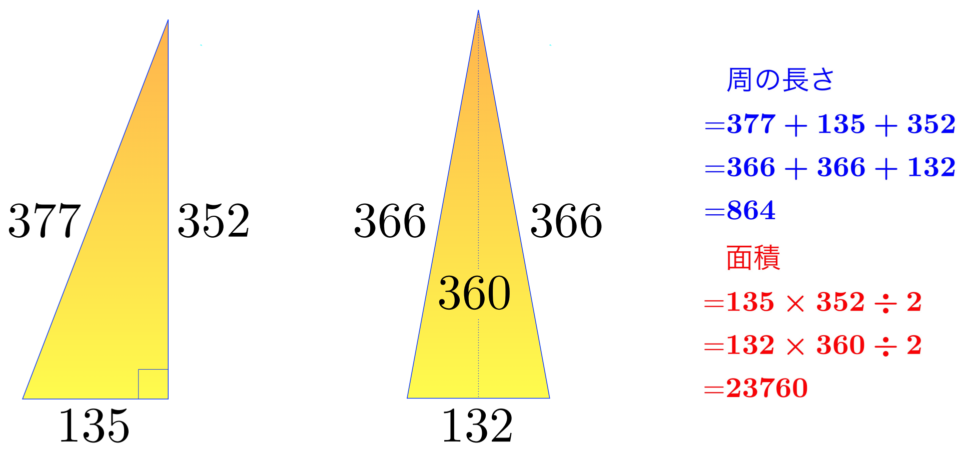
概要

「辺の長さと面積が全て有理数であるような三角形」を有理三角形と呼ぶ．この発表では，「有理直角三角形と有理二等辺三角形の組の中には，周の長さ同士が等しく，また面積同士も等しい組が相似を除いてただ 1 組しか存在しない」という定理を紹介する．この定理の証明は，超楕円曲線上の有理点集合の決定に帰着される．超楕円曲線上の有理点集合を決定する際，Chabauty-Coleman 法と降下法が中心的な役割を果たす．また，降下法は MAGMA を用いて実行される．本研究は平川義之輔氏との共同研究である．本稿の前半では定理の証明の概略を述べ，後半では降下法のアイデアを説明する．

1　主定理

古代ギリシャ時代以来，何人もの数学者達が「辺の長さと面積が全て有理数であるような三角形」を探求してきた．このような三角形を「有理三角形」と呼ぶ．数論的な観点から，周の長さと面積は有理三角形の基本的な不変量であり，有理三角形を周の長さと (または) 面積で分類するという問題が考えられてきた．例えば，周の長さ同士が等しく，また面積同士も等しい有理三角形の組が無限に多く構成されている ([Bre06], [vL07] やその参考文献を参照)．本稿で紹介する定理は次の通りである．

定理 1.1 ([HM19, Theorem 1.1])**.** 周の長さ同士が等しく，また面積同士も等しい有理直角三角形と有理二等辺三角形の組は相似を除いて以下の組しかない．



この定理の証明は種数 2 の超楕円曲線の有理点集合の決定に帰着される．超楕円曲線の有理点集合の決定には, 以下の **Chabauty-Coleman 法**を用いる．

定理 1.2 (Chabauty-Coleman 法, [Cha41], [Col85], [MP12, Theorem 5.3 (b)])**.** C を $\mathbb{Q}$ 上の種数 $g \geq 2$ の曲線[*1]とし, J を C の Jacobi 多様体, p を素数とする．C が $p > 2g$ で良い還元を持ち, **$J(\mathbb{Q})$ の Mordell-Weil rank** [*2]**が g より小さい**とき, 以下の不等式が成立する．

$$\#C(\mathbb{Q}) \leq \#C(\mathbb{F}_p) + (2g-2).$$

有理三角形に関する先行研究はいくつかあるが, 筆者の知る限り, 超楕円曲線の理論を使う研究は [ZP17] のみである．ここでは周の長さ同士が等しく, また面積同士も等しい有理二等辺三角形とある条件を満たす有理菱形の組が存在しない事が証明されている．

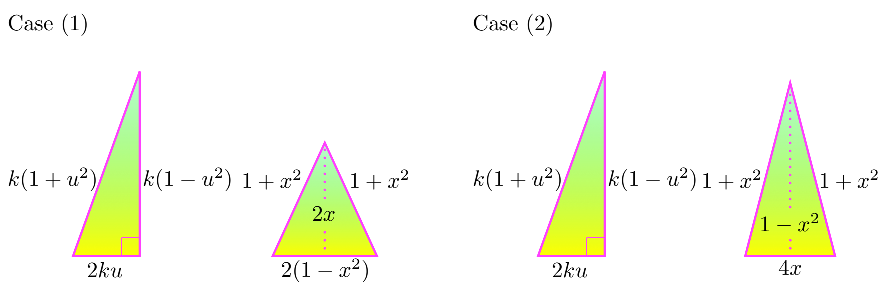
注意 1.3. (1) 周の長さ同士が等しく, また面積同士も等しい直角三角形[*3] の組は全て合同な組である．

(2) 周の長さ同士が等しく, また面積同士も等しい合同でない有理二等辺三角形の組は相似を除いて無限に多く存在する．

2　証明の概略

定理 *1.1* の証明．Step (1): 三角形の組を全て超楕円曲線でパラメータ付けする．

Pythagoras の定理と素因数分解の一意性より, 三角形の組の辺の長さはある正の有理数 x, u, k を用いて以下のように表される事が分かる．



Case (1) では以下の連立方程式を得る．

$$\begin{cases} k + ku = 2 \\ k^2 u(1-u^2) = 2x(1-x^2). \end{cases}$$

[*2] $\mathbb{Q}$ 上の曲線とは Spec($\mathbb{Q}$) 上の 1 次元の滑らかな射影幾何的整 scheme の事である．

[*2] 有理点を持つ曲線の有理点集合は Jacobi 多様体という代数多様体の有理点集合に埋め込める．Jacobi 多様体の有理点集合は有限生成 Abel 群をなす (Mordell-Weil 群)．この Mordell-Weil 群の rank を Mordell-Weil rank という．

[*3] 有理直角三角形とは限らない．

1 番目の方程式より, $u = 2/k - 1$ を得る. これを 2 番目の方程式に代入して整理すると, k に関する 2 次方程式

$$2k^2 - (x^3 - x + 6)k + 4 = 0$$

を得る. k は有理数なので, 左辺の判別式はある有理数 y を用いて y^2 と表される. すなわち,

$$y^2 = (x^3 - x + 6)^2 - 32$$

を得る. C をこの方程式で定義される affine 曲線の滑らかな compact 化とすると, これは超楕円曲線を定める. 無限遠点 2 点と $(x, y) = (0, \pm 2), (1, \pm 2), (-1, \pm 2), (5/6, \pm 217/216)$ は C の有理点である. 最初の 8 点は三角形の組に対応しない*4 . さらに, $(x, y) = (5/6, 217/216)$ と $(5/6, -217/216)$ より, それぞれ $(k, u, x) = (27/16, 5/27, 5/6)$ と $(32/27, 11/16, 5/6)$ を得る. ここから, 定理の三角形の組が得られる.

Step (2): Step (1) を踏まえると, あとは $\#C(\mathbb{Q}) \leq 10$ を示せば良い事が分かる. 実際, 以下のように $\#C(\mathbb{Q}) \leq 10$ を証明できる.

C の種数は 2 であり, $p = 5$ で良い還元を持ち, $\#C(\mathbb{F}_5) = 8$ となる. また, **降下法**より, C の Jacobi 多様体の $\mathbb{Q}$ 上の Mordell-Weil rank は 1 以下である事が分かる*5. 従って, **Chabauty-Coleman 法** (定理 1.2) より, 所望の不等式 $\#C(\mathbb{Q}) \leq 10$ を得る.

Case (2) も同様に, 超楕円曲線*6 の有理点集合の決定に帰着されるが, この超楕円曲線の有理点に対応する三角形の組は存在しない事が分かる. □

3 降下法のアイデア

Chabauty-Coleman 法における Mordell-Weil rank の条件を示すために, **降下法**を用いて **Mordell-Weil rank r を上から抑える**. 降下法の計算は, ある特定の代数体の**イデアル類群**や**単数群**という, より古典的な数論的不変量の計算に帰着される. この節では, [FPS97], [PS97], [Sto01] による降下法のアイデアを説明する*7. 以下, C を $y^2 = f(x)$ で定義される $\mathbb{Q}$ 上の超楕円曲線, $\deg f = 6$ とし, J を C の Jacobi 多様体とする.

(1) $J(\mathbb{Q})$ は有限生成 Abel 群なので, $r = \dim_{\mathbb{F}_2} J(\mathbb{Q})/2J(\mathbb{Q}) - \dim_{\mathbb{F}_2} J(\mathbb{Q})[2]$ となる. 2-ねじれ部分 $J(\mathbb{Q})[2]$ の次元は容易に計算できる. 我々の超楕円曲線 C の場合は, $\dim_{\mathbb{F}_2} J(\mathbb{Q})[2] = 1$ である. 次に, $J(\mathbb{Q})/2J(\mathbb{Q})$ の次元を上から抑える.

(2) $J(\mathbb{Q})/2J(\mathbb{Q})$ から $J(\mathbb{Q})/\mathrm{Ker}(x - T)$ という $\mathbb{F}_2$ ベクトル空間へ全射が存在し, その核は 0 または $\mathbb{F}_2$ である (cf. [FPS97, Proposition 5]) *8. 我々の超楕円曲線 C の場合は $J(\mathbb{Q})/2J(\mathbb{Q})$ と $J(\mathbb{Q})/\mathrm{Ker}(x - T)$ は同型であるので, $\dim_{\mathbb{F}_2} J(\mathbb{Q})/2J(\mathbb{Q}) = \dim_{\mathbb{F}_2} J(\mathbb{Q})/\mathrm{Ker}(x - T)$ となる.

(3) また, $J(\mathbb{Q})/\mathrm{Ker}(x - T)$ は **fake 2-Selmer 群**という $\mathbb{F}_2$ ベクトル空間に埋め込める*9. よっ

*4 実際, $(x, y) = (0, \pm 2)$ のとき, 二等辺三角形の高さ $2x$ が 0 となり, $(x, y) = (1, \pm 2), (-1, \pm 2)$ のとき, 二等辺三角形の底辺の長さ $2(1 - x^2)$ が 0 となる.

*5 Magma Calculator を用いた. 実際には, Mordell-Weil rank が 1 である事も分かる.

*6 C と同型である.

*7 この節の内容は C が有理点を持たない場合にも成り立つ.

*8 $x - T$ 写像の定義は後述.

*9 Fake 2-Selmer 群の定義は後述.

て, $\dim_{\mathbb{F}_2} J(\mathbb{Q})/\mathrm{Ker}(x-T) \le \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ となる.

(4) 以上より, $\boldsymbol{r \le \dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) - \dim_{\mathbb{F}_2} J(\mathbb{Q})[2]}$ となる.

我々の超楕円曲線 C の場合は, $\dim_{\mathbb{F}_2} \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) = 2$ なので, $\boldsymbol{r \le 1}$ である事が証明できる.

$$\begin{tikzcd}
0 \arrow[r] & 0 \text{ or } \mathbb{F}_2 \arrow[r] & J(\mathbb{Q})/2J(\mathbb{Q}) \arrow[r] \arrow[d, hook] & J(\mathbb{Q})/\mathrm{Ker}(x-T) \arrow[r] \arrow[d, hook] & 0 \\
0 \arrow[r] & 0 \text{ or } \mathbb{F}_2 \arrow[r] & \mathrm{Sel}^{(2)}(\mathbb{Q}, J) \arrow[r] & \mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) \arrow[r] & 0.
\end{tikzcd}$$

注意 3.1. (1) Fake 2-Selmer 群の計算は, $f(x)$ の既約因子の分解体の**イデアル類群**や**単数群**という, より古典的な不変量の計算に帰着される. 現在, 降下法は計算代数システム MAGMA に実装されている.

(2) 2-Selmer 群から fake 2-Selmer 群へ全射が存在し, その核も 0 または $\mathbb{F}_2$ である (cf. [PS97, Theorem 13.2]). 我々の超楕円曲線 C の場合は $\mathrm{Sel}^{(2)}(\mathbb{Q}, J)$ と $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ は同型である.

Mordell-Weil rank を上から抑えるためには, $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ の次元を計算できれば十分である. 以下, $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ を集合として明示するアイデアを述べる.

まず, $x-T$ 写像を定義する.

定義と命題 3.2 (cf. [FPS97, Proposition 1, 2])**.** K を $\mathbb{Q}$ の拡大体, $L_K := K[T]/(f(T))$ とする. $J(K)$ の代表元をうまく取る事により, 次の写像が well-defined な群準同型写像になる.

$$\begin{array}{cccc}
x-T: & J(K) & \xrightarrow{f} & \mathrm{Ker}(N_K : L_K^\times/{L_K^\times}^2 K^\times \to K^\times/{K^\times}^2) \\
 & \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\
 & [D := \Sigma_P n_P P] & \longmapsto & \prod_P (x_P - T)^{n_P}
\end{array}$$

ここで, N_K はノルム写像から誘導される写像, x_P は P の x 座標である.

$J(\mathbb{Q})/\mathrm{Ker}(x-T)$ の次元を上から抑えるために, $J(\mathbb{Q})/\mathrm{Ker}(x-T)$ を fake 2-Selmer 群に埋め込み, fake 2-Selmer 群を集合として明示する.

$L := \mathbb{Q}[T]/(f(T))$, $L_{\mathbb{Q}_p} := \mathbb{Q}_p[T]/(f(T))$, $S := \{p \in \mathbb{Z} : 素数 \mid p は f の判別式を割る \} \cup \{2, \infty\}$ とすると, 次の図式は可換である.

$$\begin{tikzcd}
0 \arrow[r] & J(\mathbb{Q})/\mathrm{Ker}(x-T) \arrow[r, "x-T"] \arrow[d] & L^\times/{L^\times}^2\mathbb{Q}^\times \arrow[d, "\prod_{p \in S} \mathrm{res}_p"] \\
0 \arrow[r] & \prod_{p \in S} J(\mathbb{Q}_p)/\mathrm{Ker}(x-T)_p \arrow[r, "\prod_{p \in S}(x-T)_p"'] & \prod_{p \in S} {L_{\mathbb{Q}_p}}^\times/{L_{\mathbb{Q}_p}}^{\times 2}{\mathbb{Q}_p}^\times.
\end{tikzcd}$$

水平方向の写像は $x-T$ 写像から誘導され, 垂直方向の写像は対角写像である.

f を $f = f_1 \cdots f_m$ と $\mathbb{Q}$ 上の既約多項式の積に分解し, $L_i := \mathbb{Q}[T]/(f_i(T))$ とおく. また, α_i を以

下のように自然な商写像が誘導する同型を通じて定義される L_i の元とする.

$$\begin{array}{ccc} L = \mathbb{Q}[T]/(f(T)) & \simeq & \prod_i L_i \\ \cup & & \cup \\ \alpha & \longmapsto & (\alpha_i) := (\alpha)_i. \end{array}$$

定義 3.3. (1) $\alpha \in L^\times$ とする. この時, α が S の外不分岐であるとは, 任意の $1 \leq i \leq m$ に対し, $L_i(\sqrt{\alpha_i})/L_i$ が S の上の素イデアルの外で不分岐拡大になる事である.

(2) $\alpha \in L^\times/L^{\times 2}$ とする. この時, α が S の外不分岐であるとは, α の代表元が S の外不分岐である事である[*10].

(3) $L^\times/L^{\times 2}$ の $\mathbb{F}_2$-部分ベクトル空間 H を次のように定義する.

$$H := \{\alpha \in L^\times/L^{\times 2} \mid \alpha \text{ は } S \text{ の外不分岐 }\}.$$

(4) H' を H の $L^{\times 2}/L^{\times 2}\mathbb{Q}^\times$ における像とする.

(5) **fake 2-Selmer 群**を以下のように定義する.

$$\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J) := \{\alpha \in H' \mid \Pi_{p\in S}\mathrm{res}_p(\alpha) \in \mathrm{Im}(\Pi_{p\in S}(x-T)_p)\} \cap \mathrm{Ker}(N_{\mathbb{Q}}).$$

命題 3.4 ([FPS97, Proposition 3])**.** $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ は $\mathrm{Im}(x-T)(\simeq J(\mathbb{Q})/\mathrm{Ker}(x-T))$ を含む H' の $\mathbb{F}_2$-部分ベクトル空間である.

従って, $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ を集合として明示する事で, $J(\mathbb{Q})/\mathrm{Ker}(x-T)$ の次元を上から抑える事ができる. H を集合として明示できれば, H' を集合として明示できる. また, $\mathrm{Ker}(N_{\mathbb{Q}})$ や $x-T$ 写像の像も集合として明示できるので (cf. [Sto01]), $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(\mathbb{Q}, J)$ を集合として明示でき, Mordell-Weil rank の具体的な上界が得られる. 最後に, H を集合として明示するアイデアを述べる.

$I(L_i)$ を L_i の分数イデアルのなす群, $I(L) := \prod_{i=1}^m I(L_i)$ とし, 素数 $p \in \mathbb{Z}$ に対し, $I_p(L) := \prod_{i=1}^m I_p(L_i)$, $I_p(L_i) := < p$ の上の L_i の素イデアル $>_{\mathbb{Z}}$, $I^S(L) := I(L)/\prod_{p\in S} I_p(L)$ とおくと, 次のような図式が存在する.

$$\begin{tikzcd}
 & \mathcal{O}_L[\frac{1}{S}]^\times \arrow[r] \arrow[d] & \mathcal{O}_L[\frac{1}{S}]^\times \arrow[r] \arrow[d] & H \arrow[d] & \\
 & L^\times \arrow[r, "2"] \arrow[d] & L^\times \arrow[r] \arrow[d] & L^\times/L^{\times 2} \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & I^S(L) \arrow[r, "2"] \arrow[d] & I^S(L) \arrow[r] \arrow[d] & I^S(L)/I^S(L)^2 \arrow[r] & 0 \\
 & I^S(L)/L^\times \arrow[r] & I^S(L)/L^\times & &
\end{tikzcd}.$$

[*10] この概念は α の $L^\times/L^{\times 2}$ における像のみに依存しており, well-defined である.

蛇の補題より, 次のような短完全列が存在する.

$$1 \to \mathcal{O}_L \left[\frac{1}{S}\right]^{\times} / \mathcal{O}_L \left[\frac{1}{S}\right]^{\times 2} \to H \to (I^S(L)/L^{\times})[2] \to 0.$$

H の両側の $\mathbb{F}_2$ ベクトル空間は集合として明示できる[*11] ので, H も集合として明示できる.

謝辞

発表の機会をくださった「第 15 回数学総合若手研究集会」の世話人の皆様に感謝申し上げます.

参考文献

[Bre06] Andrew Bremner, *On Heron triangles*, Ann. Math. Inform. **33** (2006), 15–21. MR2385463

[Cha41] Claude Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885 (French). MR0004484

[Col85] Robert F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770, DOI 10.1215/S0012-7094-85-05240-8. MR808103

[FPS97] E. V. Flynn, Bjorn Poonen, and Edward F. Schaefer, *Cycles of quadratic polynomials and rational points on a genus-2 curve*, Duke Math. J. **90** (1997), no. 3, 435–463, DOI 10.1215/S0012-7094-97-09011-6. MR1480542

[HM19] Yoshinosuke Hirakawa and Hideki Matsumura, *A unique pair of triangles*, J. Number Theory **194** (2019), 297–302, DOI 10.1016/j.jnt.2018.07.007. MR3860476

[MP12] William McCallum and Bjorn Poonen, *The method of Chabauty and Coleman*, Explicit methods in number theory, Panor. Synthèses, vol. 36, Soc. Math. France, Paris, 2012, pp. 99–117 (English, with English and French summaries). MR3098132

[PS97] Bjorn Poonen and Edward F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math. **488** (1997), 141–188, DOI 10.1515/crll.1997.488.141. MR1465369

[Sto01] Michael Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277, DOI 10.4064/aa98-3-4. MR1829626

[vL07] Ronald van Luijk, *An elliptic $K3$ surface associated to Heron triangles*, J. Number Theory **123** (2007), no. 1, 92–119, DOI 10.1016/j.jnt.2006.06.006. MR2295433

[ZP17] Yong Zhang and Junyao Peng, *Heron triangle and rhombus pairs with a common area and a common perimeter*, Forum Geom. **17** (2017), 419–423. MR3733032

[*11] S-単数群 $\mathcal{O}_L[\frac{1}{S}]^{\times}$ が有限生成なので $\mathcal{O}_L[\frac{1}{S}]^{\times}/\mathcal{O}_L[\frac{1}{S}]^{\times 2}$ は有限であり, イデアル類群の有限性より $L^{\times}/I^S(L)[2] \subset \mathrm{Cl}[2]$ も有限である. これらの計算方法は古典的に知られている.