数理解析研究所講究録
第1710巻 2010年 113-123



# On exponential Diophantine equations concerning Pythagorean triples

Takafumi Miyazaki (Tokyo Metropolitan University)

2009年10月15日

## 1 Introduction and result

以下, $\mathbb{N}, \mathbb{Z}$ でそれぞれ自然数全体の集合, 整数全体の集合を表すことにする. $a, b, c$ を1より大きい自然数として, どの二つも互いに素であるとする. このとき不定方程式

$$a^x + b^y = c^z, \quad x, y, z \in \mathbb{N} \tag{1}$$

を考える. これは指数の位置に文字があるので, 指数型不定方程式と呼ばれる. この分野の歴史は豊富であり, 始めは具体的な $(a, b, c)$ に対して方程式 (1) の解が考察されてきた. まずは具体的な $a, b, c$ について対応する方程式 (1) の解の一覧表 (表1) を挙げる ($a, b, c$ は互いに素な自然数で $b > a > 1$ とする).

| $(a, b, c)$ | $(x, y, z)$ |
|---|---|
| $(3, 5, 2)$ | $(1, 1, 3), (3, 1, 5), (1, 3, 7)$ |
| $(2, 3, 5)$ | $(1, 1, 1), (4, 2, 2)$ |
| $(3, 11, 2)$ | 解なし |
| $(2, 11, 3)$ | $(4, 1, 3)$ |
| $(2, 3, 11)$ | $(1, 2, 1), (3, 1, 1)$ |
| $(5, 11, 2)$ | $(1, 1, 4)$ |
| $(2, 11, 5)$ | $(2, 2, 3)$ |
| $(7, 11, 2)$ | $(1, 2, 7)$ |
| $(2, 11, 7)$ | 解なし |
| $(2, 7, 11)$ | $(2, 1, 1)$ |
| $(3, 13, 2)$ | $(1, 1, 4), (5, 1, 8)$ |
| $(2, 13, 3)$ | 解なし |
| $(2, 3, 13)$ | $(2, 2, 1)$ |

-表1-

解を持つもの持たないものがある. ここで挙げた例は底 $a, b, c$ が小さいものだけであるが, 一般の大きい $a, b, c$ に対しても, 表の様子は同じような感じになる. 各トリプル $(a, b, c)$ に対して, 対応する指数型方程式 (1) のすべての解を求めるには, 基本的には初等的手段である 合同式や二次体での分解等がある. 具体例を見るには, [14], [28], [33], [37] などを参照されたい.

さて, 一般の (1) について知られる結果は非常に少ない. 代表的なものとして, 解の個数について次のことが知られている.

**Theorem (Mahler [26]-Gel'fond [12]).** (1) の解は高々有限個である.

この定理は, 初めに Mahler によって証明されたが, 彼の手法は Siegel の有限性の定理に依存していて effective なものではなかった. 後に Gel'fond は Baker の方法を用いて, この定理を effectively に示した. ここで, 'effectively' とは, $a, b, c$ が与えられたときに, $a, b, c$ にのみに依存する計算可能な定数 $C = C(a, b, c)$ が存在して, (1) のすべての解 $(x, y, z)$ について $x, y, z < C$ が成り立つ, ということである. 一般的に, この定数 $C$ は非常に大きくなる. その後, [2], [11] で与えられた $S$-単数方程式に関する結果を用いて, Hirata-Kohno は, $x > 1, y > 1, z > 1$ であるような (1) の解の個数は, $2^{36}$ 個以下であることを示している ([15]).

また, 解の個数については, 次の予想が知られている ([4], [21], [36] を参照).

**Conjecture (Terai conjecture).** $x > 1, y > 1, z > 1$ となるような (1) の解は高々 1 個である.

この予想は, 累乗数と累乗数の和は, 累乗数になることが稀であることを示唆している. このことは整数論において非常に重要であり興味が持たれている問題の一つである. 底を変数にして指数を固定して得られる, 一般化された Fermat 方程式 $X^p + Y^q = Z^r$ の分野における Beal's conjecture [27] とも関係が深い (一般化された Fermat 方程式については, [1], [10] 等を参照されたい). よって, Terai conjecture は非常に難しいものであることが推測される.

現在までに Terai conjecture は, $(a, b, c)$ がある固定された自然数 $p > 1$, $q > 1$, $r > 1$ に対して

$$a^p + b^q = c^r$$

を満たすような場合に考えられてきた. 特に

$$\underbrace{p = q = r = 2}_{\text{ピタゴラストリプル}} \quad \text{または} \quad p = q = 2,\ r = (\text{奇数} \geq 3)$$

の場合である.

前者の $p = q = r = 2$ の場合を考えることが, 本稿の主なテーマである (後者については, [4], [5], [6], [22], [23], [24] などを参照されたい).

互いに素であるような自然数の三つ組み $(a, b, c)$ は $a^2 + b^2 = c^2$ を満たすとき, 原始ピタゴラストリプルとよばれる (以下, ピタゴラストリプルとよぶ). 指数型不定方程式 (1) の歴史の中でも ピタゴラストリプルを扱うことは最も古い問題である. Sierpiński は $(a, b, c) = (3, 4, 5)$ の場合を考え, 対応する方程式 (1) の解が $(x, y, z) = (2, 2, 2)$ だけであることを証明している ([35]). 1956 年に Jeśmanowicz は, Sierpiński の結果に続いて, 方程式 (1) を別のピタゴラストリプル $(a, b, c) = (5, 12, 13), (7, 24, 25), (9, 40, 41), (11, 60, 61)$ について考察して, 対応する方程式はいずれも $(x, y, z) = (2, 2, 2)$ 以外に解を持たないことを示した. そして次のことを予想した.

**Conjecture (Jeśmanowicz [16]).** $(a, b, c)$ は $a^2 + b^2 = c^2$ を満たすピタゴラストリプルとする. このとき指数型方程式

$$a^x + b^y = c^z, \quad x, y, z \in \mathbb{N}$$

は, 唯一の解 $(x,y,z)=(2,2,2)$ を持つ.

よく知られているように, ピタゴラストリプル $(a,b,c)$ は,

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

とパラメータ表示される. ここで整数 $m,n$ は

$$m>n>0,\ \gcd(m,n)=1,\ m\not\equiv n \pmod 2$$

を満たす. よって Jeśmanowicz の予想は, 次のように言い換えることが出来る.

**Conjectute (J).** 整数 $m,n$ は

$$m>n>0,\ \gcd(m,n)=1,\ m\not\equiv n \pmod 2.$$

を満たすとする. このとき指数型方程式

$$(m^2-n^2)^x+(2mn)^y=(m^2+n^2)^z,\quad x,y,z\in\mathbb{N} \tag{2}$$

は, 唯一の解 $(x,y,z)=(2,2,2)$ を持つ.

本稿の主結果はこの予想に関するものである. それを述べる前に, 予想 (J) について現在までに知られている結果を挙げていく. 以下の場合, 予想 (J) は正しいことが分かっている.

(以下, $a=m^2-n^2,\ b=2mn,\ c=m^2+n^2$ と置く)

まずは古典的な結果として, 次のようなものがある.

- $(a,b,c)=(3,4,5)$ (Sierpiński [35]),
- $(a,b,c)=(5,12,13),(7,24,25),(9,40,41),(11,60,61)$ (Jeśmanowicz [16]),
- $n=1$ (Lu [25]),
- $m-n=1$ (Ko [17, 18], Podsypanin [34], Dem'janenko [7]).

これらは, 基本的には, 初等的な考察のみによって証明されるが, 特に, Ko, Podsypanin と Dem'janenko らによる結果の証明はあまり易しくはない.

さらにより広いクラスの $m,n$ を扱う結果としては

- $mn\equiv 2 \pmod 4$, $m^2+n^2$ が素数ベキ (Le [19]),
- $m\equiv 2 \pmod 4$, $n\equiv 3 \pmod 4$, $m\geq 81n$ (Le [20]),
- Cao [3]

$$\begin{cases} m\equiv 2 \pmod 4,\ n\equiv 1 \pmod 4 \\ \text{または} \\ m\equiv 2 \pmod 4,\ n\equiv 3 \pmod 4,\ \exists d\mid (m+n); d\equiv 3 \pmod 4 \\ \text{または} \\ m\equiv 1 \pmod 8,\ n\equiv 6 \pmod 8 \\ \text{または} \\ m\equiv 5 \pmod 8,\ n\equiv 2 \pmod 8 \end{cases}$$

などが知られている (その他の結果については, 例えば, [21] を参照されたい). 特に, 上の Cao の結果は, $m,n$ について合同式のみを仮定している所は良い点であるといえる.

しかし, これらの結果はすぐに分かるように, いずれも $mn$ がちょうど 2 で割れる場合 (つまり $mn \equiv 2 \pmod 4$) を扱っていることが分かる. ここに紹介できなかった予想 (J) に関する他の多くの既知の結果も, その場合を扱っている. それには次のような理由がある. まず第一に, 予想 (J) を考察する上では, 解 $x,y,z$ の偶奇性を知ることは極めて重要であることが分かっているが, $mn \equiv 2 \pmod 4$ の場合, Cao のような簡単な合同式を $m,n$ に仮定することだけで, $x,y,z$ が偶数であることを示すことが可能になる (Lemma 1 を参照). さらに, $mn \equiv 2 \pmod 4$ かつ $x,y,z$ のすべてが偶数ならば, 簡単に $x=y=z=2$ が示せることが分かっている ([13]).

よって $mn \equiv 0 \pmod 4$ のときにも予想 (J) が成り立つことを示す結果を得ることは非常に重要であるといえる. 今回の主結果は, それに適するものであり, 次に述べる.

**Main Theorem (Theorem 1.5 [29]).** $m,n$ が次の合同式の条件

$$m \equiv 4 \pmod 8,\ n \equiv 7 \pmod{16}$$

または

$$m \equiv 7 \pmod{16},\ n \equiv 4 \pmod 8$$

を満たすとする. このとき予想 (J) が成り立つ.

Main Theorem は $mn$ が (ちょうど) 4 で割れる場合を扱っていることに注意する.

**補足.** $mn \equiv 0 \pmod 4$ となる場合に予想が成り立つような結果としては, 上の Main Theorem の他に, Deng, Cohen [9] による結果, また, Miyazaki [29] (上の結果とは別のもの) によるものがある.

# 2. Preliminaries for Main Theorem

以下, $(x,y,z)$ は (2) の解とする. まずは, 解 $x,y,z$ 達が偶数であることを示すための簡単な条件を lemma として示す.

**Lemma 1.** 次が成り立つ.

(i) $m \not\equiv 1 \pmod 4$ ならば $2 \mid x$.
(ii) $m+n \equiv 7 \pmod 8$ ならば $2 \mid y$.
(iii) $m+n \equiv 3 \pmod 8$ ならば $2 \mid z$.
(iv) $m-n \equiv \pm 3 \pmod 8$ ならば $y \equiv z \pmod 2$.

**Proof.** 以下, 記号 $(*)/(*)$ で Jacobi 記号を表すことにする.

(i) まずは $m$ が偶数の場合を考える. $n$ は奇数である. 法 4 では, 奇数の二乗は 1 と合同になるから, (2) より

$$(-1)^x \equiv 1 \pmod 4$$

を得る. これより $2 \mid x$.

$m \equiv 3 \pmod 4$ の場合を考える. (2) を法 $m$ で考えれば

$$(-n^2)^x \equiv n^2 \pmod m.$$

これより Jacobi 記号を使えば

$$\left(\frac{-1}{m}\right)^x = 1$$

を得る. 平方剰余の第一補充法則によって, $m \equiv 3 \pmod 4$ のときは, $\left(\frac{-1}{m}\right) = -1$ だから $2 \mid x$ となる.

(ii,iii) (2) より

$$(-2m^2)^y \equiv (2m^2)^z \pmod{m+n}$$

が分かる. この両辺の Jacobi 記号を取ることを考える. まず左辺は, 平方剰余の第二補充法則によって

$$\left(\frac{-2m^2}{m+n}\right)^y = \left(\frac{-2}{m+n}\right)^y = \begin{cases} (-1)^y & \text{if } m+n \equiv 7 \pmod 8, \\ 1 & \text{if } m+n \equiv 3 \pmod 8 \end{cases}$$

となる. 右辺についても同様にして

$$\left(\frac{2m^2}{m+n}\right)^z = \left(\frac{2}{m+n}\right)^z = \begin{cases} 1 & \text{if } m+n \equiv 7 \pmod 8, \\ (-1)^z & \text{if } m+n \equiv 3 \pmod 8. \end{cases}$$

これらより主張は得られる.

(iv) (ii,iii) と同様である. □

**Notations.** 次に, 整数 $m, n$ の次のようなパラメータ表示を考える ([25] より, $n > 1$ としてよい). これは従来の研究には無い新しいものである. $m, n$ によって決まる自然数

$$\alpha \geq 1,\ \beta \geq 2,\ \underbrace{i \geq 1,\ j \geq 1}_{\text{奇数}}$$

を次のように定める:

$$m = 2^\alpha i,\quad n = 2^\beta j \pm 1 \quad m \text{ が偶数のとき},$$

$$m = 2^\beta j \pm 1,\quad n = 2^\alpha i \quad m \text{ が奇数のとき}.$$

このパラメータ $\alpha, \beta, i, j$ 間の場合分けを考えることによって, (2) の解 $(x, y, z)$ に対する $x, y, z$ の parity を, 以前までの研究より本質的に考察できるようになる. まずは次の lemma を示す (Main Theorem の証明には, (iii) のみを用いる).

**Lemma 2.** 次が成り立つ.

(i) $\alpha > 1,\ \alpha \neq \beta,\ 2\alpha \neq \beta + 1$ ならば $x \equiv z \pmod 2$.

(ii) $2\alpha \neq \beta + 1$ かつ $y > 1$ ならば $x \equiv z \pmod 2$.

(iii) $2\alpha = \beta + 1$ ならば $2 \mid x$ または $2 \mid z$.

**Proof.** 以下, 記号 $\nu_2$ で 2 進付値を表すことにする. $m$ が偶数のときだけ証明する.

(i) $2\alpha \neq \beta + 1$ とする. さらに $x \not\equiv z \pmod 2$ を仮定する. Lemma 1 (i) より, $2 \mid x$ かつ $2 \nmid z$ の場合を考えればよい. (2) より

$$\begin{aligned}(2mn)^y &= (m^2+n^2)^z - (m^2-n^2)^x \\ &\equiv zm^2n^{2z-2} + n^{2z} + xm^2n^{2x-2} - n^{2x} \pmod{2^{2\alpha+1}} \\ &\equiv m^2 \underbrace{(zn^{2z-2} + xn^{2x-2})}_{\text{奇数}} + n^{2z} - n^{2x} \\ &\equiv A + B,\end{aligned}$$

ここで

$$A = m^2(zn^{2z-2} + xn^{2x-2}),\ B = n^{2z} - n^{2x}.$$

$A, B$ のそれぞれの $\nu_2$ の値を調べる.

$$\nu_2(A) = \nu_2(m^2) = 2\alpha,$$

さらに, $2 \nmid n$, $x \not\equiv z \pmod 2$, $n^2 - 1 = 2^{2\beta}j^2 \pm 2^{\beta+1}j$, $\beta \geq 2$ から

$$\nu_2(B) = \nu_2(n^{2|z-x|} - 1) = \nu_2(n^2 - 1) = \beta + 1,$$

が分かる. これらより

$$\nu_2((2mn)^y) = (\alpha + 1)y.$$

を得る.

$2\alpha \neq \beta + 1$ なので,

もし $2\alpha < \beta + 1$ ならば, $(\alpha+1)y = 2\alpha$ となり, これからすぐに $y = 1$, $\alpha = 1$ がわかる.

もし $2\alpha > \beta + 1$ ならば, $(\alpha+1)y = \beta+1$ となり, これからすぐに $y = 1$, $\alpha = \beta$ がわかる.

(ii) (i) より OK.

(iii) $2\alpha = \beta + 1$ を仮定する. このとき, $2\beta = 4\alpha - 2$ かつ $\alpha > 1$ であることに注意する.

(2) に $\alpha, \beta, i, j$ のパラメータ表示を代入して,

$$\left(2^{2\alpha}i^2 - (2^{2\beta}j^2 \pm 2^{\beta+1}j + 1)\right)^x + 2^{(\alpha+1)y}k = \left(2^{2\alpha}i^2 + (2^{2\beta}j^2 \pm 2^{\beta+1}j + 1)\right)^z,\ 2 \nmid k$$

を得る. これを法 $2^{4\alpha-2}$ で考えてやれば,

$$\left((i^2 \mp j)2^{2\alpha} - 1\right)^x + 2^{(\alpha+1)y}k \equiv \left((i^2 \pm j)2^{2\alpha} + 1\right)^z \pmod{2^{4\alpha-2}}$$

となり, さらに

$$(-1)^{x-1}(i^2 \mp j)2^{2\alpha}x + e + 2^{(\alpha+1)y}k \equiv (i^2 \pm j)2^{2\alpha}z + 1, \quad e = \pm 1.$$

がわかる. この合同式からすぐに, $e \equiv 1 \pmod 4$ より $e = 1$ がわかる. また, $\alpha > 1$ より $y > 1$ も分かる. よって

$$(-1)^{x-1}(i^2 \mp j)x + 2^{\alpha(y-2)+y}k \equiv (i^2 \pm j)z \pmod{2^{2\alpha-2}}.$$

さらに

$$(-1)^{x-1}(1 \mp j)x \equiv (1 \pm j)z \pmod 4$$

を得る. $j$ は奇数なので, この合同式から, $x$ または $z$ は偶数であることがわかる (複号同順であることに注意). □

**Lemma 3.** $2\alpha = \beta + 1$ を仮定する. $(x, y, z)$ を (2) の解とする. $x, z$ は偶数であると仮定する. $x = 2X$, $z = 2Z$ と置く. このとき, もし $y > 3$ ならば, $X$ または $Z$ は偶数とならなくてはいけない.

**Proof.** $D = (m^2+n^2)^Z + (m^2-n^2)^X, E = (m^2+n^2)^Z - (m^2-n^2)^X$ と置くと, (2) より, $(2mn)^y = DE$ である. すぐに分かるように, $D, E$ は偶数であり,

$$\gcd(D, E) = 2, \quad 2^{(\alpha+1)y} \parallel DE.$$

よって適切な符号を選ぶことで

$$(m^2+n^2)^Z \pm (m^2-n^2)^X \equiv 0 \pmod{2^{(\alpha+1)y-1}}$$

となる. ここで $y > 3$ を仮定する. すると $(\alpha+1)y - 1 \geq 4\alpha + 3$ となるから, 上の合同式は

$$(m^2+n^2)^Z \pm (m^2-n^2)^X \equiv 0 \pmod{2^{4\alpha-2}}$$

となり, Lemma 2 の証明と同様に考えれば, $X$ または $Z$ は偶数となることが分かる. □

# 3. Proof of Main Theorem.

**証明の流れ.** Main Theorem の証明は, 次の Step ①-③を踏む.

① Darmon, Merel による一般化された Fermat 方程式の結果を用いて,

$$\text{`}x, y, z \text{ はすべて偶数} \implies x/2, y/2, z/2 \text{ はすべて奇数'}$$

を示す.

② ①と Lemma 3 より,

$$\text{`}2\alpha = \beta + 1 \text{ かつ } x, y, z \text{ はすべて偶数} \implies y \leq 3 \ (\rightsquigarrow x = y = z = 2)\text{'}$$

が分かる.

③ 最後に

$$\text{`Main Theorem の仮定} \implies 2\alpha = \beta + 1 \text{ かつ } x, y, z \text{ はすべて偶数'}$$

を示す.

**一般化された Fermat 方程式.** Main Theorem の証明には, 上の①を示すことが最も重要な箇所である. その証明には, Fermat 方程式 $X^n + Y^n = Z^n$ の一般化された (あるいは類似物である) 方程式の分野における深い結果を用いる.

$A, B, C, p, q, r$ は整数とし,

$$ABC \neq 0, \gcd(A, B, C) = 1, \ p > 1, \ q > 1, \ r > 1$$

を満たすとする. このとき

$$AX^p + BY^q = CZ^r,$$
$$X, Y, Z \in \mathbb{Z},\ \gcd(X, Y) = 1,\ XYZ \neq 0$$

を一般化された Fermat 方程式（generalized Fermat equations）という.

次の lemma は, この分野における最も著しい結果の一つである. その証明には, Wiles の Fermat の最終定理でも使われた非常に深い結果（楕円曲線, 保系形式）にもとづいて証明される.

**Lemma 4 (Darmon-Merel [8]).** $n \geq 3$ のとき, 方程式

$$X^n + Y^n = 2Z^n,\ \ \gcd(X, Y) = 1,\ XYZ \notin \{0, \pm 1\}$$

は整数解を持たない. また $n \geq 4$ のとき, 方程式

$$X^n + Y^n = Z^2,\ \ \gcd(X, Y) = 1,\ XYZ \notin \{0, \pm 1\}$$

は整数解を持たない.

この Lemma 4 から, 次のことが初等的な手段によって導かれる.

**Lemma 5 (Cao-Dong [4, 5]).** $N > 1$ とする. このとき, 方程式

$$X^{2N} + Y^4 = Z^2,\ \ \gcd(X, Y) = 1,\ XYZ \neq 0$$

は整数解を持たない. また, 方程式

$$X^{2N} + Y^2 = Z^4,\ \ \gcd(X, Y) = 1,\ XYZ \neq 0,\ 2 \mid X$$

は整数解を持たない.

これらを用いて ① を示す.

次の命題は, 以前までは様々な仮定の下で証明されてきたものであるが, Lemma 5 を使えば無条件で証明できる.

**Proposition.** $(x, y, z)$ を (2) の解として, $x, y, z$ がすべて偶数であると仮定する. $x = 2X, y = 2Y, z = 2Z$ と置く. このとき $X, Y, Z$ はすべて奇数となる.

**Proof.** $(m^2 - n^2)^X, (2mn)^Y, (m^2 + n^2)^Z$ はピタゴラストリプルなので

$$(m^2 - n^2)^X = s^2 - t^2,$$
$$(2mn)^Y = 2st,$$
$$(m^2 + n^2)^Z = s^2 + t^2,$$

となる整数 $s, t$ があり, $s > t > 0, \gcd(s, t) = 1, s \not\equiv t \pmod 2$ を満たす. これらから容易に

$$(*) \qquad Z < 2X,\ \ Z < 2Y$$

が示される.

- $2 \nmid X, 2 \nmid Y$ であること.

仮に $2 \mid X$ だとする. (2) より

$$(2mn)^{2Y} + ((m^2 - n^2)^{X/2})^4 = (m^2 + n^2)^{2Z}$$

が分かる. ここで $Y>1$ とすると, Lemma 5 に矛盾するから, $Y=1$ である. よってまた, $(*)$ より, $Z=1$ が分かる. ところが (2) から, $x=2$ $(X=1)$ が分かるがこれは矛盾である. よって $2\nmid X$ が分かる. 同様にして $2\nmid Y$ が分かる.

- $2\nmid Z$ であること.

仮に $2\mid Z$ だとする. (2) より

$$(2mn)^{2Y}+(m^2-n^2)^{2X}=((m^2+n^2)^{Z/2})^4$$

が分かる. ここで, $Y>1$ とすると, Lemma 5 に矛盾するから, $Y=1$ となる. しかしこれは, 上でも見たように, $Z=1$ を導く. これは矛盾である. よって $2\nmid Z$ である. □

**Lemma 6.** $2\alpha=\beta+1$ を仮定する. $(x,y,z)$ を (2) の解とする. このとき, もし

$$x\equiv z \pmod 2,\ 2\mid y$$

ならば, $(x,y,z)=(2,2,2)$ が成り立つ.

**Proof.** Lemma 2 (iii) より, $x,y,z$ はすべて偶数であることが分かる. よって, Proposition より, $x=2X$, $y=2Y$, $z=2Z$, $2\nmid X$, $2\nmid Z$. Lemma 3 より $y\leq 3$ だから, $y=2$ $(Y=1)$ を得る. よって $(*)$ より, $Z=1$ $(z=2)$, そして $x=2$ を得る. □

**Proof of Main Theorem.** $m\equiv 4 \pmod 8, n\equiv 7 \pmod{16}$ のときにのみ示す. $(x,y,z)$ を (2) の解とする. いま仮定より $\alpha=2$, $\beta=3$. 特に $2\alpha=\beta+1$ なので, Lemma 6 より, $x,y,z$ のすべてが偶数であることがいえればよい.

まずは, $m$ が偶数であることから, Lemma 1 (i) より $2\mid x$ がわかる, 次に, $m+n\equiv 3 \pmod 8$ であることから, Lemma 1 (iii) より $2\mid z$ である. 最後に, $m-n\equiv 5 \pmod 8$ であることから, Lemma 1 (iv) より $y\equiv z \pmod 2$ がわかる. $z$ は偶数であるから, $y$ も偶数である.

以上より, $x,y,z$ はすべて偶数である. $m\equiv 7 \pmod{16}, n\equiv 4 \pmod 8$ のときも同様に示される. これで Main Theorem の証明が終わった. □

# 4. An analogue of Jeśmanowicz' conjecture

[31] で Jesmanowicz の予想の一つのアナローグとして次の予想を提起した.

**Conjectute (M).** $(a,b,c)$ は $a^2+b^2=c^2$ を満たすピタゴラストリプルとし, $b$ を偶数とする. このとき指数型方程式

$$c^x+b^y=a^z,\quad x,y,z\in\mathbb{N} \tag{3}$$

は, $c>b+1$ のときには解を持たず, $c=b+1$ のときには唯一の解 $(x,y,z)=(1,1,2)$ を持つ.

予想 (J) のときと同様に, この予想は次のように言い換えることが出来る ($c=b+1\Leftrightarrow m=n+1$ に注意する).

**Conjectute** (M). 整数 $m,n$ は

$$m > n > 0,\ \gcd(m,n) = 1,\ m \not\equiv n \pmod 2.$$

を満たすとする. このとき指数型方程式

$$(3) \qquad (m^2+n^2)^x + (2mn)^y = (m^2-n^2)^z,\quad x,y,z \in \mathbb{N}$$

は, $m > n+1$ のときには解を持たず, $m = n+1$ のときは唯一の解 $(x,y,z) = (1,1,2)$ を持つ.

[31] で初等的な議論と, Baker 理論にもとづく対数の一次形式に関する下限についての Mignotte の定理 [29] を用いて次のことを証明した.

**Theorem 7** ([31]). $n = 1$ ならば予想 (M) は正しい.

**Theorem 8** ([31]). $c = b+1$ $(m = n+1)$ ならば 方程式 (3) は唯一の自然数解 $(x,y,z) = (1,1,2)$ を持つ.

これらは, 予想 (J) に関する結果 Lu, Ko-Podsypanin-Dem'janenko の結果に対応するものであるといえる. 特に, Theorem 8 より, Conjecture (M.) の半分は証明されたことになる. Mignotte の定理の他の Application の例としては, [36] が非常に参考になる.

その後, その拡張になる次のことの証明も出来た.

**Theorem 9** ([32]). $c \equiv 1 \pmod b$ ならば予想 (M) は正しい.

## References


[1] F. Beukers, The diophantine equation $Ax^p + By^q = Cz^r$, *Duke Math. J.* 91 (1998), 61–88.

[2] F. Beukers and H. P. Schlickewei, The equation $x + y = l$ in finitely generated groups, *Acta Arith.* 78 (1996), 189–199.

[3] Z. F. Cao, A note on the Diophantine equation $a^x + b^y = c^z$, *Acta Arith.* 91 (1999), 85–93.

[4] Z. F. Cao and X. L. Dong, On the Terai-Jeśmanowicz conjecture, *Publ. Math. Debrecen*, 61 (2002), 253–265.

[5] ——, An application of a lower bound for linear forms in two logarithms to the Terai-Jeśmanowicz conjecture, *Acta Arith.* 110 (2003), 153–164.

[6] M. Cipu and M. Mignotte, On a conjecture on exponential Diophantine equations, *Acta Arith.* 140 (2009), 251–270.

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

[8] H. Darmon and L. Merel, Winding quotients and some variants of Fermat's last Theorem, *J. Reine. Angew. Math.* 490 (1997), 81–100.

[9] M. -J. Deng and G. L. Cohen, A note on a conjecture of Jeśmanowicz, *Colloq. Math.* 86 (2000), 25–30.

[10] H. Darmon and A. Granville, On the equations $z^m = F(x,y)$ and $Ax^p + By^q = Cz^r$, *Bull. London Math. Soc.* 27 (1995), 513–543.

[11] J. -H. Evertse, H. P. Schlickewei and W. M. Schmidt, Linear equations in variables which lie in a multiplicative group, *Annals of Math.* 155 (2002), 1–30.

[12] A. O. Gel'fond, Sur la divisibilité de la différence des puissances de deux nombres entiers par une puissance d´un idéal premier, *Mat. Sb.* 7 (1940), 7–25.

[13] Y. -D. Guo and M. -H. Le, A note on Jeśmanowicz conjecture concerning Pythagorean numbers, *Comment. Math. Univ. St. Pauli*, 44 (1995), 225–228.

[14] T. Hadano, On the Diophantine equation $a^x + b^y = c^z$, *Math. J. Okayama Univ.* 19, No.1 (1976/77), 25–29.
[15] N. Hirata-Kohno, $S$-Unit Equations and Integer Solutions to Exponential Diophantine Equations (Analytic Number Theory and Surrounding Areas). *RIMS Kokyuroku*, 1511 (2006), 92–97.
[16] L. Jeśmanowicz, Several remarks on Pythagorean numbers, *Wiadom. Mat.* 1 (1955/56), 196–202 (in Polish).
[17] C. Ko, On Pythagorean numbers, *Sichuan Daxue Xuebao*, 1 (1958), 73–80 (in Chinese).
[18] ——, On Jesmanowicz conjecture, *Sichuan Daxue Xuebao*, 2 (1958), 31–40 (in Chinese).
[19] M. -H. Le, A note on Jeśmanowicz conjecture, *Colloq. Math.* 69 (1995), 47–51.
[20] ——, On Jeśmanowicz conjecture concerning Pythagorean numbers, *Proc. Japan Acad. Ser. A Math. Sci.* 72 (1996), 97–98.
[21] ——, A conjecture concerning the exponential diophantine equation, *Acta Arith.* 106 (2003), 345–353.
[22] ——, A conjecture concerning the pure exponential equation $a^x + b^y = c^z$, *Acta Math. Sinica, English Series*, 21 (2004), 943–948.
[23] ——, On the Diophantine system $a^2 + b^2 = c^3$ and $a^x + b^y = c^z$ for $b$ is an Odd prime, *Acta. Math. Sinica.* No. 6, 24 (2008), 917–924.
[24] ——, A note on Jeśmanowicz' conjecture concerning primitive Pythagorean triplets, *Acta Arith.* 138 (2009), 137–144.
[25] 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).
[26] K. Mahler, Zur Approximation algebraischer Zahlen I: Über den grössten Primteiler binärer Formen, *Math. Ann.* 107 (1933), 691–730.
[27] D. R. Mauldin, A Generalization of Fermat's Last Theorem: The Beal Conjecture and Prize Problem, *Not. Amer. Math. Soc.* 44 (1997), 1436–1437.
[28] A. Makowski, On the Diophantine equation $2^x + 11^y = 5^z$, *Noridisk Mat. Tidskr.* 7 (1959), 81.
[29] M. Mignotte, A corollary to a theorem of Laurent-Mignotte-Nesterenko, *Acta Arith.* 86 (1998), 101–111.
[30] T. Miyazaki, On the conjecture of Jeśmanowicz concerning Pythagorean triples, *Bull. Austral. Math. Soc.* 80 (2009), 413–422.
[31] ——, A new conjecture on exponential Diophantine equations, submitted.
[32] ——, An analogue of Jeśmanowicz' conjecture concerning Pythagorean triples, submitted.
[33] T. Nagell, Sur une classe d'équations exponentielles, *Ark. Mat.* 3 (1958), 569–582.
[34] V. D. Podsypanin, On a propery of Pythagorean numbers, *Izv. Vyssh. Uchebn. Zaved. Mat.* 4 (1962), 130–133 (in Russian).
[35] W. Sierpiński, On the equation $3^x + 4^y = 5^z$, *Wiadom. Mat.* 1 (1955/56), 194–195 (in Polish).
[36] N. Terai, Applications of a lower bound for linear forms in two logarithms to exponential Diophantine equations, *Acta Arith.* 90 (1999), 17–35.
[37] S. Uchiyama, On the Diophantine equation $2^x = 3^y + 13^z$, *Math. J. Okayama Univ.* 19 (1976), 31–38.

Department of Mathematics and Information Sciences, Tokyo Metropolitan University, 1-1, Minami-Ohsawa, Hachioji, Tokyo 192-0397, Japan
*E-mail address*: miyazaki-takafumi@ed.tmu.ac.jp