角の二等分線の傾きに関する不定方程式とペル方程式の有理数解の構造

廣津 孝

2023 年 5 月 1 日 (Ver. 7.3)

概要

座標平面において 2 直線の傾き a, b とそれらのなす角の二等分線の傾き c は, 不定方程式 $(a-c)^2(b^2+1) = (b-c)^2(a^2+1)$ を満たす. 最近, この方程式のすべての非自明な整数解をネガティブなペル方程式の整数解を用いて表す公式 [4, Theorem 1] が発見された. 本稿では, 方程式 $|x^2-dy^2| = 1$ の有理数解を $\mathbb{Q}(\sqrt{d})$ の基本単数と $|x^2-dy^2| = p^n$ (p: 素数, n: 正整数) の基本解を用いて記述し, その応用として上記の方程式の有理数解の構造を決定する.

1 はじめに

座標平面上の 2 直線とそれらがなす角の二等分線の傾きについて, 次のような問題が考えられる.

問題 1. どのような有理数 a, b に対して, 傾きが a, b である 2 直線のなす角の二等分線の傾き c は有理数になるか.

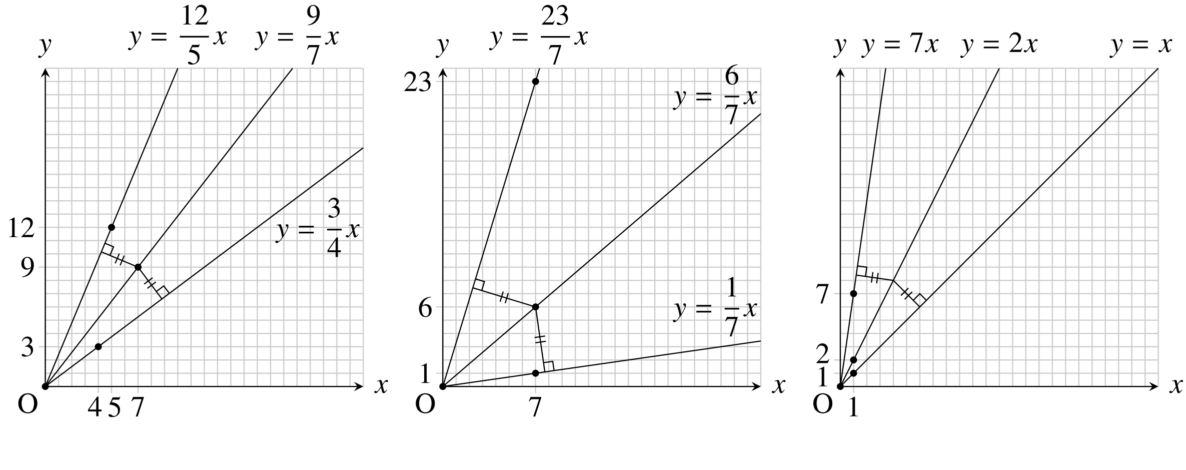
注意 1. 2 直線のなす角は鈍角を含めて考える. 2 直線のなす角と補角の二等分線は互いに垂直であり, 座標軸に平行でなければ, 傾きの積は -1 で, 一方の傾きが有理数であれば他方も有理数である.

この問題は,「与えられた格子点 O, A, B に対して, 2 直線 OA, OB のなす角の二等分線が O と他の格子点 C を結ぶことで描けるのはいつか」という意味をもち, 描画の技術上重要な問題である. また, 工学では, この問題の解を用いて, 光の放射範囲と放射軸を数値計算による誤差が生じないように整数の比で指定するという応用も考えられる. 問題 1 は, 方程式

$$(a-c)^2(b^2+1) = (b-c)^2(a^2+1) \tag{$\star$}$$

の有理数解を求める問題に帰着される ([4, Proposition 1]). ($\star$) の $b = \pm a$ なる解 (a, b, c) を**自明解**と呼ぶ.

例 1. $(a, b, c) = (3/4, 12/5, 9/7)$, $(1/7, 23/7, 6/7)$, $(1, 7, 2)$ は ($\star$) を満たすから, $(a, b) = (3/4, 12/5)$, $(1/7, 23/7)$, $(1, 7)$ は問題 1 の解である (図を参照).



問題 1 を解く上で, 次の命題が非常に重要な役割を果たす (証明は第 3 節で述べる).

命題 1. ($\star$) の任意の非自明な有理数解は, 平方因数をもたない適当な整数 $d \geqq 1$ に対して

$$x^2 - dy^2 = -1$$

の有理数解 $(x, y) = (a, a'), (b, b')$ を用いて

$$(a, b, c) = \left(a, b, \frac{ab' + a'b}{b' + a'}\right), \left(a, b, \frac{ab' - a'b}{b' - a'}\right)$$

の形に表される.

定義 1. $d > 1$ を平方因数をもたない整数, $c \geqq 1$ を整数とする.

(1) $|x^2 - dy^2| = c$ の正整数解 $(x, y) = (x_1, y_1), (x_2, y_2)$ に対して, $x_1 + y_1\sqrt{d} < x_2 + y_2\sqrt{d}$ が成り立つとき, (x_1, y_1) は (x_2, y_2) より小さい, (x_2, y_2) は (x_1, y_1) より大きいという.

(2) $|x^2 - dy^2| = c$ の整数解 (x, y) で x, dy が互いに素 (つまり x, d も x, y も互いに素) であるものが存在するとき, (x, y) は**原始的** (primitive) であるという.

(3) $c = 1$ または $c = p^n$ (p: 素数, n: 正整数) のとき, $x^2 - dy^2 = c$, $x^2 - dy^2 = -c$, $|x^2 - dy^2| = c$ の各方程式に対して, 原始的な正整数解のうち最小の解を**基本解** (fundamental solution) と呼ぶ.

注意 2. • $|x^2 - dy^2| = 1$ の任意の整数解は, 原始的である.

• p を素数, n を正整数とする. $|x^2 - dy^2| = p^n$ の整数解 (x, y) が原始的であることと, d, x, y がすべて p の倍数でないことは同値である. よって, p が d の素因数でないとき, $|x^2 - dy^2| = p$ は原始的でない整数解をもたない.

筆者により, ペル方程式の整数解の性質, 特に整除性の判定法を用いた議論によって, ($\star$) の整数解は, 次のように表されることが示されている.

定理 1 ([4, Theorem 1])**.** ペル方程式 $x^2 - dy^2 = -1$ が整数解をもつような, 平方因数をもたない整数 $d > 1$ に対して, $|x^2 - dy^2| = 1$ の n 番目に小さい正整数解を $(x, y) = (x_n^{(d)}, y_n^{(d)})$ とおく. ($\star$) の任意の非自明な整数解 (a, b, c) は, a, b の入れ替えを許せば, 適当な正整数 d, m, n に対して

$$(a, b, c) = \pm\left(x^{(d)}_{(2m-1)(2n-1)}, x^{(d)}_{(2m-1)(2n+1)}, \frac{y^{(d)}_{2(2m-1)n}}{y^{(d)}_{2m-1}}\right), \tag{1.1}$$

$$\pm\,(x^{(2)}_{2n-1}, -x^{(2)}_{2n+1}, x^{(2)}_{2n}) \tag{1.2}$$

の形に表され, この形の (a, b, c) で ($\star$) の整数解でないものはない. ただし, (1.1) は $d = 2$ の場合を含む.

以下, 次の記法を用いる.

記法 1. $d > 1$ を平方因数をもたない整数とする. 実 2 次体 $K = \mathbb{Q}(\sqrt{d})$ の基本単数を η とおく. さらに, $|x^2 - dy^2| = 1$ の基本解が $(x, y) = (x_1, y_1)$ であるとして

$$\varepsilon = x_1 + y_1\sqrt{d},$$
$$S_\pm = \{p\text{: 素数} \mid \text{ある正整数 } l \text{ に対して } |x^2 - dy^2| = p^l \text{ が原始的な整数解をもつ}\}$$

とおく. $p \in S_\pm$ のとき,

$$l_p = \min\{l \in \mathbb{Z} \mid |x^2 - dy^2| = p^l \text{ が原始的な整数解をもつ}, \ l > 0\}$$

とおき, $|x^2 - dy^2| = p^{l_p}$ の基本解が $(x,y) = (a_p, b_p)$ であるとして

$$\gamma_p = a_p + b_p\sqrt{d},$$
$$S_- = \{p \in S_\pm \mid {a_p}^2 - db_p^2 = -p^{l_p}\}$$

とおく. また, $\alpha = a + a'\sqrt{d}$ $(a, a' \in \mathbb{Q})$ のとき

$$\tilde{\alpha} = a - a'\sqrt{d},$$
$$N(\alpha) = \alpha\tilde{\alpha} = a^2 - da'^2$$

と定める.

注意 3. • $c = 1$ のとき $|x^2 - dy^2| = 1$ の正整数解 $(x,y) = (x_1, y_1), (x_2, y_2)$ に対して

$$x_1 < x_2 \iff y_1 < y_2 \iff x_1 + y_1\sqrt{d} < x_2 + y_2\sqrt{d}$$

が成り立ち, $x^2 - dy^2 = -1$ が整数解をもてばその基本解は $x^2 - dy^2 = 1$ の基本解より小さいが, $c > 1$ のときこれが成り立つとは限らない. 例えば, $x^2 - 2y^2 = -23$ の基本解 $(x,y) = (3,4)$ は $x^2 - 2y^2 = 23$ の基本解 $(x,y) = (5,1)$ より大きい, つまり $3 + 4\sqrt{2} > 5 + \sqrt{2}$ である.

• $d \equiv 2, 3 \pmod 4$ かつ $\mathbb{Q}(\sqrt{d})$ の類数が 1 であるとき, 素数 p が $\mathbb{Q}(\sqrt{d})$ において分解するときに限り $|x^2 - dy^2| = p$ は原始的な整数解をもち, そのような素数 p に対して $l_p = 1$ が成り立つ. 例えば, $|x^2 - 2y^2| = 7$ は原始的な整数解 $(x,y) = (1,2)$ をもち, これより小さい正整数解はないから, $d = 2$ のとき $l_7 = 1, \gamma_7 = 1 + 2\sqrt{2}$ である.

• $|x^2 - 10y^2| = 3$ は整数解をもたず, $|x^2 - 10y^2| = 3^2$ は原始的な整数解 $(x,y) = (1,1)$ をもつから, $d = 10$ のとき $l_3 = 2, \gamma_3 = 1 + \sqrt{10}$ である. また, $|x^2 - 82y^2| = 3^l$ $(1 \leqq l \leqq 3)$ は原始的な整数解をもたず, $|x^2 - 82y^2| = 3^4$ は原始的な整数解 $(x,y) = (1,1)$ をもつから, $d = 82$ のとき $l_3 = 4, \gamma_3 = 1 + \sqrt{82}$ である.

本稿の主定理の 1 つは, 次の通りである (証明は第 3 節で述べる).

定理 2. $(\star)$ の任意の非自明な有理数解 (a,b,c) は, 次のいずれかを満たす.

(I) a, b が方程式 $x^2 - y^2 = -1$ の有理数解の x 成分であるとき. (a,b,c) は, 適当な整数 l, m, n $(m \neq \pm l,\ lm \neq n^2,\ lmn \neq 0)$ を用いて

$$(a,b,c) = \left(\frac{l^2 - n^2}{2ln}, \frac{m^2 - n^2}{2mn}, \frac{lm - n^2}{(l+m)n}\right), \left(\frac{l^2 - n^2}{2ln}, \frac{m^2 - n^2}{2mn}, -\frac{(l+m)n}{lm - n^2}\right) \tag{1.3}$$

の形に表される.

(II) a, b が共通のペル方程式 $x^2 - dy^2 = -1$ ($d > 1$: 平方因数をもたない整数) の有理数解の x 成分であるとき. (a,b,c) は, $\mathbb{Q}(\sqrt{d})$ の $N(\alpha) = N(\beta) = -1, \beta \neq \pm\alpha$ を満たす元 α, β を用いて

$$(a,b,c) = \left(\frac{\alpha + \tilde{\alpha}}{2}, \frac{\beta + \tilde{\beta}}{2}, \frac{\alpha\beta - \tilde{\alpha}\tilde{\beta}}{\alpha + \beta - \tilde{\alpha} - \tilde{\beta}}\right), \left(\frac{\alpha + \tilde{\alpha}}{2}, \frac{\beta + \tilde{\beta}}{2}, -\frac{\alpha + \beta - \tilde{\alpha} - \tilde{\beta}}{\alpha\beta - \tilde{\alpha}\tilde{\beta}}\right) \tag{1.4}$$

の形に表される. ここで, α, β は,

$$l_p m_p \equiv l_p n_p \equiv 0 \pmod 2 \quad (p \in S_\pm)$$

かつ

$$\begin{cases} m + \sum_{p \in S_-} m_p \equiv n + \sum_{p \in S_-} n_p \equiv 1 \pmod 2 & (x^2 - dy^2 = -1 \text{ が整数解をもつとき}), \\ \sum_{p \in S_-} m_p \equiv \sum_{p \in S_-} n_p \equiv 1 \pmod 2 & (x^2 - dy^2 = -1 \text{ が整数解をもたないとき}) \end{cases}$$

を満たす整数 m, n, 非負整数 m_p, n_p $(p \in S_\pm)$, $\mathbb{Z}[\sqrt{d}]$ の元 $\alpha_p, \beta_p \in \{\gamma_p, \widetilde{\gamma_p}\}$ $(p \in S_\pm)$ を用いて

$$\alpha = \pm\eta^m \prod_{p \in S_\pm} {\alpha_p}^{m_p} p^{-l_p m_p/2}, \quad \beta = \pm\eta^n \prod_{p \in S_\pm} {\beta_p}^{n_p} p^{-l_p n_p/2}$$

の形に表される.

(1.3), (1.4) の形の (a, b, c) で $(\star)$ の有理数解でないものはない.

例 2. (1)　(1.3) において, $(l, m, n) = (2, 3, 1)$ とすると $(\star)$ の有理数解

$$(a, b, c) = \left(\frac{3}{4}, \frac{4}{3}, 1\right), \left(\frac{3}{4}, \frac{4}{3}, -1\right)$$

が得られ, $(l, m, n) = (2, 5, 1)$ とすると $(\star)$ の有理数解

$$(a, b, c) = \left(\frac{3}{4}, \frac{12}{5}, \frac{9}{7}\right), \left(\frac{3}{4}, \frac{12}{5}, -\frac{7}{9}\right)$$

が得られる.

(2)　(1.4) において, $d = 2, \alpha = \dfrac{1 + 5\sqrt{2}}{7}, \beta = \dfrac{1 + 5\sqrt{2}}{7}(1 + \sqrt{2})^2$ とすると $(\star)$ の有理数解

$$(a, b, c) = \left(\frac{1}{7}, \frac{23}{7}, \frac{6}{7}\right), \left(\frac{1}{7}, \frac{23}{7}, -\frac{7}{6}\right)$$

が得られ, $d = 34, \alpha = \dfrac{5 + \sqrt{34}}{3}, \beta = \dfrac{5 + \sqrt{34}}{3}(35 + 6\sqrt{34})$ とすると $(\star)$ の有理数解

$$(a, b, c) = \left(\frac{5}{3}, \frac{379}{3}, \frac{32}{9}\right), \left(\frac{5}{3}, \frac{379}{3}, -\frac{9}{32}\right)$$

が得られる.

$(\star)$ の (II) のタイプの有理数解の構造の決定には, ペル方程式の有理数解の構造に関する, 次の定理を用いる. これも本稿の主定理の 1 つである (証明は第 2 節で述べる).

定理 3. $r \in \{0, 1\}$ とする. $x^2 - dy^2 = (-1)^r$ の任意の有理数解 (x, y) は, 適当な整数 n, 非負整数 n_p $(p \in S_\pm)$, $\mathbb{Z}[\sqrt{d}]$ の元 $\gamma'_p \in \{\gamma_p, \widetilde{\gamma_p}\}$ $(p \in S_\pm)$ に対して

$$x + y\sqrt{d} = \pm\eta^n \prod_{p \in S_\pm} {\gamma'_p}^{n_p} p^{-l_p n_p/2}$$

を満たす. ここで,

$$l_p n_p \equiv 0 \pmod 2 \quad (p \in S_\pm)$$

かつ

$$\begin{cases} n + \displaystyle\sum_{p \in S_-} n_p \equiv r \pmod 2 & (x^2 - dy^2 = -1 \text{ が整数解をもつとき}), \\ \displaystyle\sum_{p \in S_-} n_p \equiv r \pmod 2 & (x^2 - dy^2 = -1 \text{ が整数解をもたないとき}) \end{cases}$$

である.

2　ペル方程式の有理数解

本節では, 2 次体の整数環における素イデアル分解の理論を用いて, 定理 3 の証明を与える. 節を通じて, $d > 1$ を平方因数をもたない整数とし, 記法 1 の記号を用いる. 特に, ε は $|x^2 - dy^2| = 1$ の基本解 $(x, y) = (x_1, y_1)$ を用いて $\varepsilon = x_1 + y_1\sqrt{d}$ と表される $\mathbb{Q}(\sqrt{d})$ の単数である. 次の定理は, 古くからよく知られている.

定理 4. (1)　$x^2 - dy^2 = 1$ は d の値によらず非自明な整数解 (よって有理数解) をもつ.
(2)　$x^2 - dy^2 = -1$ が有理数解をもつのは, d が $p \equiv 3 \pmod 4$ なる素因数 p をもたない場合に限る.

証明. (1)　ラグランジュによる証明が有名である.
(2)　$x^2 - dy^2 = -1$ は実数解をもつ. ハッセ原理により, $x^2 - dy^2 = -1$ が有理数解をもつためには, 各素数 p に対して $x^2 - dy^2 = -1$ が p 進数体 $\mathbb{Q}_p$ において解をもつことが必要十分である. $x^2 - dy^2 = -1$ が $\mathbb{Q}_p$ で解をもつためには, ヒルベルト記号 $(-1, d)_p$ の値が 1 であることが必要十分であり, $\mathbb{Q}_p$ の任意の単数 a, b に対して $(a, b)_p = 1$ が成り立つから, これは d の各素因数 p に対して $(-1, p)_p = 1$ が成り立つことと同値である. $1^2 - 2 \cdot 1^2 = -1$ により $(-1, 2)_2 = 1$ であり, $p \neq 2$ のとき

$$(-1, p)_p = \begin{cases} 1 & (p \equiv 1 \pmod 4 \text{ のとき}), \\ -1 & (p \equiv 3 \pmod 4 \text{ のとき}) \end{cases}$$

であるから, 定理の主張が成り立つ. □

注意 4. $x^2 - dy^2 = -1$ が整数解をもつためには, d が $p \equiv 3 \pmod 4$ なる素因数 p をもたないことが必要であるが, これは十分条件ではない. また, $x^2 - dy^2 = -1$ は, 整数解をもたなくても, 有理数解をもつことがある. 例えば, $x^2 - 34y^2 = -1$ は, 整数解をもたないが, 有理数解 $(x, y) = (5/3, 1/3)$ をもつ.

以下では, 与えられた整数 $c > 1$ に対して, 方程式 $|x^2 - dy^2| = c$ の整数解の構造について考察する.

整数 c_1, c_2 に対して, $x^2 - dy^2 = c_1$ の整数解 $(x, y) = (a_1, b_1)$ と $x^2 - dy^2 = c_2$ の整数解 $(x, y) = (a_2, b_2)$ が与えられれば, ノルム写像の乗法性と

$$(a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1a_2 + db_1b_2) + (a_1b_2 + a_2b_1)\sqrt{d}$$

により, $x^2 - dy^2 = c_1c_2$ の整数解

$$(x, y) = (a_1a_2 + db_1b_2, a_1b_2 + a_2b_1)$$

が得られる. $c_1 = 1$ の場合, この形の解はペル・マルチプル (Pell multiple) と呼ばれる.

定理 5 ([2, Corollary 3.5])**.** $c \neq 0$ を整数とする. $x^2 - dy^2 = c$ が整数解をもつならば, その有限個の整数解 $(x, y) = (a_1, b_1), \cdots, (a_s, b_s)$ で, 任意の整数解 (x, y) が適当な番号 i $(1 \leqq i \leqq s)$ と整数 n に対して

$$x + y\sqrt{d} = \pm(a_i + b_i\sqrt{d})\varepsilon^n$$

を満たすようなものが存在する ($x^2 - dy^2 = -1$ が整数解をもつとき n は偶数).

本稿では, このペル・マルチプルの考え方を一般化する. 次の 2 つの命題は基本的である.

命題 2. (1)　$p_1, \cdots, p_s$ を相異なる素数, $n_1, \cdots, n_s$ を非負整数とする. 各 i $(1 \leqq i \leqq s)$ に対して $|x^2 - dy^2| = {p_i}^{n_i}$ の整数解 $(x, y) = (a_i, b_i)$ が原始的ならば,

$$x + y\sqrt{d} = \pm \prod_{i=1}^{s} (a_i + b_i\sqrt{d}) \tag{2.1}$$

で定まる整数の組 (x, y) は $|x^2 - dy^2| = {p_1}^{n_1} \cdots {p_s}^{n_s}$ の原始的な整数解である.

(2)　p を素数, m, n を正整数とする. $|x^2 - dy^2| = p^m$ の整数解 $(x, y) = (a, b)$ が原始的ならば,

$$x + y\sqrt{d} = \pm(a + b\sqrt{d})^n \tag{2.2}$$

で定まる整数の組 (x, y) は $|x^2 - dy^2| = p^{mn}$ の原始的な整数解である.

証明. (1)　対偶を示す. 各 i $(1 \leqq i \leqq s)$ に対して $|x^2 - dy^2| = {p_i}^{n_i}$ が整数解 $(x, y) = (a_i, b_i)$ をもつとき, (2.1) で定まる $|x^2 - dy^2| = {p_1}^{n_1} \cdots {p_s}^{n_s}$ の整数解 (x, y) が原始的でないとし, $\alpha_i = a_i + b_i\sqrt{d}$ $(1 \leqq i \leqq s)$ とおく. このとき, x, dy は右辺のある素因数 p_j $(1 \leqq j \leqq s)$ で割り切れる.

- d が p_j の倍数であるとき. ${a_j}^2 = d{b_j}^2 \pm {p_j}^{n_j}$ は p_j の倍数で, よって a_j も p_j の倍数である.
- d が p_j の倍数でないとき. y は p_j の倍数であり,

$$(x + y\sqrt{d}) \prod_{i \neq j} \widetilde{\alpha_i} = \pm\alpha_j \prod_{i \neq j} \alpha_i \widetilde{\alpha_i} = \pm\alpha_j \prod_{i \neq j} {p_i}^{n_i}$$

　は p_j で割り切れるから, α_j は p_j で割り切れ, a_j, b_j は p_j で割り切れる.

よって, a_j, db_j は p_j の倍数であるから, (a_j, b_j) は原始的でない.

(2)　対偶を示す. $|x^2 - dy^2| = p^m$ が整数解 $(x, y) = (a, b)$ をもつとし, (2.2) で定まる $|x^2 - dy^2| = p^{mn}$ の整数解 (x, y) が原始的でないとする. このとき, x, dy は p の倍数である.

- d が p の倍数であるとき. $a^2 = db^2 \pm p^m$ は p の倍数で, よって a も p の倍数である.
- d が p の倍数でないとき. y は p の倍数であり, $x + y\sqrt{d}$ は p で割り切れて, p 進付値の $\mathbb{Q}(\sqrt{d})$ への延長 v について

$$nv(a + b\sqrt{d}) = v(x + y\sqrt{d}) > 0 \quad \text{よって} \quad v(a + b\sqrt{d}) > 0$$

　が成り立ち, a, b は p で割り切れる.

よって, a, db は p の倍数であるから, (a, b) は原始的でない. □

系 1. $c > 1$ を整数とする. $x^2 - dy^2 = -1$ が整数解をもつとき, $x^2 - dy^2 = c$ が原始的な整数解をもつことと $x^2 - dy^2 = -c$ が原始的な整数解をもつことは同値である.

証明. $r \in \{0, 1\}$ とする. $x^2 - dy^2 = (-1)^r c$ が原始的な整数解 $(x, y) = (a, b)$ をもてば, $x + y\sqrt{d} = (a + b\sqrt{d})\varepsilon$ で定まる整数の組 (x, y) は $x^2 - dy^2 = (-1)^{r+1} c$ の原始的な整数解である. □

次の命題では,

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & (\text{適当な整数 } x \text{ に対して } x^2 \equiv a \not\equiv 0 \pmod{p} \text{ のとき}) \\ -1 & (\text{任意の整数 } x \text{ に対して } x^2 \not\equiv a \pmod{p} \text{ のとき}) \\ 0 & (a \equiv 0 \pmod{p} \text{ のとき}) \end{cases}$$

(p: 奇素数, $a \in \mathbb{Z}$) で定義されるルジャンドル記号を用いる.

命題 3. $c > 1$ を整数とする. $|x^2 - dy^2| = c$ が原始的な整数解をもつならば, c の各素因数 $p \neq 2$ は $\mathbb{Q}(\sqrt{d})$ において分解する, つまり

$$\left(\frac{d}{p}\right) = 1$$

が成り立つ. この条件のもとで c が偶数であるとき, $d \equiv 1, 3 \pmod 4$ であり, c が 8 の倍数または $d \equiv 3 \pmod 4$ ならば $p = 2$ は $\mathbb{Q}(\sqrt{d})$ において分解する.

証明. c が $K = \mathbb{Q}(\sqrt{d})$ において分解しない素因数 p をもつとし, (x, y) を $|x^2 - dy^2| = c$ の任意の整数解とする. K の整数環 O_K が

$$O_K = \begin{cases} \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right] & (d \equiv 1 \pmod 4 \text{ のとき}), \\ \mathbb{Z}[\sqrt{d}] & (d \equiv 2,\ 3 \pmod 4 \text{ のとき}) \end{cases} \tag{2.3}$$

であることに注意する.

- $p \neq 2$ が K において不分岐, または "$d \equiv 3 \pmod 4$ かつ $p = 2$ が K において不分岐" であるとき. 単項イデアル (c) は O_K において
$$(c) = (x + y\sqrt{d})(x - y\sqrt{d}) \tag{2.4}$$
と分解し, 両辺は (p) で割り切れる. よって, $(x + y\sqrt{d})$ と $(x - y\sqrt{d})$ は (p) で割り切れる (素イデアル (p) は一方を割り切り, 自己共役性により他方も割り切る). 仮定により
$$pO_K \cap \mathbb{Z}[\sqrt{d}] \subset p\mathbb{Z}[\sqrt{d}]$$
であるから, $\mathbb{Z}[\sqrt{d}]$ において $(x+y\sqrt{d})$ と $(x-y\sqrt{d})$ は (p) で割り切れる. したがって, $x+y\sqrt{d}$ は p で割り切れるから, x, y は p で割り切れる.
- c が 8 の倍数かつ $d \equiv 1 \pmod 4$ かつ $p = 2$ が K において不分岐であるとき. (2.4) の両辺は $(2)^3$ で割り切れる. よって, $(x + y\sqrt{d})$ と $(x - y\sqrt{d})$ は $(2)^2$ で割り切れる (素イデアル (2) は一方を割り切り, 自己共役性により他方も同じ回数だけ割り切る).
$$2^2 O_K \cap \mathbb{Z}[\sqrt{d}] \subset 2\mathbb{Z}[\sqrt{d}]$$
であるから, $\mathbb{Z}[\sqrt{d}]$ において $(x+y\sqrt{d})$ と $(x-y\sqrt{d})$ は (2) で割り切れる. したがって, $x+y\sqrt{d}$ は 2 で割り切れるから, x, y は 2 で割り切れる.
- p が K において分岐するとき. d は p で割り切れ,
$$x^2 = dy^2 \pm c$$
は p で割り切れるから, x は p で割り切れる.

ゆえに, x, dy は p で割り切れるから, (x, y) は原始的でない. これで命題の主張が示された. □

定理 3 は, 次の定理から直ちに従う.

定理 6. 整数 $c > 1$ が
$$c = \prod_{p:\ \text{素数}} p^{i_p}$$
と素因数分解されるとする. このとき, $|x^2 - dy^2| = c$ の任意の整数解 (x, y) は, 適当な整数 n, n_p $(p \in S_\pm)$, $\mathbb{Z}[\sqrt{d}]$ の元 $\gamma'_p \in \{\gamma_p, \widetilde{\gamma_p}\}$ $(p \in S_\pm)$ に対して
$$x + y\sqrt{d} = \pm\eta^n \prod_{p \in S_\pm} {\gamma'_p}^{n_p} p^{(i_p - l_p n_p)/2} \prod_{q \notin S_\pm} q^{i_q/2} \tag{2.5}$$
を満たす. ここで,
$$i'_p = \begin{cases} i_2 - 2 & (p = 2 \in S_\pm,\ \eta^n \notin \mathbb{Z}[\sqrt{d}] \text{ のとき}), \\ i_p & (\text{その他のとき}) \end{cases}$$

として
$$0 \leqq n_p \leqq i'_p/l_p \quad (p \in S_\pm)$$
である.

証明. $|x^2 - dy^2| = c$ の整数解 (x, y) をとって, x, y の最大公約数を g とおき,
$$a = \frac{x}{g}, \quad b = \frac{y}{g}, \quad \frac{c}{g^2} = \prod_{p \in S_\pm} p^{l_p n_p + j_p} \prod_{q \notin S_\pm} q^{j_q} \quad (n_p,\ j_p\text{: } \mathrm{ord}_p(cg^{-2}) \text{ を } l_p \text{ で割った商, 余り},\ j_q\text{: 非負整数})$$
とする. 以下, $K = \mathbb{Q}(\sqrt{d})$ の整数環 O_K の単項イデアル $(a^2 - db^2) = (cg^{-2})$ について, $p \in S_\pm$ のとき $(\gamma_p)(\widetilde{\gamma_p}) = (p)^{l_p}$ であるから,
$$\begin{aligned}(a + b\sqrt{d})(a - b\sqrt{d}) &= \prod_{p \in S_\pm} (p)^{l_p n_p + j_p} \prod_{q \notin S_\pm} (q)^{j_q} \\ &= \prod_{p \in S_\pm} (\gamma_p)^{n_p} (\widetilde{\gamma_p})^{n_p} (p)^{j_p} \prod_{q \notin S_\pm} (q)^{j_q}\end{aligned}$$
が成り立つ. 各素数 p に対して, $p\mathbb{Z}$ の上にある O_K の素イデアル $\mathfrak{p}_p$ をとる.

命題 3 により, cg^{-2} の素因数 p ($d \equiv 1 \pmod 4$ のときは $p \neq 2$ とする) は O_K において
$$(p) = \mathfrak{p}_p \widetilde{\mathfrak{p}_p} \quad (\mathfrak{p}_p \neq \widetilde{\mathfrak{p}_p})$$
と分解するが, 仮に $(a + b\sqrt{d})$ が $\mathfrak{p}_p$ と $\widetilde{\mathfrak{p}_p}$ の両方を因数にもてば $\mathfrak{p}_p \widetilde{\mathfrak{p}_p} = (p)$ は $(a + b\sqrt{d})$ を割り切り, よって p が互いに素な 2 つの整数 a, b を割り切ることになってしまうから, $(a + b\sqrt{d})$ は $\mathfrak{p}_p, \widetilde{\mathfrak{p}_p}$ のいずれか一方で割り切れる. γ_p も $\mathfrak{p}_p, \widetilde{\mathfrak{p}_p}$ のいずれか一方で割り切れ,
$$\{(\gamma_p), (\widetilde{\gamma_p})\} = \{\mathfrak{p}_p{}^{l_p}, \widetilde{\mathfrak{p}_p}{}^{l_p}\} \tag{2.6}$$
が成り立つ.

次に, c が偶数かつ $d \equiv 1 \pmod 4$ のとき, 2 の分解を考える. このとき, 2 は分岐しない.

- 2 が K において分解するとき. イデアル類群の有限性によりある正整数 n, s, t に対して
$$\mathfrak{p}_2{}^n = \left(\frac{s + t\sqrt{d}}{2}\right) \quad \text{つまり} \quad |s^2 - dt^2| = 2^{n+2}$$
となるから, 両辺を 2 で割れるだけ割ることにより, ある正整数 l に対して $|x^2 - dy^2| = 2^l$ の原始的な整数解が得られる. よって, このとき $2 \in S_\pm$ であり, (2.6) と同様の等式が成り立つ.
- 2 が K において不分岐であるとき. $(a + db)$ と $(a - db)$ は (2) で同じ回数 $j_2/2$ だけ割り切れる (j_2 は偶数). 仮に $j_2 \geqq 4$ とすると $2^2 O_K \cap \mathbb{Z}[\sqrt{d}] \subset 2\mathbb{Z}[\sqrt{d}]$ により $\mathbb{Z}[\sqrt{d}]$ において $(a + db)$ が (2) で割り切れ, a, b が互いに素であることに反するから, このとき $j_2 = 2$ である.

以上を踏まえて, $(a + b\sqrt{d})$ の O_K における素イデアル分解を考える.

(i) $c \equiv 0 \pmod 2$, $d \equiv 1 \pmod 4$, $2 \notin S_\pm$ のとき. デデキント整域 O_K における素イデアル分解の一意性により, $(a + b\sqrt{d})$ は
$$(a + b\sqrt{d}) = \left(2 \prod_{p \in S_\pm} \gamma'_p{}^{n_p}\right) \prod_{p\text{: 奇素数}} \mathfrak{p}'_p{}^{j_p} \quad (\gamma'_p \in \{\gamma_p, \widetilde{\gamma_p}\},\ \mathfrak{p}'_p \in \{\mathfrak{p}_p, \widetilde{\mathfrak{p}_p}\})$$
と表される.
$$\left(\frac{a + b\sqrt{d}}{2 \prod_{p \in S_\pm} \gamma'_p{}^{n_p}}\right) = \prod_{p\text{: 奇素数}} \mathfrak{p}'_p{}^{j_p}$$

は, ±1 以外の整数では割り切れない単項イデアルであるから, 単位イデアルである. つまり, 各奇素数 p に対して $j_p = 0$ が成り立つ. さらに, $O_K^\times = \{\pm\eta^n \mid n \in \mathbb{Z}\}$ であるから, ある整数 n に対して

$$a + b\sqrt{d} = \pm 2\eta^n \prod_{p \in S_\pm} {\gamma'_p}^{n_p}$$

が成り立つ. 両辺に

$$g = 2^{(i_2-2)/2} \prod_{p \in S_\pm} p^{(i_p - l_p n_p)/2} \prod_{q \notin S_\pm \cup \{2\}} q^{i_q/2}$$

を掛けると, (2.5) が得られる.

(ii) その他のとき. $(a + b\sqrt{d})$ は

$$(a + b\sqrt{d}) = \left(\prod_{p \in S_\pm} {\gamma'_p}^{n_p} \right) \prod_{p:\text{ 素数}} {\mathfrak{p}'_p}^{j_p} \quad (\gamma'_p \in \{\gamma_p, \widetilde{\gamma_p}\},\ \mathfrak{p}'_p \in \{\mathfrak{p}_p, \widetilde{\mathfrak{p}_p}\})$$

と表される.

$$\left(\frac{a + b\sqrt{d}}{\prod_{p \in S_\pm} {\gamma'_p}^{n_p}} \right) = \prod_{p:\text{ 素数}} {\mathfrak{p}'_p}^{j_p}$$

は, ±1 以外の整数では割り切れない単項イデアルであるから, 単位イデアルである. つまり, 各素数 p に対して $j_p = 0$ が成り立つ. さらに, $O_K^\times = \{\pm\eta^n \mid n \in \mathbb{Z}\}$ であるから, ある整数 n に対して

$$a + b\sqrt{d} = \pm\eta^n \prod_{p \in S_\pm} {\gamma'_p}^{n_p}$$

が成り立つ. 両辺に

$$g = \prod_{p \in S_\pm} p^{(i_p - l_p n_p)/2} \prod_{q \notin S_\pm} q^{i_q/2}$$

を掛けると, (2.5) が得られる. □

注意 5. 定理 6 により, $x^2 - dy^2 = -1$ が整数解をもたないとき, $x^2 - dy^2 = p^n$, $x^2 - dy^2 = -p^n$ の両方が原始的な整数解をもつことはないとわかる.

例 3. $x^2 - 34y^2 = -1$ は整数解をもたない. $x^2 - 34y^2 = 1$ の基本解は $(x, y) = (35, 6)$ である. $x^2 - 34y^2 = -3^2$, $x^2 - 34y^2 = -5^2$, $x^2 - 34y^2 = -11^2$ はそれぞれ基本解 $(x, y) = (5, 1), (3, 1), (27, 5)$ をもつ. $\varepsilon = 35 + 6\sqrt{34}$ とおくと, $x^2 - 34y^2 = -(3 \cdot 5 \cdot 11)^2$ の任意の整数解 (x, y) は

- $x + y\sqrt{d} = \pm(5 \pm \sqrt{34}) \cdot 5 \cdot 11 \cdot \varepsilon^n \quad (n \in \mathbb{Z})$
- $x + y\sqrt{d} = \pm 3 \cdot (3 \pm \sqrt{34}) \cdot 11 \cdot \varepsilon^n \quad (n \in \mathbb{Z})$
- $x + y\sqrt{d} = \pm 3 \cdot 5 \cdot (27 \pm 5\sqrt{34}) \cdot \varepsilon^n \quad (n \in \mathbb{Z})$
- $x + y\sqrt{d} = \pm(5 \pm \sqrt{34})(3 \pm \sqrt{34})(27 \pm 5\sqrt{34})\varepsilon^n \quad (n \in \mathbb{Z})$

のいずれかの形に表される (複号任意).

3 角の二等分線の傾きに関する不定方程式の有理数解

命題 1 の証明. $(\star)$ の有理数解 (a, b, c) をとり,

$$a = \frac{A}{Z}, \quad b = \frac{B}{Z}, \quad c = \frac{C}{Z} \quad (A,\ B,\ C,\ Z \in \mathbb{Z},\ Z \neq 0)$$

とおく. これを $(\star)$ を代入すると, (A, B, C, Z) は

$$(A-C)^2(B^2+Z^2) = (B-C)^2(A^2+Z^2) \tag{3.1}$$

を満たすことがわかる. (3.1) において, 両辺の素因数分解を考える. $(A-C)^2$, $(B-C)^2$ は平方数であるから, 残りの各因数 A^2+Z^2, B^2+Z^2 について p 進付値が奇数であるような素因数 p の組合せは等しい. これらの素因数の積を d とおく (このような素因数が存在しなければ $d=1$ とする) と, A^2+Z^2, B^2+Z^2 は適当な整数 A', B' を用いて

$$A^2+Z^2 = dA'^2, \quad B^2+Z^2 = dB'^2 \tag{3.2}$$

の形に表されるから, A, B は方程式

$$X^2 - dY^2 = -Z^2$$

の整数解の X 成分になり, a, b は方程式 $x^2-dy^2=-1$ の有理数解の x 成分になる. (3.2) を (3.1) に代入して両辺を d で割ると

$$(A-C)^2B'^2 = (B-C)^2A'^2 \quad つまり \quad (A-C)B' = \pm(B-C)A'$$

となるから, これを C について解くと

$$C = \frac{AB'+A'B}{B'+A'}, \frac{AB'-A'B}{B'-A'} \quad よって \quad c = \frac{ab'+a'b}{b'+a'}, \frac{ab'-a'b}{b'-a'}.$$

が得られる. □

定理 2 の証明. (I) a, b が $x^2-y^2=-1$ の有理数解 $(x,y)=(a,a'), (b,b')$ の x 成分であるとき.

$$a = \frac{A}{n}, \quad a' = \frac{A'}{n}, \quad b = \frac{B}{n}, \quad b' = \frac{B'}{n} \quad (A,\ A',\ B,\ B',\ n \in \mathbb{Z},\ n \neq 0)$$

とおく. このとき,

$$A'^2 - A^2 = B'^2 - B^2 = n^2$$

が成り立つ.

$$A'+A = l, \quad B'+B = m$$

とすると,

$$A'-A = \frac{n^2}{l}, \quad B'-B = \frac{n^2}{m}$$

から,

$$a = \frac{l-n^2/l}{2n} = \frac{l^2-n^2}{2ln}, \qquad a' = \frac{l+n^2/l}{2n} = \frac{l^2+n^2}{2ln},$$
$$b = \frac{m-n^2/m}{2n} = \frac{m^2-n^2}{2mn}, \qquad b' = \frac{m+n^2/m}{2n} = \frac{m^2+n^2}{2mn}$$

となり,

$$\frac{ab'+a'b}{b'+a'} = \frac{1}{2}\cdot\frac{(l^2-n^2)(m^2+n^2)+(l^2+n^2)(m^2-n^2)}{ln(m^2+n^2)+mn(l^2+n^2)} = \frac{1}{2}\cdot\frac{2(l^2m^2-n^4)}{n(lm+n^2)(l+m)} = \frac{lm-n^2}{(l+m)n},$$
$$\frac{ab'-a'b}{b'-a'} = -\left(\frac{ab'+a'b}{b'+a'}\right)^{-1} = -\frac{(l+m)n}{lm-n^2}$$

となる.

(II) a, b が $x^2 - dy^2 = -1$ ($d > 1$: 平方因数をもたない整数) の有理数解 $(x, y) = (a, a'), (b, b')$ の x 成分であるとき. 定理 3, および $\alpha = a + a'\sqrt{d}, \beta = b + b'\sqrt{d}$ ($a, a', b, b' \in \mathbb{Z}$) のとき

$$a = \frac{\alpha + \tilde{\alpha}}{2}, \quad b = \frac{\beta + \tilde{\beta}}{2}$$

であり,

$$\alpha + \beta = (a + b) + (a' + b')\sqrt{d}, \quad \alpha\beta = (ab + da'b') + (ab' + a'b)\sqrt{d}$$

から

$$a' + b' = \frac{(\alpha + \beta) - (\widetilde{\alpha + \beta})}{2\sqrt{d}}, \quad ab' + a'b = \frac{\alpha\beta - \widetilde{\alpha\beta}}{2\sqrt{d}}$$

であることから, 求める主張が得られる. □

4 付録

定理 2 において, γ_p の値は, $d \leqq 34$, $p \leqq 97$ ($x^2 - dy^2 = -1$ は有理数解をもつ) のとき, 次の表の通りである. 参考のため, $\mathbb{Q}(\sqrt{d})$ の整数環が単項イデアル整域 (PID) であるか否か, 基本単数 η の値, および $N(\eta), N(\gamma_p)$ の値 (それぞれ η, γ_p の直下) を付記する.

d	2	5	10	13	17	26	29	34
PID	Yes	Yes	No	Yes	Yes	No	Yes	No
η	$1+\sqrt{2}$ -1	$(1+\sqrt{5})/2$ -1	$3+\sqrt{10}$ -1	$(3+\sqrt{13})/2$ -1	$4+\sqrt{17}$ -1	$5+\sqrt{26}$ -1	$(5+\sqrt{29})/2$ -1	$35+6\sqrt{34}$ 1
γ_2		$1+\sqrt{5}$ -2^2		$3+\sqrt{13}$ -2^2	$3+\sqrt{17}$ -2^3		$5+\sqrt{29}$ -2^2	
γ_3			$1+\sqrt{10}$ -3^2	$4+\sqrt{13}$ 3				$5+\sqrt{34}$ -3^2
γ_5						$1+\sqrt{26}$ -5^2	$11+2\sqrt{29}$ 5	$3+\sqrt{34}$ -5^2
γ_7	$1+2\sqrt{2}$ -7						$6+\sqrt{29}$ 7	
γ_{11}		$4+\sqrt{5}$ 11				$15+2\sqrt{26}$ 11^2		$27+5\sqrt{34}$ -11^2
γ_{13}			$9+5\sqrt{10}$ -13^2		$2+\sqrt{17}$ -13		$4+\sqrt{29}$ -13	
γ_{17}	$1+3\sqrt{2}$ -17			$10+3\sqrt{13}$ -17		$3+\sqrt{26}$ -17		
γ_{19}		$1+2\sqrt{5}$ -19			$6+\sqrt{17}$ 19	$17+5\sqrt{26}$ -19^2		
γ_{23}	$5+\sqrt{2}$ 23			$6+\sqrt{13}$ 23		$7+\sqrt{26}$ 23	$21+4\sqrt{29}$ -23	
γ_{29}		$4+3\sqrt{5}$ -29		$9+2\sqrt{13}$ 29				$3+5\sqrt{34}$ -29^2
γ_{31}	$1+4\sqrt{2}$ -31	$6+\sqrt{5}$ 31	$3+2\sqrt{10}$ -31					
γ_{37}			$53+12\sqrt{10}$ 37^2			$63+10\sqrt{26}$ 37^2		$141+25\sqrt{34}$ -37^2
γ_{41}	$7+2\sqrt{2}$ 41	$2+3\sqrt{5}$ -41	$9+2\sqrt{10}$ 41					
γ_{43}			$47+6\sqrt{10}$ 43^2	$3+2\sqrt{13}$ -43	$5+2\sqrt{17}$ -43			
γ_{47}	$7+\sqrt{2}$ 47				$8+\sqrt{17}$ 47			$9+\sqrt{34}$ 47
γ_{53}			$9+17\sqrt{10}$ -53^2	$8+3\sqrt{13}$ -53	$11+2\sqrt{17}$ 53		$13+2\sqrt{29}$ 53	
γ_{59}		$8+\sqrt{5}$ 59			$3+2\sqrt{17}$ -59	$85+12\sqrt{26}$ 59^2	$28+5\sqrt{29}$ 59	
γ_{61}		$9+2\sqrt{5}$ 61		$23+6\sqrt{13}$ 61				$45+13\sqrt{34}$ -61^2
γ_{67}			$77+12\sqrt{10}$ 67^2		$1+2\sqrt{17}$ -67	$55+17\sqrt{26}$ -67^2	$7+2\sqrt{29}$ -67	
γ_{71}	$1+6\sqrt{2}$ -71	$3+4\sqrt{5}$ -71	$9+\sqrt{10}$ 71				$10+\sqrt{29}$ 71	
γ_{73}	$9+2\sqrt{2}$ 73							
γ_{79}	$9+\sqrt{2}$ 79	$1+4\sqrt{5}$ -79	$9+4\sqrt{10}$ -79	$14+3\sqrt{13}$ 79		$5+2\sqrt{26}$ -79		
γ_{83}			$39+29\sqrt{10}$ -83^2		$10+\sqrt{17}$ 83	$25+17\sqrt{26}$ -83^2	$31+6\sqrt{29}$ -83	
γ_{89}	$3+7\sqrt{2}$ -89	$6+5\sqrt{5}$ -89	$1+3\sqrt{10}$ -89		$8+3\sqrt{17}$ -89			$15+2\sqrt{34}$ 89
γ_{97}	$1+7\sqrt{2}$ -97							

参考文献

[1] E. J. Barbeau, *Pell's Equation*, Problem Books in Mathematics, Springer, New York, 2003.

[2] K. Conrad, Pell's equation II, Retrieved 14 October 2021.

[3] T. Koshy, *Pell and Pell–Lucas Numbers with Applications*, Springer, New York, 2014.

[4] T. Hirotsu, Diophantine equation related to angle bisectors and solutions of Pell's equations, https://arxiv.org/abs/2209.10434

[5] R. A. Mollin, *Quadratics*, CRC Press, 2019.

[6] J. Neukirch, *Algebraic Number Theory*, Springer Verlag, 1999.

[7] R. C. Ochieng, C. J. Chikunji, V. Onyango-Otieno, Pythagorean triples with common sides, *J. of Math.*, 2019, 1–8.