数理解析研究所講究録
1521 巻 2006 年 119-125

The extensibility of Diophantine pairs $\{k-1, k+1\}$

東北大学大学院理学研究科　藤田 育嗣 (Yasutsugu Fujita)
Mathematical Institute of Tohoku University

1 Diphantine m-tuples

本節では, Diophantine m-tuple について知られている主要なことを紹介し, 主定理を述べる.

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 $(1 \leq i < j \leq 4)$ 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 自身によって, 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 1.1. m 個の相異なる正整数の集合 $\{a_1, \ldots, a_m\}$ が **Diophantine m-tuple** であるとは, 各 $1 \leq i < j \leq m$ に対し a_ia_j+1 が平方数であるときにいう.

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

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

さらに, 任意の Diophantine triple $\{a, b, c\}$ $(r := \sqrt{ab+1},\ s := \sqrt{ac+1},\ t := \sqrt{bc+1})$ は Diophantine quadruple に拡張できる (Arkin-Hoggatt-Strauss [1]):

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

($\because$ $ad_+ + 1 = (at+rs)^2$, $bd_+ + 1 = (bs+rt)^2$, $cd_+ + 1 = (cr+st)^2$.)

このような quadruple $\{a, b, c, d_+\}$ を **regular Diophantine quadruple** と呼ぶ. Diophantine 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 Diophantine quadruple であることが知られている (cf. [10, Lemma 6]).

予想 1.2. (cf. [1]) 任意の Diophantine quadruple は regular である.

予想 1.2 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 1.3. Diophantine quintuple は存在しない.

予想 1.3 の解決は, もう一歩というところまできている:

定理 1.4. (Dujella [10]) (i) Diophantine sextuple は存在しない.
(ii) Diophantine quintuples は高々有限個 (10^{1930} 個) しか存在しない.

予想 1.2 を支持する最初の結果は, Baker-Davenport によるものである.

定理 1.5. ([2]) $\{1,3,8,d\}$ が Diophantine quadruple ならば, $d = 120(= d_+)$ である.
(従って, $\{1,3,8\}$ は Diophantine quintuple に拡張できない.)

定理 1.5 は, 以下の 3 通りに一般化されている.

定理 1.6. (Dujella [5]) $\{k-1, k+1, 4k, d\}$ $(k \geq 2)$ が Diophantine quadruple ならば, $d = 4k(4k^2-1)(= d_+)$ である.
(従って, $\{k-1, k+1, 4k\}$ は Diophantine quintuple に拡張できない.)

定理 1.7. (Dujella-Pethő [11]) $\{1,3,c,d\}$ $(c < d)$ が Diophantine 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 Diophantine quintuple に拡張できない.)

定理 1.8. (Dujella [6]) $\{F_{2k}, F_{2k+2}, F_{2k+4}, d\}$ $(k \geq 1)$ が Diophantine 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 Diophantine quintuple に拡張できない.)

ここでは, 定理 1.6 と 1.7 をおよそ一般化して次を得た.

定理 1.9. 整数 $k \geq 2$ に対し, 整数 $c = c_\nu$ を次で定義する:

$$c_\nu := \frac{1}{2(k^2-1)} \times \left\{ (k+\sqrt{k^2-1})^{2\nu+1} + (k-\sqrt{k^2-1})^{2\nu+1} - 2k \right\} \quad (\nu = 1,2,\ldots). \tag{1.1}$$

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

系 1.10. 整数 $k \geq 2$ に対し, $\{k-1, k+1\}$ は Diophantine 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 Diophantine quintuple になり得ないことを示せばよい. これが Diophantine 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 Diophantine 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 1.9 に反する. □

注意 1.11. 定理 1.6, 1.7, 1.8 に現れる Diophantine triples に伴って得られる楕円曲線の整数点は, "多くの場合に" 自明なものと regular Diophantine quadruple からくるもののみであることが知られている (cf. [12], [7], [9]). 例えば, 楕円曲線

$$E_k : y^2 = ((k-1)x+1)((k+1)x+1)(4kx+1)$$

は整数点

$$(x,y) = (0,\pm 1),\ (4k(4k^2-1), \pm(128k^6 - 112k^4 + 20k^2 - 1))$$

をもつが, E_k の $\mathbb{Q}$ 上の階数が 1 ならば, 整数点はこれらで尽くされる (ここで, E_k の関数体 $\mathbb{Q}(k)$ 上の階数は 1 である). また, $3 \leq k \leq 1000$ の各場合にも同じことが成り立つ.

2 定理 1.9 の証明

本節では, 定理 1.9 の証明の概略を述べる.
定理 1.6, 1.7 によって,

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

と仮定してよい. $\{k-1, k+1, c, d\}$ を Diophantine 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.

$$\begin{cases} (k-1)z^2 - cx^2 = k-1-c, & (2.1) \\ (k+1)z^2 - cy^2 = k+1-c. & (2.2) \end{cases}$$

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 (2.1) の基本解 (z_0, x_0), (2.2) の基本解 (z_1, y_1) が存在する (cf. [8, Lemma 1]):

$$z\sqrt{k-1} + x\sqrt{c} = (z_0\sqrt{k-1} + x_0\sqrt{c})(s + \sqrt{(k-1)c})^m, \quad (2.3)$$

$$z\sqrt{k+1} + y\sqrt{c} = (z_1\sqrt{k+1} + y_1\sqrt{c})(t + \sqrt{(k+1)c})^n, \quad (2.4)$$

$$1 \leq x_0 \leq \sqrt{\frac{(k-1)(c-k+1)}{2(s-1)}} < \sqrt{\frac{s+1}{2}}, \quad (2.5)$$

$$1 \leq |z_0| \leq \sqrt{\frac{(s-1)(c-k+1)}{2(k-1)}} < \sqrt{\frac{c\sqrt{c}}{2\sqrt{k-1}}} < \frac{c}{2}, \quad (2.6)$$

$$1 \leq y_1 \leq \sqrt{\frac{(k+1)(c-k-1)}{2(t-1)}} < \sqrt{\frac{t+1}{2}}, \quad (2.7)$$

$$1 \leq |z_1| \leq \sqrt{\frac{(t-1)(c-k-1)}{2(k+1)}} < \sqrt{\frac{c\sqrt{c}}{2\sqrt{k+1}}} < \frac{c}{2}. \quad (2.8)$$

(2.3) より $z=v_m$, (2.4) より $z=w_n$ とかける. ここで,

$$v_0=z_0,\ v_1=sz_0+cx_0,\ v_{m+2}=2sv_{m+1}-v_m, \tag{2.9}$$

$$w_0=z_1,\ w_1=tz_1+cy_1,\ w_{n+2}=2tw_{n+1}-w_n \tag{2.10}$$

である.

以下, $\{k-1,k+1,c,d\}$ $(c<d)$ が regular ではなく, かつ, 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 2.1. すべての $0<c'<c_{\nu-1}$ に対して, $\{k-1,k+1,c',c\}$ は Diophantine quadruple ではない.

(2.5), (2.6), (2.7), (2.8) に注意すれば, (2.9), (2.10) を使って $z=v_m=w_n$ を mod $2c$ で考えることにより, 基本解の可能性を絞ることができる (ここで, 仮定 2.1 を使う):

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

(ii) $v_{2m+1}=w_{2n+1}$ かつ $z_0=\pm t$, $z_1=\pm s$ $(z_0z_1>0)$.

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

補題 2.2. (cf. [11, Lemma 4]) $c\geq c_3$ と仮定する.

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

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

また, (2.1) 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 2.3. (cf. [5, Lemma 4]) $c\geq c_2$ 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, 次の Rickert (或いは Bennett) の定理を少しだけ改良したものを使う.

定理 2.4. (cf. [4, Theorem 3.2], [13, Theorem], [14, 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

$$\max\left\{\left|\theta_1-\frac{p_1}{q}\right|,\left|\theta_2-\frac{p_2}{q}\right|\right\}>\left\{16.1\frac{(k^2-1)^2}{k}N\right\}^{-1}q^{-1-\lambda} \tag{2.11}$$

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, (2.1), (2.2) から, (2.11) の左辺は

$$\max\left\{\left|\theta_1 - \frac{(k-1)ty}{(k^2-1)z}\right|, \left|\theta_2 - \frac{(k+1)sx}{(k^2-1)z}\right|\right\} < \frac{c}{2(k-1)}z^{-2} \tag{2.12}$$

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 2.4 が適用できるので, このとき (2.12) 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 2.2, 2.3 と合わせれば, 次が示される.

命題 2.5. $k \geq 3$ を整数とし, ある $d > c_{\nu+1}$ に対して $\{k-1, k+1, c, d\}$ が Diophantine quadruple であると仮定すると, 仮定 2.1 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 2.6. 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, $= (k+1)^9$) ならば $\lambda < 1$ が成り立つ. 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 1.10 が得られない. 従って, 定理 2.4 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 2.5 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:

$$\text{(i)} \quad 0 < m_1 \log \alpha_1 - n_1 \log \alpha_2 + \log \alpha_3 < 1.2\alpha_1^{-2m_1}; \tag{2.13}$$

$$\text{(ii)} \quad 0 < m_2 \log \alpha_1 - n_2 \log \alpha_2 + \log \alpha_4 < 4.1k^2\alpha_1^{-2m_2}. \tag{2.14}$$

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, (2.13), (2.14) 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 "reduction lemma" を適用して矛盾を示す:

補題 2.7. (cf. [11, 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 2.1 の下で, $c = c_2$ が成り立つ. あとは, 次を示せばよい.

定理 2.8. $k \geq 3$ を整数とし, ある $c = c_\nu \geq c_4$ に対し $\{k-1, k+1, c_2, c\}$ が Diophantine 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 Diophantine quadruple ではない.

この定理は, 上と全く同様の議論によって示される.

注意 2.9. $c = c_2$ の場合には, 補題 2.3 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 2.7 を各 k に適用することが出来ない.

参考文献

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

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

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

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

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

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

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

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

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

[14] 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.