Diophantine m-tuples

東北大学大学院理学研究科　藤田育嗣 (Yasutsugu Fujita)

1 Known Results (cf. [7])

Diophantus は次の問題を提起した:

> 各 2 数の積に 1 加えたもの a_ia_j+1 $(1 \le i < j \le 4)$ が平方数となるような 4 数 $\{a_1, a_2, a_3, a_4\}$ を探せ.

有理数からなる解 $\{1/16, 33/16, 68/16, 105/16\}$ は Diophantus 自身によるが, 最初の正整数からなる解 $\{1, 3, 8, 120\}$ は Fermat によって発見された.

定義 1.　0 でない整数 n に対し, m 個の相異なる正整数の集合 $\{a_1, \dots, a_m\}$ が $D(n)$-m-tuple (または Diophantine m-tuple with the property $D(n)$, または P_n-set of size m) であるとは, 各 $1 \le i < j \le m$ に対し a_ia_j+n が平方数であるときにいう．($n=1$ のときは, しばしば, 単に Diophantine m-tuples という.)

本節では, $D(n)$-m-tuples について知られていることを紹介する.

● <u>$n=1$ の場合.</u>

任意の $D(1)$-pair $\{a, b\}$ $(r := \sqrt{ab+1}\,)$ は $D(1)$-quadruple に拡張できる (Euler):

$$\{a, b, a+b+2r, 4r(a+r)(b+r)\}.$$

上の triple $\{a, b, a+b+2r\}$ を Euler の $D(1)$-triple (または regular $D(1)$-triple) と呼ぶ. $D(1)$-pair $\{a, b\}$ $(a < b)$ が与えられたとき, それは, $b < c$ なる最小の $D(1)$-triple $\{a, b, c\}$ であることは容易に分かる．さらに, 任意の $D(1)$-triple $\{a, b, c\}$ $(r := \sqrt{ab+1},\ s := \sqrt{ac+1},\ t := \sqrt{bc+1}\,)$ は $D(1)$-quadruple に拡張できる (Arkin-Hoggatt-Strauss [1]):

$$\{a, b, c, d_+\}, \quad d_+ := a+b+c+2abc+2rst.$$

($\because$ $ad_++1 = (at+rs)^2$, $bd_++1 = (bs+rt)^2$, $cd_++1 = (cr+st)^2$. ちなみに, $d_- := a+b+c+2abc-2rst$ とおくとき, $c > a+b+2r$ ならば $\{a, b, c, d_-\}$ も $D(1)$-quadruple である.)

このような quadruple $\{a, b, c, d_+\}$ を **regular $D(1)$-quadruple** と呼ぶ. $D(1)$-triple $\{a, b, c\}$ $(a < b < c)$ が与えられたとき, それは, $c < d$ なる最小の $D(1)$-quadruple $\{a, b, c, d\}$ であることが知られている ([17, Lemma 6]).

予想 1. ([1])　任意の $D(1)$-quadruple は regular である.

予想 1 が正しければ, 次の古くからある予想も正しいことが即座に分かる.

予想 2.　$D(1)$-quintuple は存在しない.

予想 2 の解決は, もう一歩というところまできている:

定理 1. (Dujella [17]) (i) $D(1)$-sextuple は存在しない.
(ii) $D(1)$-quintuples は高々有限個 (10^{1930} 個) しか存在しない.

予想 1 を支持する最初の結果は, Baker-Davenport によるものである.

定理 2. ([2]) $\{1, 3, 8, d\}$ が $D(1)$-quadruple ならば, $d = 120 (= d_+)$ である (従って, $\{1, 3, 8\}$ は $D(1)$-quintuple に拡張できない).

定理 2 は, 以下の 3 通りに一般化されている.

定理 3. (Dujella [7]) $\{k-1, k+1, 4k, d\}$ $(k \geq 2)$ が $D(1)$-quadruple ならば, $d = 4k(4k^2-1)(= d_+)$ である (従って, $\{k-1, k+1, 4k\}$ は $D(1)$-quintuple に拡張できない).

定理 4. (Dujella-Pethő [22]) $\{1, 3, c, d\}$ $(c < d)$ が $D(1)$-quadruple ならば, $d = c_{\nu+1}(= d_+)$ である. ここで, $c = c_\nu$ $(\nu \geq 1)$ は, $\{1, 3, c_\nu\}$ が Diophantine triple となるような数 $(c_1 = 8 < c_2 < c_3 < \cdots)$ である (従って, $\{1, 3\}$ は $D(1)$-quintuple に拡張できない).

定理 5. (Dujella [11]) $\{F_{2k}, F_{2k+2}, F_{2k+4}, d\}$ $(k \geq 1)$ が $D(1)$-quadruple ならば, $d = 4F_{2k+1}F_{2k+2}F_{2k+3}(= d_+)$ である. ここで, F_n は n 番目の Fibonacci 数である (従って, $\{F_{2k}, F_{2k+2}, F_{2k+4}\}$ は $D(1)$-quintuple に拡張できない).

さらに, 定理 3 と 4 の結果はおおよそ一般化されている.

定理 6. ([29]) 整数 $k \geq 2$ に対し, 整数 $c = c_\nu$ を次で定義する :

$$c_\nu := \frac{1}{2(k^2-1)} \times \left\{(k + \sqrt{k^2-1})^{2\nu+1} + (k - \sqrt{k^2-1})^{2\nu+1} - 2k\right\} \quad (\nu = 1, 2, \ldots). \qquad (1)$$

$c \neq c_2$ に対し, もし $\{k-1, k+1, c, d\}$ $(c < d)$ が $D(1)$-quadruple ならば, $d = c_{\nu+1}(= d_+)$ である $(c_1 = 4k,\ c_2 = 4k(4k^2-1),\ c_3 = 8k(8k^4 - 6k^2 + 1), \ldots)$.

第 2 節で, この定理の証明の概略を述べる. 定理 6 から即座に次が分かる.

系 1. 整数 $k \geq 2$ に対し, $\{k-1, k+1\}$ は $D(1)$-quintuple に拡張できない.

[系の証明] $\{k-1, k+1, c_2, c, d\}$ $(c_2 < c = c_\nu < d)$ が $D(1)$-quintuple でないことを示せばよい. これが $D(1)$-quintuple であると仮定する. d_+, d'_+ をそれぞれ $\{k-1, k+1, c, d_+\}$, $\{k+1, c_2, c, d'_+\}$ が regular となるような数とすると, regular $D(1)$-quadruple の最小性と d_+, d'_+ の定義から,

$$d \geq d'_+ > d_+ = c_{\nu+1}$$

が分かるが, これは定理 6 に反する. □

最近, $c = c_2$ の場合にも定理 6 が証明され, 従って定理 3 と 4 の結果の完全な一般化がなされた.

定理 7. (Bugeaud-Dujella-Mignotte [6]) 定理 6 の記号の下で, もし $\{k-1, k+1, c_2, d\}$ $(c_2 < d)$ が $D(1)$-quadruple なら, $d = c_3(= d_+)$ である.

注意 1. (1) 性質 $D(n)$ をもつ m 個の相異なる有理数 $(\neq 0)$ の組を rational $D(n)$-m-tuple という. もし $\{a, b, c, d\}$ が $D(1)$-quadruple なら, $\{a, b, c, d, e\}$ が rational $D(1)$-quintuple となるような $0 < e < 1$ が存在する ([8]). また, rational $D(1)$-sextuples が存在することも知られている ([32]). 例えば,

$$\{11/192, 35/192, 155/27, 512/27, 1235/48, 180873/16\}.$$

(2) 性質 $D(n)$ をもつ m 個の相異なる整数係数の多項式 ($\neq 0$, すべてが定数ではない) の組を, polynomial $D(n)$-m-tuple という. polynomial $D(1)$-quadruple は regular であることが知られている ([20]).

(3) $n=4$ の場合も, 上と同様に調べられる. 例えば, $\{F_{2k}, 5F_{2k}, F_{2k+2}, d\}$ が $D(4)$-quadruple なら $d = 4L_{2k}F_{4k+2}$ ([24]) であり, $\{k-2, k+2, 4k, d\}$ が $D(4)$-quadruple なら $d = 4k(k^2-1)$ である ([26]).

● $n=-1$ の場合.

次の定理により, $D(-1)$-quintuple は存在しないことが分かる:

定理 8. (Dujella-Fuchs [21]) $2 \leq a < b < c < d$ なら, $\{a, b, c, d\}$ は $D(-1)$-quadruple ではない.

この定理から, 次の Diophantus と Euler の問題が肯定的に解決される:

> “各 $a_ia_j + (a_i + a_j)$ $(1 \leq i < j \leq 4)$ が平方数となるような 4 つの正整数 $\{a_1, a_2, a_3, a_4\}$ は存在しない.”

従って $D(-1)$-triples $\{1, b, c\}$ の拡張可能性が問題となるが, $b = 2, 5, 10, 17, 26, 37, 50, 65, 82$ の各場合には拡張できないことが知られている ([12, 25, 27, 40]). また, 最近, $D(-1)$-quadruples は高々有限個しか存在しないことが示された (Dujella-Filipin-Fuchs [18]).

注意 2. (1) polynomial $D(-1)$-quadruple は存在しないことが知られている ([19]).

(2) $\{a_1, a_2, a_3, a_4\}$ を $D(-4)$-quadruple とすると, 各 a_i は偶数であることが分かり, $\{a_1/2, a_2/2, a_3/2, a_4/2\}$ が $D(-1)$-quadruple となる ([8, Remark 3]). 従って, $D(-1)$-quadruple が存在しないことが分かれば, $D(-4)$-quadruple が存在しないことが分かる.

(3) $\{a, b, c\}$ を $D(-1)$-triple とすると,

$$ad + 1 = \square,\ bd + 1 = \square,\ cd + 1 = \square \quad (\square : \text{平方数})$$

をみたす整数 d が存在する ($\because$ $r := \sqrt{ab-1},\ s := \sqrt{ac-1},\ t := \sqrt{bc-1}$ とするとき, $d := d^{\pm} := -(a+b+c) + 2abc \pm 2rst$ とおけばよい. ただし, $d^- > 0 \Longleftrightarrow c > a + b + 2r$ である). $d > 0$ のとき $\{a, b, c; d\}$ は性質 $D(-1; 1)$ をもつということにすると, 次が分かる.

- $\{F_{2k+1}, F_{2k+3}, F_{2k+5}, d\} : D(-1; 1)$ $(k \geq 0) \Longrightarrow d = 4F_{2k+1}F_{2k+3}F_{2k+5} (= d^{\pm})$ ([30]).
- $\{1, 2, c; d\} : D(-1; 1) \Longrightarrow d = d^{\pm}$ ([31]).

● 一般の n の場合.

まず, すべての整数 $n \neq 0$ に対して, $D(n)$-triple は存在する.

$\because$ $\cdot\ n \equiv 2 \pmod 4 \Longrightarrow \{1, k^2-2k-1, k^2+2\} :\ D(4k+2)$.

$\cdot\ n \not\equiv 2 \pmod 4 \Longrightarrow n = b^2 - a^2$ $(\exists a, \exists b \in \mathbf{Z}_{>0})$

$\Longrightarrow \{a, 2a+2b, 5a+4b\} :\ D(n)$. □

$n \equiv 2 \pmod 4$ ならば $D(n)$-quadruple は存在しないことも容易に分かる ([5, 33, 35]).

$\because$ $\{a_1, a_2, a_3, a_4\} :\ D(n) \Longrightarrow a_ia_j \equiv 2$ または $3 \pmod 4$

$\Longrightarrow \forall a_i \not\equiv 0 \pmod 4 \Longrightarrow a_i \equiv a_j \pmod 4$ $(\exists i, \exists j)$

$\Longrightarrow a_ia_j \equiv 0$ または $1 \pmod 4$, 矛盾. □

Dujella は, $n \not\equiv 2 \pmod 4$ かつ $n \notin S := \{-4, -3, -1, 3, 5, 8, 12, 20\}$ ならばいつも $D(n)$-quadruple が存在することを示した ([8]). より正確に,

$$n = 4k+3,\ 8k+1,\ 8k+5,\ 8k,\ 16k+4,\ 16k+12$$

の各場合に "多項式" $D(n)$-quadruple を与えた. 例えば, , $\{1, 9k^2+8k+1, 9k^2+14k+6, 36k^2+44k+13\}$ は $D(4k+3)$-quadruple である. ここで, $k=0,-1$ とすれば上の集合に 1 が 2 度現れてしまう. こうした k の値に対応する n が例外集合 S を構成している.

予想 3. ([10]) $n \in S$ ならば, $D(n)$-quadruple は存在しない.

$M_n := \sup\{m\,;\,\{a_1,\ldots,a_m\} : D(n)\}$ とおくとき, M_n の上限について次のようなことが知られている ([16]):

$$M_n \le 31 \qquad (|n| \le 400),$$
$$M_n < 15.476 \log|n| \quad (|n| > 400).$$

一般に, $n \notin \{\pm 1, \pm 4\}$ のとき, $\mod 4, 8, 16$ で調べて不明な場合には, $D(n)$-triple $\{a,b,c\}$ の拡張可能性を調べるのは難しい. その理由の一つは

$$ay^2 - bx^2 = 1,\ \ az^2 - cx^2 = 1,\ \ bz^2 - cy^2 = 1. \tag{2}$$

の基本解が一般には分からないことである. 今, $D(4k)$-triple $\{1, 4k(k-1), 4k^2+1\}$ ($k \in \mathbf{Z}$) を考えると, 各 ab, ac, bc は Richaud-Degert type (cf. [36, Section 3.2]) なので, (2) の基本解が分かる. さらに, $|k|$ が素数なら,

$$z^2 - (4k^2+1)x^2 = -16k^3$$

の基本解を完全に決定することができ, $\{1, 4k(k-1), 4k^2+1\}$ が $D(4k)$-quadruple に拡張できないことが分かる.
$\because$ 次の事実を使って示される (cf. [38]).

$$X^2 - DY^2 = N \tag{3}$$

について,

- (X_0, Y_0) : 原始解 $\Longrightarrow \exists j \in \mathbf{Z}$ s.t. $X_0 \equiv jY_0,\ j^2 \equiv D \pmod N$

(このとき, "(X_0, Y_0) は j に属する" という).

- $j \equiv D \pmod N$ とし, $M := (j^2 - D)/N$ とおくとき,
  (3) が j に属する解をもつ $\Longleftrightarrow T^2 - DU^2 = M$ が j に属する解をもつ.
- $|N| < \sqrt{D}$ とするとき,
  (X, Y) : (3) の解 $\Longrightarrow X/Y$ は $\sqrt{D}$ の連分数展開の主近似分数である. □

最後に, 楕円曲線の整数点との関係について述べる. E を

$$E : y^2 = (ax+1)(bx+1)(cx+1)$$

で与えられる $\mathbf{Q}$ 上の楕円曲線とし, $\mathbf{Q}$ 上の階数を $\operatorname{rk} E$ とかく.

$\{a,b,c\}$ が $D(1)$-triples $\{k-1, k+1, 4k\}$, $\{1,3,c\}$, $\{F_{2k}, F_{2k+2}, F_{2k+4}\}$ や $D(-1)$-triples $\{F_{2k+1}, F_{2k+3}, F_{2k+5}\}$, $\{1,2,c\}$ のときに, E の整数点は "多くの場合に" 自明なものと "$d_\pm$" や "$d^\pm$" からくるもののみであることが知られている. より正確に, 上の $D(1)$-triples に対し, もし, $\operatorname{rk} E = 1$ ($\{1,3,c\}$ の場合は $\operatorname{rk} E = 2$) ならば, E の整数点の x 座標は $0, d_+$ ($\{1,3,c\}$ の場合はさらに d_-) のみであり ([13, 15, 23]), 上の $D(-1)$-triples (ただし $c-2$ は平方因子を含まないと仮定する) に対し, もし, $\operatorname{rk} E = 1$ ($\{1,2,c\}$ の場合は $\operatorname{rk} E = 2$) ならば, E の整数点の x 座標は $0, d^+$ ($\{1,2,c\}$ の場合はさらに $d^-, -1, (c-3)/2$) のみである ([30, 31]).

2 $D(1)$-pairs $\{k-1, k+1\}$

本節では, 定理 6 の証明の概略を述べる.
定理 3, 4 によって,

$$\nu \geq 2, \;\; k \geq 3$$

と仮定してよい. $\{k-1, k+1, c, d\}$ を $D(1)$-quadruple とすると, 正の整数 x, y, z が存在して,

$$(k-1)d+1 = x^2, \;\; (k+1)d+1 = y^2, \;\; cd+1 = z^2$$

が成り立つ. d を消去すれば, 次の同時 Pell 方程式が得られる.

$$\begin{cases} (k-1)z^2 - cx^2 = k-1-c, & (4) \\ (k+1)z^2 - cy^2 = k+1-c. & (5) \end{cases}$$

Pell 方程式の理論より, 次をみたすような整数 $m \geq 0$, $n \geq 0$ と (4) の基本解 (z_0, x_0), (5) の基本解 (z_1, y_1) が存在する ([14, Lemma 1]):

$$z\sqrt{k-1} + x\sqrt{c} = (z_0\sqrt{k-1} + x_0\sqrt{c})(s + \sqrt{(k-1)c})^m, \tag{6}$$

$$z\sqrt{k+1} + y\sqrt{c} = (z_1\sqrt{k+1} + y_1\sqrt{c})(t + \sqrt{(k+1)c})^n, \tag{7}$$

$$1 \leq x_0 \leq \sqrt{\frac{(k-1)(c-k+1)}{2(s-1)}} < \sqrt{\frac{s+1}{2}}, \tag{8}$$

$$1 \leq |z_0| \leq \sqrt{\frac{(s-1)(c-k+1)}{2(k-1)}} < \sqrt{\frac{c\sqrt{c}}{2\sqrt{k-1}}} < \frac{c}{2}, \tag{9}$$

$$1 \leq y_1 \leq \sqrt{\frac{(k+1)(c-k-1)}{2(t-1)}} < \sqrt{\frac{t+1}{2}}, \tag{10}$$

$$1 \leq |z_1| \leq \sqrt{\frac{(t-1)(c-k-1)}{2(k+1)}} < \sqrt{\frac{c\sqrt{c}}{2\sqrt{k+1}}} < \frac{c}{2}. \tag{11}$$

(6) より $z = v_m$, (7) より $z = w_n$ とかける. ここで,

$$v_0 = z_0, \;\; v_1 = sz_0 + cx_0, \;\; v_{m+2} = 2sv_{m+1} - v_m, \tag{12}$$

$$w_0 = z_1, \;\; w_1 = tz_1 + cy_1, \;\; w_{n+2} = 2tw_{n+1} - w_n \tag{13}$$

である.

以下, $\{k-1, k+1, c, d\}$ $(c < d)$ が regular ではないと仮定する. さらに, 基本解 (z_0, x_0), (z_1, y_1) の可能性を絞るために, 次の意味で c が最小であると仮定して, $c = c_2$ 以外はあり得ないことを示す.

仮定 1. すべての $0 < c' < c_{\nu-1}$ に対して, $\{k-1, k+1, c', c\}$ は $D(1)$-quadruple ではない.

(8), (9), (10), (11) に注意すれば, (12), (13) を使って $z = v_m = w_n$ を $\bmod\ (2c)$ で考えることにより, 次が分かる.

(i) $v_{2m} = w_{2n}$ かつ $z_0 = z_1 = \pm 1$;

(ii) $v_{2m+1} = w_{2n+1}$ かつ $z_0 = \pm t$, $z_1 = \pm s$ $(z_0 z_1 > 0)$.

さらに, $v_{2m} = w_{2n}$, $v_{2m+1} = w_{2n+1}$ をそれぞれ $\bmod\ (8c^2)$, $\bmod\ (4c^2)$ で考えることにより, 次が得られる.

補題 1. $c \geq c_3$ と仮定する.

(i) $m \geq n > \min\left\{0.7\sqrt[8]{\dfrac{c}{k+1}},\, 1.6\sqrt[8]{\dfrac{c}{k^4(k+1)}}\right\};$

(ii) $m \geq n > 0.5\left(\sqrt[4]{\dfrac{c}{(k+1)^3}} - 1\right).$

また, (4) と $(k-1)y^2 - (k+1)x^2 = -2$ とから x を $x = p_l = q_m$ と 2 通りに表し, (i) の場合は mod $(4k(k-1))$ で, (ii) の場合は mod $(2k)$ で考えることにより, 次が得られる.

補題 2. $c \geq c_2$ と仮定する.

(i) $m \geq 2k-1;$

(ii) $m \geq k-1.$

c, k の上限を得るには, あとは, m の上限, 即ち, z の上限を得ればよい. そのために, Rickert (或いは Bennett) の定理を少しだけ改良した次の定理を使う.

定理 9. (cf. [4, Theorem 3.2], [37, Theorem], [39, Theorem]) k, N を $k \geq 3$, $N \geq 10k^7$ なる整数とするとき, すべての整数 p_1, p_2, q $(q > 0)$ に対し,

$$\theta_1 := \sqrt{1 + \frac{k-1}{N}} \text{ と } \theta_2 := \sqrt{1 + \frac{k+1}{N}}$$

は

$$\max\left\{\left|\theta_1 - \frac{p_1}{q}\right|, \left|\theta_2 - \frac{p_2}{q}\right|\right\} > \left\{16.1\frac{(k^2-1)^2}{k}N\right\}^{-1} q^{-1-\lambda} \tag{14}$$

をみたす. ここで,

$$\lambda := \frac{\log\left(\dfrac{8.1(k^2-1)^2}{k}N\right)}{\log\left(\dfrac{0.84}{(k^2-1)^2}N^2\right)} < 1$$

である.

今,

$$N = (k^2-1)c,\ q = (k^2-1)z,\ p_1 = (k-1)ty,\ p_2 = (k+1)sx$$

とすると, (4), (5) から, (14) の左辺は

$$\max\left\{\left|\theta_1 - \frac{(k-1)ty}{(k^2-1)z}\right|, \left|\theta_2 - \frac{(k+1)sx}{(k^2-1)z}\right|\right\} < \frac{c}{2(k-1)} z^{-2} \tag{15}$$

と上から評価できることが分かる. $c \geq c_3 (> 58k^5)$ ならば $N \geq 10k^7$ となり定理 9 が適用できるので, このとき (15) と合わせて z の上限が得られる:

$$\begin{aligned}\log z &< \frac{\log(0.84c^2)\log(\frac{8.05(k+1)(k^2-1)^4c^2}{k})}{\log(\frac{0.1037kc}{(k^2-1)^3})} \\ &< \frac{4\log(0.917c)\log(3.28k^4c)}{\log(\frac{0.1037}{k^5}c)}.\end{aligned}$$

補題 1, 2 と合わせれば, 次が示される.

命題 1.　$k \geq 3$ を整数とし, ある $d > c_{\nu+1}$ に対して $\{k-1, k+1, c, d\}$ が $D(1)$-quadruple であると仮定すると, 仮定 1 の下で次が成り立つ.

(i) $z = v_{2m} = w_{2n}$ ならば $c \leq c_6$ であり, さらに次が成り立つ.

(1) $c = c_3$ ならば, $3 \leq k \leq 34$;

(2) $c = c_4$ ならば, $3 \leq k \leq 7$;

(3) $c = c_5$ ならば, $3 \leq k \leq 5$;

(4) $c = c_6$ ならば, $k = 3$.

(ii) $z = v_{2m+1} = w_{2n+1}$ ならば $c \leq c_4$ であり, さらに次が成り立つ.

(1) $c = c_3$ ならば, $3 \leq k \leq 83$;

(2) $c = c_4$ ならば, $3 \leq k \leq 9$.

注意 3.　Rickert の定理は, θ_1, θ_2 の k のところが 0 の場合であり, $N \geq 26$ と仮定すれば $\lambda < 1$ となる. Bennett の定理は, $k-1$, $k+1$ のところが一般の相異なる整数 a_1, a_2 の場合であり, $N > \max\{|a_1|, |a_2|\}$ (今の場合, $= (k+1)^9$) なる仮定が置かれている (これはおおよそ $\lambda < 1$ となるための十分条件である). しかし, $N > (k+1)^9$ となるためには $c \geq c_4$ でなければならないので, $c = c_3$ のとき k の上限が得られず, よって, 系 1 が得られない. 従って, 定理 9 はほんのわずかな改良ではあるが, ここでは本質的である.

命題 1 で残った有限個の $c \geq c_3$ と $k \geq 3$ の場合があり得ないことをいうには, Baker-Davenport ([2]) による標準的な方法を使えばよい. すなわち, まず, m, n を係数とする対数の一次形式を評価する:

$$\text{(i)} \quad 0 < m_1 \log\alpha_1 - n_1 \log\alpha_2 + \log\alpha_3 < 1.2\alpha_1^{-2m_1}; \tag{16}$$

$$\text{(ii)} \quad 0 < m_2 \log\alpha_1 - n_2 \log\alpha_2 + \log\alpha_4 < 4.1k^2\alpha_1^{-2m_2}. \tag{17}$$

ここで, $m_1 := 2m$, $m_2 := 2m+1$, $n_1 := 2n$, $n_2 := 2n+1$,

$$\alpha_1 := s + \sqrt{(k-1)c}, \qquad \alpha_2 := t + \sqrt{(k+1)c},$$

$$\alpha_3 := \frac{(\sqrt{c} \pm \sqrt{k-1})\sqrt{k+1}}{(\sqrt{c} \pm \sqrt{k+1})\sqrt{k-1}}, \qquad \alpha_4 := \frac{(k\sqrt{c} \pm t\sqrt{k-1})\sqrt{k+1}}{(k\sqrt{c} \pm s\sqrt{k+1})\sqrt{k-1}}.$$

である. 次に, Baker 理論 (例えば [3]) を使って, 各 c, k に対して m の上限を得る:

(i)　$m_1 \leq 4 \cdot 10^{18}$;

(ii)　$m_2 \leq 6 \cdot 10^{18}$.

最後に, 各 c, k に対して, (16), (17) を $\log\alpha_2$ で割ったもの

$$0 < m_1\kappa - n_1 + \mu_1 < A_1 B^{-m_1},$$
$$0 < m_2\kappa - n_2 + \mu_2 < A_2 B^{-m_2}$$

$$\left(\kappa := \frac{\log\alpha_1}{\log\alpha_2},\ \mu_1 := \frac{\log\alpha_3}{\log\alpha_2},\ \mu_2 := \frac{\log\alpha_4}{\log\alpha_2},\ A_1 := \frac{1.2}{\log\alpha_2},\ A_2 := \frac{4.1k^2}{\log\alpha_2},\ B := \alpha_1^2\right)$$

に次の補題を適用して矛盾を示す (“reduction method” と呼ばれる方法である):

補題 3. ([22, Lemma 5 a)], [2, Lemma])　M を正の整数, p/q を κ の連分数展開の近似分数で $q > 6M$ なるものとし, $\epsilon := ||\mu q|| - M\,||\kappa q||$ とおく ($||\cdot||$ は最も近い整数との距離を表す). もし $\epsilon > 0$ ならば, 不等式

$$0 < m\kappa - n + \mu < AB^{-m}$$

は

$$\frac{\log(Aq/\epsilon)}{\log B} \leq m < M$$

の範囲に整数解をもたない.

従って, 仮定 1 の下で, $c = c_2$ が成り立つ. あとは, 次を示せばよい.

命題 2. $k \geq 3$ を整数とし, ある $c = c_\nu \geq c_4$ に対し $\{k-1, k+1, c_2, c\}$ が $D(1)$-quadruple であると仮定すると, 任意の $d > c_{\nu+1}$ に対し $\{k-1, k+1, c, d\}$ は $D(1)$-quadruple ではない.

この命題は, 上と全く同様の議論によって示される.

注意 4. (1) $c = c_2$ の場合には, 補題 2 と Baker 理論によって, $m_1 < 10^{21}$, $m_2 < 10^{21}$ が分かり, 従っていずれの場合にも $k \leq 5 \cdot 10^{20}$ が分かる. しかし, この k の上限は非常に大きいので, 補題 3 を各 k に適用することが出来ない.

(2) [6] では, 合同式をより詳細に調べることにより, 補題 2 を改良し, Baker 理論として, [3] のものを Mignotte の定理 ([34]) に置き換えることにより, $k > 1000$ ならば

$$m < 3.6 \cdot 10^{16}, \text{ 従って } k < 5.4 \cdot 10^8$$

となることを示し, reduction method により, 矛盾を導いている.

References

[1] J. Arkin, V. E. Hoggatt and E. G. Strauss, On Euler's solution of a problem of Diophantus, Fibonacci Quart. 17 (1979), 333–339.

[2] A. Baker and H. Davenport, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, Quart. J. Math. Oxford Ser. (2) 20 (1969), 129–137.

[3] A. Baker and G. Wüstholz, Logarithmic forms and group varieties, J. Reine Angew. Math. 442 (1993), 19–62.

[4] M. A. Bennett, On the number of solutions of simultaneous Pell equations, J. Reine Angew. Math. 498 (1998), 173–199.

[5] E. Brown, Sets in which $xy + k$ is a always a square, Math. Comp. 45 (1985), 613–620.

[6] Y. Bugeaud, A. Dujella and M. Mignotte, On the family of Diophantine triples, preprint.

[7] A. Dujella, Andrej Dujella home page, http://www.math.hr/~duje/.

[8] A. Dujella, Generalization of a problem of Diophantus, Acta Arith. 65 (1993), 15–27.

[9] A. Dujella, The problem of the extension of a parametric family of Diophantine triples, Publ. Math. Debrecen 51 (1997), 311–322.

[10] A. Dujella, On the exceptional set in the problem of Diophantus and Davenport, Applications of Fibonacci Numbers 7 (1998) 69–76.

[11] A. Dujella, A proof of the Hoggatt-Bergum conjecture, Proc. Amer. Math. Soc. 127 (1999), 1999–2005.

[12] A. Dujella, Complete solution of a family of simultaneous Pellian equations, Acta Math. Inform. Univ. Ostraviensis 6 (1998), 59–67.

[13] A. Dujella, A parametric family of elliptic curves, Acta Arith. 94 (2000), 87–101.

[14] A. Dujella, An absolute bound for the size of Diophantine m-tuples, J. Number Theory 89 (2001), 126–150.

[15] A. Dujella, Diophantine m-tuples and elliptic curves, J. Theor. Nombres Bordeaux 13 (2001), 111–124.

[16] A. Dujella, Bounds for the size of sets with the property $D(n)$, Glas. Mat. Ser. III 39 (2004), 199–205.

[17] A. Dujella, There are only finitely many Diophantine quintuples, J. Reine Angew. Math. 566 (2004), 183–214.

[18] A. Dujella, A. Filipin and C. Fuchs, Effective solution of the $D(-1)$-quadruple conjecture, preprint.

[19] A. Dujella and C. Fuchs, A polynomial variant of a problem of Diophantus and Euler, Rocky Mountain J. Math. 33 (2003), 797–811.

[20] A. Dujella and C. Fuchs, Complete solution of the polynomial version of a problem of Diophantus, J. Number Theory 106 (2004), 326–344.

[21] A. Dujella and C. Fuchs, Complete solution of a problem of Diophantus and Euler, J. London Math. Soc. 71 (2005), 33–52.

[22] A. Dujella and A. Pethő, A generalization of a theorem of Baker and Davenport, Quart. J. Math. Oxford Ser. (2) 49 (1998), 291–306.

[23] A. Dujella and A. Pethő, Integer points on a family of elliptic curves, Publ. Math. Debrecen 56 (2000), 321–335.

[24] A. Dujella and A. M. S. Ramasamy, Fibonacci numbers and sets with the property $D(4)$, Bull. Belg. Math. Soc. Simon Stevin 12 (2005), 401–412.

[25] A. Filipin, Non-extendibility of $D(-1)$-triples of the form $\{1, 10, c\}$, Internat. J. Math. Math. Sci. 35 (2005), 2217–2226.

[26] Y. Fujita, The unique representation $d = 4k(k^2 - 1)$ in $D(4)$-quadruples $\{k-2, k+2, 4k, d\}$, Math. Commun. 11 (2006), 69–81.

[27] Y. Fujita, The extensibility of $D(-1)$-triples $\{1, b, c\}$, Publ. Math. Debrecen, to appear.

[28] Y. Fujita, The non-extensibility of $D(4k)$-triples $\{1, 4k(k-1), 4k^2+1\}$ with $|k|$ prime, Glas. Mat. Ser. III, to appear.

[29] Y. Fujita, The extensibility of Diophantine pairs $\{k-1, k+1\}$, preprint.

[30] Y. Fujita, The Hoggatt-Bergum conjecture on $D(-1)$-triples $\{F_{2k+1}, F_{2k+3}, F_{2k+5}\}$ and integer points on the attached elliptic curves, preprint.

[31] Y. Fujita, The $D(1)$-extensions of $D(-1)$-triples $\{1, 2, c\}$ and integer points on the attached elliptic curves, preprint.

[32] P. Gibbs, Some rational Diophantine sextuples, Glas. Math. Ser. III, to appear.

[33] H. Gupta and K. Singh, On k-triad sequences, Internat. J. Math. Math. Sci. 5 (1985), 799–804.

[34] M. Mignotte, A kit on linear forms in three logarithms, preprint.

[35] S. P. Mohanty and A. M. S. Ramasamy, On $P_{r,k}$ sequences, Fibonacci Quart. 23 (1985), 36–44.

[36] R. A. Mollin, *Quadratics*, CRC Press, 1996.

[37] J. H. Rickert, Simultaneous rational approximation and related Diophantine equations, Math, Proc. Cambridge Philos. Soc. 113 (1993), 461–472.

[38] J. E. Shockley, *Introduction to number theory*, Holt, Rinehart and Winston, 1967.

[39] 須藤真樹, 連立ペル方程式に関するリッケルトの方法について, 成蹊大学工学研究報告 38 (2001), 41–50.

[40] R. Tamura, Non-extendibility of $D(-1)$-triples $\{1, b, c\}$, preprint.

藤田育嗣
東北大学大学院理学研究科
〒 980-8578
仙台市青葉区荒巻字青葉
email: fyasut@yahoo.co.jp

Yasutsugu Fujita
Mathematical Institute
Tohoku University
Sendai 980-8578, Japan