

ディオファントスの m 組 – 連立ペル方程式の解法 –

日大生産工 ○ 藤田 育嗣

1 デイオファントスの m 組とは？

古代ギリシアの数学者ディオファントス (Diophantus) は

「各 2 数の積に 1 加えたもの $a_i a_j + 1$ ($1 \leq i < j \leq 4$) が平方数となるような 4 数の組 $\{a_1, a_2, a_3, a_4\}$ を見つけよ」

という問題を提起し、有理数からなる解

$$\left\{ \frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16} \right\}$$

を見つけた。整数からなる解を最初に見つけたのはフェルマー (Fermat) で、その 4 数の組は $\{1, 3, 8, 120\}$ である。実際、

$$\begin{aligned} 1 \cdot 3 + 1 &= 2^2, \quad 1 \cdot 8 + 1 = 3^2, \quad 1 \cdot 120 + 1 = 11^2 \\ 3 \cdot 8 + 1 &= 5^2, \quad 3 \cdot 120 + 1 = 19^2, \quad 8 \cdot 120 + 1 = 31^2. \end{aligned}$$

一般に、相異なる m 個の正整数の組 $\{a_1, a_2, \dots, a_m\}$ は、すべての $1 \leq i < j \leq m$ に対して $a_i a_j + 1$ が平方数であるとき、ディオファントスの m 組 (Diophantine m -tuple) と呼ばれる。本講演の目的は、ディオファントスの m 組に関する予想といくつかの定理を紹介し、それら定理の証明方法を概説することである。

$\{a, b, c\}$ をディオファントスの 3 組とし、 r, s, t を

$$ab + 1 = r^2, \quad ac + 1 = s^2, \quad bc + 1 = t^2$$

をみたす正整数とすると、

$$\{a, b, c, d_+\} \quad (d_+ = a + b + c + 2abc + 2rst)$$

はディオファントスの 4 組である。実際、

$$\begin{aligned} ad_+ + 1 &= a(a + b + c + 2abc + 2rst) + 1 \\ &= a^2(bc + 1) + (ab + 1)(ac + 1) + 2arst \\ &= a^2 t^2 + r^2 s^2 + 2arst = (at + rs)^2 \end{aligned}$$

であり、 $bd_+ + 1 = (bs + rt)^2$, $cd_+ + 1 = (cr + st)^2$ も同様に分かる。このような 4 組 $\{a, b, c, d_+\}$ を

正則なディオファントスの 4 組 (regular Diophantine quadruple) と呼ぶ。 $\{a, b, c, d\}$ がディオファントスの m 組であるような d の中で、 $d = d_+$ は最小である。現在知られているディオファントスの 4 組はすべて正則であり、そのようなものしかないと思われている。

予想. $\{a, b, c, d\}$ ($a < b < c < d$) がディオファントスの 4 組ならば、 $d = d_+$ である。つまり、ディオファントスの m 組はすべて正則である。

この予想が正しいければ、「ディオファントスの 5 組は存在しない」という古くからある予想が正しいことが即座に分かる。

2 定理

予想を支持する定理をいくつか紹介する。まず最初の重要な結果はフェルマーの 4 組 $\{1, 3, 8, 120\}$ に関するものである。

定理 1. ([1]) $\{1, 3, 8, d\}$ がディオファントスの 4 組ならば、 $d = 120$ である。

この場合、 $r = 2$, $s = 3$, $t = 5$ であるから、 $d_+ = 1 + 3 + 8 + 2 \cdot 1 \cdot 3 \cdot 8 + 2 \cdot 2 \cdot 3 \cdot 5 = 120$ である。定理 1 の拡張で最も一般的なものが次の定理である。

定理 2. ([4, 2]) $\{k-1, k+1, c, d\}$ ($c < d$) がディオファントスの 4 組ならば、 $d = d_+$ である。
(例えば $c = 4k$ なら、 $d = 16k^3 - 4k$.)

定理 1 は、定理 2 において $k = 2$, $c = 8$ としたものである。一般に、次が知られている。

定理 3. ([3]) (i) デイオファントスの 6 組は存在しない。

(ii) デイオファントスの 5 組は高々有限個しか存在しない。

定理 4. ([5]) $\{a, b, c, d, e\}$ ($a < b < c < d < e$) がディオファントスの 5 組ならば、 $d = d_+$ である。

3 連立ペル方程式

ディオファントスの 3 組 $\{a, b, c\}$ ($a < b < c$) が与えられているとする (従って a, b, c は定数である). $\{a, b, c, d\}$ ($c < d$) をディオファントスの 4 組と仮定すると,

$$ad + 1 = x^2, \quad bd + 1 = y^2, \quad cd + 1 = z^2 \quad (1)$$

をみたす整数 x, y, z が存在する. (1) から d を消去して, 連立ペル方程式

$$az^2 - cx^2 = a - c, \quad (2)$$

$$bz^2 - cy^2 = b - c \quad (3)$$

を得る.

一般に, 整数解だけを対象にした整数係数の方程式を不定方程式 (Diophantine equation) といい, $X^2 - DY^2 = 1$ ($D > 0$) の形の不定方程式をペル方程式 (Pell equation) という. (2) や (3) はペル方程式を少し一般化したものであるが, ここではこれらもペル方程式と呼ぶことにする.

定理 1, 2, 3, 4 は, いずれも $d > d_+$ と仮定して矛盾を導くことにより, 証明される. 証明方法は大きく分けて

- (I) ベイカー理論 (Baker's theory) を使う方法,
- (II) デイオファントス近似 (Diophantine approximation) を使う方法

の二通りある.

(I) は, どんな場合でも適用できるが, 得られる評価が非常に大きい. 従って, $\{a, b, c\}$ が “まばら” に分布しているような場合には, 有用である. 定理 1 の証明には (I) の方法が使われている.

(II) は, 適用できる場合は限られているけれども, もし適用できれば, 非常にいい評価が得られる. 定理 4 の証明には (II) の方法が使われており, 定理 2, 3 の証明には (I), (II) 両方の方法が使われている.

以下に (II) の方法のアイデアを紹介しよう. ペル方程式 (2) の両辺を cz^2 で割ると,

$$\frac{a}{c} - \frac{x^2}{z^2} = \left(\frac{a}{c} - 1\right) \cdot \frac{1}{z^2}. \quad (4)$$

左辺を因数分解して絶対値をつけると, $a < c$ なので,

$$\left| \sqrt{\frac{a}{c}} - \frac{x}{z} \right| = \left(\sqrt{\frac{a}{c}} + \frac{x}{z} \right)^{-1} \left(1 - \frac{a}{c} \right) \cdot \frac{1}{z^2}.$$

(4) と $a < c$ より, $a/c < x^2/z^2$, よって, $\sqrt{a/c} < x/z$ なので,

$$\left| \sqrt{\frac{a}{c}} - \frac{x}{z} \right| < \left(2\sqrt{\frac{a}{c}} \right)^{-1} \left(1 - \frac{a}{c} \right) \cdot \frac{1}{z^2}.$$

a, c は定数なので

$$\left| \sqrt{\frac{a}{c}} - \frac{x}{z} \right| < \frac{A}{z^2} \quad (A \text{ は定数})$$

とかける. 同様にして, ペル方程式 (3) から,

$$\left| \sqrt{\frac{b}{c}} - \frac{y}{z} \right| < \frac{B}{z^2} \quad (B \text{ は定数})$$

も分かる. 従って, $\max\{A, B\} = C$ とおくと,

$$\max \left\{ \left| \sqrt{\frac{a}{c}} - \frac{x}{z} \right|, \left| \sqrt{\frac{b}{c}} - \frac{y}{z} \right| \right\} < \frac{C}{z^2} \quad (5)$$

を得る. 一方で, デイオファントス近似を使うと, “2 次無理数は有理数とあまり近くない” ことが分かる. 例えば, $a = k - 1, b = k + 1, c = 4k$ の場合には, すべての正整数 p_1, p_2, q に対し,

$$\max \left\{ \left| \sqrt{\frac{a}{c}} - \frac{p_1}{q} \right|, \left| \sqrt{\frac{b}{c}} - \frac{p_2}{q} \right| \right\} > \frac{550^{-1}}{q^\lambda} \quad (6)$$

(λ は k で表される数で, $k \geq 29$ なら $\lambda < 2$) が成り立つ. (6) を $p_1 = x, p_2 = y, q = z$ で適用して (5) と比べると, 解 z の上限 $z^{2-\lambda} < 550C$ が得られる. これは “初等的に” 得られる z の下限に矛盾する. 残りの $k \leq 28$ の場合を個別にチェックすることにより, 証明が完了する.

参考文献

- [1] 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.
- [2] Y. Bugeaud, A. Dujella and M. Mignotte, On the family of Diophantine triples $\{k - 1, k + 1, 16k^3 - 4k\}$, Glasgow Math. J., 49 (2007), 333–344.
- [3] A. Dujella, There are only finitely many Diophantine quintuples, J. Reine Angew. Math. 566 (2004), 183–214.
- [4] Y. Fujita, The extensibility of Diophantine pairs $\{k - 1, k + 1\}$, J. Number Theory 128 (2008), 322–353.
- [5] Y. Fujita, Any Diophantine quintuple contains a regular Diophantine quadruple, J. Number Theory 129 (2009), 1678–1697.