数理解析研究所講究録
第1874巻 2014年 64-70

On an analogue of Jeśmanowicz' conjecture on exponential Diophantine equations

Takafumi Miyazaki
(Tokyo Metropolitan University)

2012年 10月 29日

1 Introduction

a, b, c を互いに素な固定された 1 より大の自然数とする. このとき, 指数型ディオファントス方程式

$$a^x + b^y = c^z \tag{1}$$

を考える. ここで, x, y, z は自然数変数である. 方程式 (1) は単数方程式の一部であり, その解の個数の有限性は, 既に得られている. また, 対数の一次形式に関する Baker の理論から, 解の大きさの上界を得ることが出来ることが知られている. しかしながら, a, b, c に具体的な値を与えた場合でさえも, 方程式 (1) を解く, すなわちその解を全て決定することは簡単ではない.

方程式 (1) に関する最近の研究の多くは, 自然数 p, q, r に対して $a^p + b^q = c^r$ を満たす三つ組み (a, b, c) を扱っている. 特に, Jeśmanowicz [2] は, $p = q = r = 2$ の場合には方程式 (1) は唯一の解 $(x, y, z) = (2, 2, 2)$ を持つと予想した. すなわち

Conjecture 1. a, b, c を互いに素な自然数とする. $a^2 + b^2 = c^2$ を仮定する. このとき方程式 (1) は唯一の解 $(x, y, z) = (2, 2, 2)$ を持つ.

この問題に対する研究は多くあるが, 一般には未解決である. Conjecture 1 の条件を満たす三つ組み a, b, c は (原始) ピタゴラス数と呼ばれる. それらは次のようなパラメータ表示を持つことが知られている (b を偶数とする):

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

ここで, m, n $(m > n)$ は互いに素かつ偶奇性が異なる自然数である. m, n に関する様々な条件下で, Conjecture 1 は正しいことが証明されている. 例えば,

- $m = 2, n = 1$ ([9]).
- $n = 1$ ([3]).
- $m = n + 1$ ([1]).
- $m \equiv 4 \pmod 8$, $n \equiv 7 \pmod{16}$ または $m \equiv 7 \pmod{16}$, $n \equiv 4 \pmod 8$ ([6]).

特に, 上記の Lu [3] と Dem'janenko [1] の結果は m, n の境界条件を扱うものであり, 他の研究結果にも役に立つもので重要である. 最近, それらは $c \equiv 1 \pmod b$ の場合に拡張された ([8]).

この稿では, Conjecture 1 の類似問題を考える. 以下の問題を提起する.

Conjecture 2. a, b, c を互いに素な自然数とする. $a^2 + b^2 = c^2$ (b は偶数) を仮定する. このとき方程式

$$c^x + b^y = a^z \tag{2}$$

は, $c = b + 1$ のときにただ一つの解 $(x, y, z) = (1, 1, 2)$ を持ち, $c > b + 1$ のときには解を持たない.

$c = b + 1$ のとき, 方程式 (2) は確かに解 $(x, y, z) = (1, 1, 2)$ を持つ. 実際, $c + b = (c + b)(c - b) = c^2 - b^2 = a^2$ が成り立つ.

主結果は, Conjecture 2 が部分的に正しいことを主張するものである.

Theorem. $c \equiv 1 \pmod{b}$ のとき, Conjecture 2 は正しい.

証明は, [8] の手法と, 対数の一次形式の理論, いわゆる Baker の理論を用いる. 以下, 方程式

$$(m^2 + n^2)^x + (2mn)^y = (m^2 - n^2)^z \tag{3}$$

を考える. ここで, m, n $(m > n)$ は互いに素かつ偶奇性が異なる自然数である.

2 $n = 1$ の場合

この節では, $n = 1$ の場合を考察する. 実際, その場合に Conjecture 2 が正しいことを証明する. これは, Conjecture 1 に関する Lu [3] による結果の類似である.

方程式 (3) に $n = 1$ を代入すると,

$$(m^2 + 1)^x + (2m)^y = (m^2 - 1)^z \tag{4}$$

となる. ここで, m は正の偶数である. 方程式 (4) の解 (x, y, z) をとる. 方程式を法 $(2m)^2$ で考えると (m が偶数であることを考慮して),

$$(m^2 + 1)^x \equiv m^2 x + 1, \quad (m^2 - 1)^z \equiv (-1)^{z-1} m^2 z + (-1)^z \pmod{4m^2}$$

だから, 合同式

$$m^2 x + 1 + (2m)^y \equiv (-1)^{z-1} m^2 z + (-1)^z \pmod{4m^2}$$

を得る. 次に, これを法 $2m$ で考えると, $1 \equiv (-1)^z \pmod{2m}$ を得る. この合同式の法 $2m$ は 2 より大きいので, 実際には等号が成立している, すなわち $(-1)^z = 1$ より, z は偶数である. よって

$$m^2 x + (2m)^y \equiv m^2 z \pmod{4m^2}$$

を得る. これから, 左辺の第二項は m^2 で割れることがわかる.

もし $y = 1$ ならば, 2 が m で割れることになるので, $m = 2$ となり, 方程式は $5^x + 4 = 3^z$ となる. これから, $(3^{z/2} + 2)(3^{z/2} - 2) = 5^x$ と書けることがわかる. この左辺の因子は互いに素であることは簡単にわかるので, その積が素数のベキであることも考慮すると, 小さい方の因子は 1 に等しいことがわかる. よって $z = 2$ であり, $x = 1$ となる.

最後に $y>1$ となる場合を考える. このとき矛盾を見つけることが出来ればよい. 場合分けをする前の合同式から, $x\equiv z \pmod 4$ を得る. 特に, x が偶数であることがわかる (z は偶数であるので). よって, $x=2X, z=2Z$ (X, Z は自然数) と書ける. すると, 方程式 (4) を変形して $DE=(2m)^y$ と書ける. ここで

$$D=(m^2-1)^Z+(m^2+1)^X, \quad E=(m^2-1)^Z-(m^2+1)^X.$$

正の偶数 D, E の形を決定するために, それらを法 $2m$ で観察する:

$$D\equiv(-1)^Z+1 \pmod{2m}, \quad E\equiv(-1)^Z-1 \pmod{2m}.$$

もし Z が偶数ならば, $D/2\equiv 1 \pmod m$ より, $D/2$ は奇数かつ m と素なので, (D が $(2m)^y$ の約数であることを考慮して) $D=2$ とならなくてはいけなくなるが, これは明らかに不可能である. よって Z は奇数であり, $E/2\equiv -1 \pmod m$ より, $E=2$ が導ける. すると $D=(2m)^y/E=2^{y-1}m^y$ なので, $(D+E)/2$ を考えて

$$(m^2-1)^Z=2^{y-2}m^y+1$$

を得る. これを法 m^2 で考えると, $(-1)^Z\equiv 1 \pmod{m^2}$ となり, 前にみたようにこれから Z が偶数であることになるが, これは矛盾である.

3 解の偶奇性

Conjecture 1 の研究において, 解 x, y, z の偶奇性を考察することは, 多くの先行研究において重要な役割を果たしている. それは, Conjecture 2 に対しても同様である.

m, n に対して, 整数 $\alpha\geq 1, \beta\geq 2, e\in\{1,-1\}$ と正の奇数 i, j を次で定める.

$$\begin{cases} m=2^\alpha i, \quad n=2^\beta j+e & m \text{ が偶数の場合,} \\ m=2^\beta j+e, \quad n=2^\alpha i & m \text{ が奇数の場合.} \end{cases} \tag{5}$$

注意として, m が偶数かつ $n=1$ の場合には, 上記の β, j, e は (一意的に) 定められないが, 前の節で示したことから, $n>1$ を仮定してよいので問題ないことがわかる. (5) の記号の下で, 次のことが証明できる.

Lemma 1. $2\alpha\neq\beta+1$ を仮定する. (x, y, z) を方程式 (3) の解とする. もし $y>1$ ならば $x\equiv z \pmod 2$ が成り立つ.

証明は, (5) を (3) に代入したものを, 法 $2^{\min\{2\alpha,\beta+1\}}$ で考察することで得られる.

以後, $c\equiv 1 \pmod b$ を仮定する. すなわち,

$$m^2+n^2=1+2mnt \tag{6}$$

と書く (t は自然数). 条件 $t=1$ は $m=n+1$ と同値であることに注意する. (6) より, 次が導かれる.

Lemma 2. (x, y, z) を方程式 (3) の解とする. すると z は偶数である.

これは, 方程式 (3) を法 m ($>n\geq 2$) で考えることと, (6) から成り立つことがわかる合同式 $n^2\equiv 1 \pmod m$ を用いれば示される.

4 特殊なペル方程式

条件 (6) は, 次の様に書き換えられる:

$$U^2-(t^2-1)V^2=1. \tag{7}$$

ここで $U=m-nt\ (>0), V=n$. (7) は ($t>1$ のとき) ペル方程式である. 以下, $t>1$ とする. ペル方程式 (7) の基本解 (最小正整数解) は, $(U,V)=(t,1)$ であるので, ペル方程式の理論から, (7) の全ての正整数解 U,V は, 次で与えられる:

$$U+V\sqrt{t^2-1}=\left(t+\sqrt{t^2-1}\right)^k \quad (k=1,2,3,\ldots.)$$

よって U,V は t の多項式である. この事実と, $(U,V)=(m-nt,n)$ を合わせて考えると, 次のことが示される.

Lemma 3. $t>1$ ならば, 次が成り立つ.

(i) m または n は $2t$ で割り切れる.
(ii) $2\alpha\neq\beta+1$.

5 役に立つ合同式

条件 (6) から, 次の合同式を得る.

$$\begin{aligned} a,c &\equiv 1+2mnt \pmod{n^2},\\ a &\equiv -1-2mnt \pmod{m^2},\\ c &\equiv 1+2mnt \pmod{m^2}. \end{aligned}$$

これから, 方程式 (3) を法 m^2,n^2 で考えることで, 次の合同式が示される.

$$\begin{cases} 2tx+2\equiv 2tz \pmod{mn} & y=1 \text{ のとき},\\ 2tx\equiv 2tz \pmod{mn} & y>1 \text{ のとき}. \end{cases}$$

もし $y=1$ とすると, Lemma 3 の (i) から mn が $2t$ で割り切れることから, $2\equiv 0 \pmod{2t}$ を得るが, これは仮定 $t>1$ に反する. 以上より, 次のことが成り立つ.

Lemma 4. $t>1$ ならば, $y>1$ かつ $x\equiv z \pmod{mn/2t}$.

Lemmas 1,2 と Lemma 3 の (ii) と Lemma 4 から, 次のことが成り立つ.

Lemma 5. $t>1$ ならば, x は偶数.

6 $t>1$

この節では, $t>1$ のときには, 方程式 (3) は解を持たないことを証明する. 仮に解 (x,y,z) が存在したとする. Lemma 4 から $y>1$ であり, また Lemmas 2,

5 から, x, z は偶数なので, $x = 2X, z = 2Z$ (X, Z は自然数) と書ける. 正の偶数 D, E ($DE = (2mn)^y$) を次のように定義する.

$$D = (m^2 - n^2)^Z + (m^2 + n^2)^X, \quad E = (m^2 - n^2)^Z - (m^2 + n^2)^X.$$

D, E の最大公約数は 2 であることはすぐにわかる. D, E の形を決定するために, 法 m, n で考察をすると

$$D \equiv (-1)^Z + 1 \pmod{m}, \quad D \equiv 2 \pmod{n},$$

$$E \equiv (-1)^Z - 1 \pmod{m}, \quad E \equiv 0 \pmod{n}.$$

ここで, (6) から従う合同式 $m^2 \equiv 1 \pmod{n}$ と $n^2 \equiv 1 \pmod{m}$ を用いた. 次のことが成り立つ.

Lemma 6. 次が成り立つ.

$$\begin{cases} (D, E) = (2^{y-1}m^y, 2n^y) & m \text{ が偶数のとき}, \\ (D, E) = (2m^y, 2^{y-1}n^y) & m \text{ が奇数のとき}. \end{cases}$$

m が偶数の場合を考える (m が奇数の場合も同様). $a = m^2 - n^2 \equiv -1 \pmod{4}$, $c = m^2 + n^2 \equiv 1 \pmod{4}$ より, $D \equiv (-1)^Z + 1 \pmod{4}$ となる. いま仮に Z が偶数であると仮定する. すると

$$D/2 \equiv 1 \pmod{2}, \quad D/2 \equiv 1 \pmod{mn/2}$$

となり, $D/2$ は奇数かつ $mn/2$ と素であることがわかる. $D/2$ は $2^{2y-1}(mn/2)^y$ の約数だから, $D/2$ は 1, すなわち $D = 2$ となるが, これは明らかに矛盾である. よって Z は奇数であるので,

$$D \equiv 0 \pmod{4}, \quad E/2 \equiv -1 \pmod{m/2}, \quad D/2 \equiv 1 \pmod{n}$$

となる. これより, $E/2$ は奇数かつ $m/2$ と素であり, $D/2$ は n と素である. すると, 等式 $(D/2)(E/2) = 2^{2y-2}(m/2)^y n^y$ から, $E/2 = n^y$, すなわち $E = 2n^y$ が従う.

Lemma 7. y は偶数である.

m が偶数の場合を考える. Lemma 6 から, $(D + E)/2$ より,

$$(m^2 - n^2)^Z = 2^{y-2}m^y + n^y$$

を得る. これを法 m で考察すると, $-1 \equiv n^y \pmod{m}$ を得る. y が偶数ならば, $n^y \equiv 1 \pmod{m}$ より, $2 \equiv 0 \pmod{m}$, となり, これは矛盾. 仮に y が奇数であると仮定する. すると, $n \equiv \pm 1 \pmod{m}$ となるが, いま仮定より, $n > 1$ かつ $m > n + 1 (\Longleftrightarrow t > 1)$ だから, この合同式は成立しない.

次に, m が奇数の場合を考える. Lemma 6 から, $(D - E)/2$ より,

$$(m^2 + n^2)^X = m^y - 2^{y-2}n^y$$

を得る. これを法 n で考察すると, $1 \equiv m^y \pmod{n}$ を得る. 仮に y が奇数であると仮定する. すると, $m \equiv 1 \pmod{n}$ となる. よって $m = 1 + hn$ (h は自然数) と書ける. これは (6) に代入すると,

$$np = 2(t - h)$$

を得る. ここで $p=h(h-2t)+1$. Lemma 3 (i) から, n は $2t$ で割れるので, h が t で割れることになる. 特に, $h=t$ または $h\geq 2t$ が成り立つ. もし $h=t$ ならば, $p=0$, すなわち, $t^2=1$ となるがこれは仮定 $t>1$ に反する. また $h\geq 2t$ ならば, $p>0$ であるので, $(-t\leq)\ t-h=np/2$ も正となるが, これも矛盾である.

Lemma 8. 次の不等式が成り立つ.

$$Z<\frac{\log c}{2\log 2}\ \left(<\frac{\log m}{\log 2}\right).$$

これは, 一般の a,b,c に対する方程式 (1) の偶数解 x,y,z の大きさの評価式から従う ([7] 参照).

いま, Lemma 7 の証明から, m は奇数であると仮定してよい. よって Lemma 3 (i) から, n が 2t で割り切れる. すると, Lemma 4 から, $2X\equiv 2Z\pmod m$ を得る. m が奇数であることから, さらに $X\equiv Z\pmod m$ を得る. 方程式 (3) から, 明らかに $Z>X$ だから, $Z\geq X+m>m$. ゆえに次の不等式を得る.

$$m<Z<\frac{\log m}{\log 2}.$$

しかしこれは成り立たない. 以上より, $t>1$ のときに方程式 (3) は解を持たないことが示された.

7 $t=1$

この節では, Theorem の証明を完成させる. $t=1$ を仮定する. このとき, (6) から, $m=n+1$ となるので, 方程式 (3) は,

$$(2m^2-2m+1)^x+(2m(m-1))^y=(2m-1)^z \tag{8}$$

となる. ここで, m は 2 以上の自然数である. (x,y,z) を方程式 (8) の解とする. Lemma 2 より, z は偶数 $(=2Z)$ である. すると, Lemma 6 の証明と同様の考察により, $y=1$ が示される ($y>1$ とすると, x が偶数であることが示せ, それによって, Lemma 6 と同じものが成り立ち, そこから矛盾を導く, という方法をとる).

$M=2m(m-1)$ と置くと, (8) は,

$$(M+1)^x+M=(2M+1)^Z \tag{9}$$

となる. これは Pillai 方程式と呼ばれるものである. Pillai 方程式には, Baker の理論が有効である. 実際, 方程式 (9) の両辺を左辺の第一項で割り, 変形すると

$$(0<)\quad \Lambda:=(2M+1)^Z(M+1)^{-x}-1=\frac{M}{(M+1)^x}$$

となり, Λ は x に関して非常に小さい. Λ は, 整数 (代数的数) のベキの積から 1 を引いた形であるが, Baker の理論は, その値の絶対値 $|\Lambda|$ の下からの評価を与える. 具体的には,

$$\log|\Lambda|\gg -\mathcal{C}(M)\log\max\{x,Z\}$$

となる ([4] 参照). ここで, $C(M)$ は, M だけに依存する正の数であり, 底 $2M+1$ と $M+1$ のそれぞれの絶対的指数的高さ (absolute logarithmic height) と呼ばれる量の積になっている. いまの場合にはそれぞれの対数がその高さに相当する. したがって,

$$-\log(M+1)\,\log(2M+1)\log x \ll -x\log(M+1)$$

を得る. これより, x (したがってまた Z の) 上界:

$$x \ll \log M(\log\log M)$$

を得る (Laurent, Mignotte, Nesterenko [5] による別の評価式を用いると, $x \ll \log M$ を得ることが出来る).

また, 一方で, 方程式 (9) を法 $M^2, (M+1)^2$ の合同式を考察することで, 次のことが証明できる.

Lemma 9. $x > 1$ ならば, 次が成り立つ.

$$2Z \equiv 1 \pmod{M+1}, \quad x+1 \equiv 2Z \pmod{2M}.$$

これによって, もし架空の解, すなわち, $(x,Z) \neq (1,1)$ が存在すれば, その下からの評価 ($\gg M$) が得られて, Baker の理論によって得られた上からの評価に矛盾する, ということを観察できる (実際には, M の, よって x, Z の有限性が出て, そのすべての可能性をチェックする必要がある). よって, 架空の解は存在せず, $x = Z = 1$ となることが示せて, 証明が終わる.

References

[1] V. A. Dem'janenko, 'On Jeśmanowicz' problem for Pythagorean numbers', *Izv. Vyssh. Ucebn. Zaved. Mat.* **48** (1965), 52–56 (in Russian).

[2] L. Jeśmanowicz, 'Several remarks on Pythagorean numbers', *Wiadom. Mat.* **1** (1955/56), 196–202 (in Polish).

[3] W. T. Lu, 'On the Pythagorean numbers $4n^2-1$, $4n$ and $4n^2+1$', *Acta Sci. Natur. Univ. Szechuan* **2** (1959), 39–42 (in Chinese).

[4] E. M. Matveev, 'An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II', *Izv. Ross. Akad. Nauk Ser. Mat.* **64** (2000), 125–180; English transl. in Izv. Math. 64 (2000), 1217–1269.

[5] M. Laurent, M. Mignotte and Y. Nesterenko, 'Formes linéaires en deux logarithmes et déterminants d'interpolation', *J. Number Theory* **55** (1995), 285–321.

[6] T. Miyazaki, 'On the conjecture of Jeśmanowicz concerning Pythagorean triples', *Bull. Austral. Math. Soc.* **80** (2009), 413–422.

[7] T. Miyazaki, 'Upper bounds for solutions of exponential Diophantine equations with applications to Fibonacci numbers', *Analytic Number Theory : related Multiple aspects of Arithmetic Functions. RIMS Kokyuroku* **1806** (2012), 134–142.

[8] T. Miyazaki, 'Generalizations of classical results on Jeśmanowicz' conjecture concerning Pythagorean triples', *J. Number Theory* **133** (2013), 583–595.

[9] W. Sierpiński, 'On the equation $3^x + 4^y = 5^z$', *Wiadom. Mat.*, **1** (1955/1956), 194–195 (in Polish).

Department of Mathematics and Information Sciences, Tokyo Metropolitan University, 1-1, Minami-Ohsawa, Hachioji, Tokyo 192-0397, Japan

E-mail address: miyazaki-takafumi@tmu.ac.jp