数理解析研究所講究録
第2013巻 2016年 50-59

On an exponential equation concerning Pythagorean numbers with congruence relations

Takafumi Miyazaki
(Nihon University)

2014年 10月 30日

1 Introduction

指数型ディオファントス方程式

(abc) $$a^x + b^y = c^z$$

を考える. ここで, a, b, c は互いに素な固定された1より大の自然数, x, y, z は未知の自然数である. ディオファントス近似の一般論から, 解の個数の有限性が得られ, 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, 方程式 (abc) を解く, すなわちその解を全て決定するためには, 上記の解析的理論に合わせて様々な他の数論の手法を必要とする. 代表的なものは, 低次の代数対の理論で, 特に初等整数論である.

方程式 (abc) に関する最近の研究の多くは次に挙げるいずれかの場合を扱っている:

(I) ピタゴラス数をなす場合 (あるいは, 類似の代数関係式成す場合),

(II) 線形回帰数列の項として与えられる場合,

(III) 整数変数の多項式として与えられる場合.

この中でも場合 (I) に関する研究は多くある. ((II) については [8] 参照, (III) については [11] を参照.) 特に, ある自然数 $r \geqslant 2$ に対して $a^2 + b^2 = c^r$ を満たす三つ組み (a, b, c) を扱っている. この稿では $r = 2$ の場合を扱う. ($r > 2$ の場合については, [1, 6, 10] 等を参照.) 1956年に Jeśmanowicz [3] は次の問題を提起している.

Conjecture. 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 (abc) 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数多くあるが, 一般には未解決である. Conjecture 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 は正しいことが証明されている. 例えば, m, n が適当に大きい範囲に属する場合, n の値だけを固定する場合, m, n が線形関係式を満たす場合, などである. (例えば, [9, 13] およびこれらの参考文献を参照.)

Conjecture の研究において, $n=1$ の場合を扱う Lu [5] の結果, $m-n=1$ の場合を扱う Dem'janenko [2] の結果は m,n の境界条件を扱うものとみなせ, 他の研究にも役に立っているもので重要である. それらは論文 [9] において次のように拡張された.

Proposition 1. 次の合同式を仮定する :

$$A \equiv \epsilon \mod b.$$

ここで $A \in \{a, c\}$ かつ $\epsilon \in \{1, -1\}$ である. このとき Conjecture は正しい.

この稿では, この命題を拡張することを考える. 以下では, 自然数 N に対して, $2^{\mathrm{ord}_2(N)}$ は N を割るような最大の 2 のベキを表すことにする. 主結果は次のように述べられる.

Theorem 1. 次の合同式を仮定する :

$$A \equiv \epsilon \mod b/2^{\mathrm{ord}_2(b)}.$$

ここで A, ϵ は Proposition 1 と同様である. このとき Conjecture は正しい.

この Theorem 1 の仮定を満たす m,n の具体例を以下に挙げる. ($A \equiv \epsilon \pmod b$ の例は論文 [9] 参照.) ここでは, $A \equiv \epsilon \pmod{b/2}$ かつ $A \not\equiv \epsilon \pmod b$ となる例を挙げる.

Example 1. $A = a$ の場合を考える. t を正の奇数とする. すると, $a = \epsilon + (b/2)\,t$ を満たす様な m,n の組は次の様にして与えられる :

$$m = \frac{U_\ell + t\,V_\ell}{2}, \quad n = V_\ell.$$

ここで, ℓ は, $\epsilon = 1$ のときは偶数になり, $\epsilon = -1$ のときは奇数になる様な 1 より大の整数である. また, $\{U_\ell\}_{\geqslant 1}, \{V_\ell\}_{\geqslant 1}$ は次のように定義される線形回帰数列である :

$$\begin{aligned} &U_1 = t, \quad U_2 = t^2 + 2, \quad U_{\ell+2} = t\,U_{\ell+1} + U_\ell, \\ &V_1 = 1, \quad V_2 = t, \qquad\quad V_{\ell+2} = t\,V_{\ell+1} + V_\ell. \end{aligned}$$

例えば,

$$\begin{aligned} \epsilon = 1,\ \ell = 2; &\quad m = t^2 + 1,\ n = t, \\ \epsilon = 1,\ \ell = 4; &\quad m = t^4 + 3t^2 + 1,\ n = t(t^2+2), \\ \epsilon = -1,\ \ell = 3; &\quad m = t(t^2+2),\ n = t^2 + 1, \\ \epsilon = -1,\ \ell = 5; &\quad m = t^5 + 2t^3 + 2t^2 + 2t + 1,\ n = t^4 + 3t^2 + 1. \end{aligned}$$

上の様にして m,n が与えられるのは, 条件式 $a = \epsilon + (b/2)\,t$ を以下の様に書き換えてみるとわかる. $m^2 - n^2 = \epsilon + mnt$ において, $(U,V) = (2m - nt, n)$ と置いてみると,

$$U^2 - (t^2+4)V^2 = 4\epsilon$$

を得る. これは U, V に関するペル方程式であり, 基本解が容易に定まる場合である. すなわち, すべての (U, V) は次の関係式によって与えられる :

$$\frac{U+V\sqrt{t^2+4}}{2} = \begin{cases} u_t\text{の偶数べキ} & (\epsilon = 1 \text{ のとき}), \\ u_t\text{の奇数べキ} & (\epsilon = -1 \text{ のとき}). \end{cases}$$

ここで, $u_t = \frac{t+\sqrt{t^2+4}}{2}$ は二次体 $\mathbb{Q}(\sqrt{t^2+4})$ の基本単数である.

Example 2. $A = c$ の場合を考える. $t \geqslant 3$ を奇数とする. すると, $c = 1 + (b/2)\,t$ を満たす様な m, n の組は次の様にして与えられる :

$$m = \frac{U_\ell + t\,V_\ell}{2}, \quad n = V_\ell,$$

ここで $\ell > 1$ は整数, $\{U_\ell\}_{\geqslant 1}, \{V_\ell\}_{\geqslant 1}$ は次のようにして定義される線形回帰数列である :

$$\begin{aligned} &U_1 = t, \quad U_2 = t^2 - 2, \quad U_{\ell+2} = t\,U_{\ell+1} - U_\ell, \\ &V_1 = 1, \quad V_2 = t, \qquad\quad V_{\ell+2} = t\,V_{\ell+1} - V_\ell. \end{aligned}$$

例えば

$$\begin{aligned} &\ell = 2; \quad m = t^2 - 1,\ n = t, \\ &\ell = 3; \quad m = t^3 - 2t,\ n = t^2 - 1, \\ &\ell = 4; \quad m = t^4 - 3t^2 + 1,\ n = t^3 - 2t. \end{aligned}$$

上記の例より, Theorem 1 は Proposition 1 の真の拡張になっていることがわかる. Theorem 1 の証明の方針は Proposition 1 とは大きく異なる点がある. Proposition 1 や上の Example でみたように特殊な場合では, m, n はペル方程式の理論からその明示的な表現が得られる. この事実は, 解の良い lower bound を得るのに役に立つ. 一方で, 一般的な場合には, 対応するペル方程式の扱いが難しいことから, 同じような表現が得ることが出来ず, よって解の lower bound が得られない. この点を処理することが新たしい部分であり, また, その手法はかなり一般的であり, 他の既知の研究結果の別証明を与える.

残りのセクションにおいて Theorem 1 の証明の概略を述べる. 証明は大きく二つに分けることが出来る. 一つは, 方程式の解の偶奇性を明らかにすることである. このために必要な補題等を次の節で挙げていく. 二つ目は, 解の偶奇性が与えられたときに方程式を解くことである. これは Section 3 において述べられる. Section 4 において, Theorem 1 の $\epsilon = 1$ の場合の証明の概略を述べる. Section 5 では, $\epsilon = -1$ の場合において必要となる Baker の手法について述べる. 最後の節では, Theorem 1 に関連する結果について述べる.

2 解の偶奇性

Conjecture の研究においては, 解の偶奇性を調べることが重要である. いま我々の方程式は次の様に書ける :

$$(\mathrm{mn}) \qquad (m^2 - n^2)^x + (2mn)^y = (m^2 + n^2)^z.$$

ここで, m, n は前節で述べた条件を満たす固定の自然数であり, x, y, z は未知の自然数である. いま, Lu [5] の結果から, n は 1 より大であると仮定してよい. すると, 整数 $\alpha \geqslant 1$, $\beta \geqslant 2$, $e \in \{1, -1\}$ と正の奇数 i, j を以下の様に定めることが出来る :

$$\text{(eo)} \qquad \begin{cases} m = 2^{\alpha} i, & n = 2^{\beta} j + e \quad (m \text{ が偶数のとき}), \\ m = 2^{\beta} j + e, & n = 2^{\alpha} i \quad (m \text{ が奇数のとき}). \end{cases}$$

この記号を使って, 次を示すことが出来る.

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

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

Lemma 3. (x, y, z) を方程式 (mn) の解とする. x と z は偶数であると仮定し, $X = x/2, Z = z/2$ と書く. すると X, Z は奇数である.

Lemma 1 と Lemma 2 は, 方程式 (mn) を適当な 2 のベキを法とする合同式を考察することによって証明される. また, Lemma 3 は数論幾何に基づく理論によって証明される. (これらについては [7] 参照.) また次の事実も必要になる. それは, $a = m^2 - n^2, c = m^2 + n^2$ に (eo) を代入した式を適当な 2 のベキを法とする合同式を考察することから従う.

Lemma 4. 次の合同式が成り立つ.

$$c - 1 \equiv 0 \mod 2^{\min\{2\alpha, \beta+1\}}$$

および

$$\begin{cases} a + 1 \equiv 0 \mod 2^{\min\{2\alpha, \beta+1\}} & (m \text{ が偶数のとき}), \\ a - 1 \equiv 0 \mod 2^{\min\{2\alpha, \beta+1\}} & (m \text{ が奇数のとき}). \end{cases}$$

3 一つの命題

ここでは次の命題を証明する.

Proposition 2. m, n $(m > n)$ は互いに素かつ偶奇性が異なる自然数とする. このとき次が成り立つ.

(i) m を偶数とする. すると次の連立方程式

$$\begin{cases} (m^2 + n^2)^Z + (m^2 - n^2)^X = 2^{2Y-1} m^{2Y}, \\ (m^2 + n^2)^Z - (m^2 - n^2)^X = 2n^{2Y} \end{cases}$$

はただ一つの自然数解 $X = Y = Z = 1$ を持つ.

(ii) n を偶数とする. すると次の連立方程式

$$\begin{cases} (m^2 + n^2)^Z + (m^2 - n^2)^X = 2m^{2Y}, \\ (m^2 + n^2)^Z - (m^2 - n^2)^X = 2^{2Y-1} n^{2Y} \end{cases}$$

はただ一つの自然数解 $X = Y = Z = 1$ を持つ.

証明. 始めの主張だけ示す. (X,Y,Z) を自然数解とする. まず, 二つの方程式を法を m^2-n^2 とする合同式で考察する. 前者からは,

$$(m^2+n^2)^Z \equiv 2^{2Y-1}m^{2Y} \mod m^2-n^2$$

を得る. 後者からは

$$(m^2+n^2)^Z \equiv 2n^{2Y} \equiv 2m^{2Y} \mod m^2-n^2$$

を得る. これらから,

$$2^{2Y-1}m^{2Y} \equiv 2m^{2Y} \mod m^2-n^2.$$

ここで, 両辺に共通に現れている m のベキは法とは互いに素なので, 結局

$$2^{2Y-2} \equiv 1 \mod m^2-n^2. \tag{cong}$$

を得る. 証明のためには, 上記合同式が実際には等式であることを示せばよい. 実際, もしそうであるならば, $Y=1$ となり, $X=Z=1$ が最初の方程式から従うことがわかる.

二つの方程式の差を考えることで,

$$(m^2-n^2)^X = (2^{Y-1}m^Y+n^Y)(2^{Y-1}m^Y-n^Y)$$

を得る. いま $\gcd(2m,n)=1$ なので, 右辺の因子は互いに素であることがわかる. よって,

$$2^{Y-1}m^Y+n^Y = s^X, \quad 2^{Y-1}m^Y-n^Y = t^X$$

と書ける. ここで, s,t $(s>t)$ は奇数の自然数であり, $st=m^2-n^2$ を満たす. $m>n$ かつ $s \geqslant t+2$ なので,

$$s^X+t^X = 2^Y m^Y > 2^{Y-1}\cdot 2n^Y = 2^{Y-1}(s^X-t^X),$$

が成り立つので

$$\begin{aligned}(2^{Y-1}+1)\,t^X &> (2^{Y-1}-1)\,s^X \\ &\geqslant (2^{Y-1}-1)(t+2)^X \\ &\geqslant (2^{Y-1}-1)\,(t^X+2X\,t^{X-1})\end{aligned}$$

を得る. これよりすぐに, $t>(2^{Y-1}-1)X$ となり, 特に

$$t \geqslant 2^{Y-1}.$$

この評価式から, (cong) の左辺はたかだか $t^2<st=m^2-n^2$ であることがわかる. 従って, (cong) は等式である. (証明終わり)

4 $\epsilon=1$ の場合

ここでは, $\epsilon=1$ の場合に Theorem 1 の証明を完成させる. $A=a$ の場合だけ述べる ($A=c$ の場合も同様である).

$r=0,1,2,\ldots,\mathrm{ord}_2(b)$ に対して, 次の命題を数学的帰納法によって示す:

$$a \equiv 1 \mod b/2^r \text{ ならば Conjecture は正しい.}$$

帰納法の第一のステップ, すなわち $r=0$ の場合は, Proposition 1 から従う. よって第二のステップを示せばよい. いま, ある r $(0 \leqslant r < \mathrm{ord}_2(b))$ に対して上記の命題が成立することを仮定する. すなわち

$$a \equiv 1 \mod b_0 \text{ ならば Conjecture は正しい.}$$

ここで, $b_0 = b/2^r$. 次に, 合同式

$$a \equiv 1 \mod b_0/2$$

を仮定する. 上記合同式から, 自然数 t を用いて

$$a = 1 + (b_0/2)t$$

と書ける. いま帰納法の仮定から, t は奇数であるとしてよい. $b_0/2$ は $b/2 = mn$ の約数であるので,

$$b_0/2 = m_0 n_0,$$

と書ける. ここで m_0, n_0 はそれぞれ m, n の (正の) 約数である. (これらは一意的に定まる.) よって, 条件式 $a = 1 + (b_0/2)t$ は

$$m^2 - n^2 = 1 + m_0 n_0 t \tag{1}$$

と書ける. いま, t は奇数なので, 上式から, m_0 または n_0 は偶数であることがわかるので,

$$\mathrm{rad}(m_0) = \mathrm{rad}(m), \quad \mathrm{rad}(n_0) = \mathrm{rad}(n) \tag{2}$$

が成り立つ. 但し, $\mathrm{rad}(N)$ で N の素因数分解に現れる素数の積を表す ($\prod_{p|N} p$ のことである). (1) から次の合同式が従う.

$$m^2 \equiv 1 \mod n_0, \tag{3}$$

$$n^2 \equiv -1 \mod m_0. \tag{4}$$

これらと前節に用意した補題を用いていくつかの補題を示していく.

Lemma 5. m は奇数とする. すると, (eo) の記号の下で, 不等式 $\alpha \geqslant \beta + 1$ が成り立つ.

証明. t は奇数なので, Lemma 4 と (1) から,

$$\min\{2\alpha, \beta+1\} \leq \mathrm{ord}_2(a-1) = \mathrm{ord}_2(m_0 n_0 t) \leq \mathrm{ord}_2(mn) = \alpha.$$

これは主張の不等式を与える. (証明終わり)

以下, (x, y, z) を方程式 (mn) の自然数解とする.

Lemma 6. z は偶数である.

証明. 方程式 (mn) を法 m_0 の合同式で考える. すると, $(-n^2)^x \equiv (n^2)^z \pmod{m_0}$ を得る. いま, (4) を使うと, この合同式は, $(-1)^z \equiv 1 \pmod{m_0}$ となる. よって, もし $m_0 \geqslant 3$ ならば z は偶数になることがわかる. もし $m_0 \leq 2$ ならば, (2) より $m_0 = 2$ となるので, つまり, m は 2 のベキになる. ところで, その様な場合には Conjecture は正しいことが証明されているので ([7, Theorem 11.2] 参照), 結論を得る. (証明終わり)

Lemma 7. x は偶数である.

証明. もし m が偶数ならば, 方程式 (mn) を法を 4 とする合同式で考えることから結論が従う. よって m を奇数と仮定してよい. すると, Lemma 1, Lemma 5 および Lemma 6 から, x が偶数であることがわかる. (証明終わり)

Lemma 3, Lemma 6 および Lemma 7 から, $x = 2X$, $z = 2Z$ と書ける. ここで X, Z は正の奇数である. 次に, 正の偶数 D, E を次の様に定義する :

$$(2mn)^y = DE.$$

ここで

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

$y > 1$ および $\gcd(D, E) = 2$ が成り立つことは容易に観察される. D, E の形は完全に決定される.

Lemma 8. 次のことが成り立つ.

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

証明. m と n は偶奇が異り, X は奇数なので,

$$\begin{cases} D \equiv 0, \quad E \equiv 2 \mod 4 & (m \text{ が偶数のとき}), \\ D \equiv 2, \quad E \equiv 0 \mod 4 & (m \text{ が奇数のとき}) \end{cases}$$

がわかる. さらに, (3) および (4) から

$$D \equiv \pm 2 \mod n_0, \quad E \equiv \pm 2 \mod m_0$$

がわかる. これらの合同式から, $D/2$ が n_0 とは素であること (よって, (2) より, n と素である), また, $E/2$ は m_0 と素であること (よって, (2) より, m と素である) がわかる. ゆえに, 関係式 $(D/2)(E/2) = 2^{y-2}m^y n^y$ から, m^y が $D/2$ を割り, かつ n^y が $E/2$ を割ることがわかる. さらに, 2 のベキ 2^{y-2} は, m が偶数のときには $D/2$ を割り, m が奇数のときには $E/2$ を割ることがわかる. (証明終わり)

Lemma 9. y は偶数である.

証明. 始めに m は偶数とする. すると Lemma 8 より, $(1 + m_0 n_0 t)^X = (D - E)/2 = 2^{y-2}m^y - n^y$ がわかる. この式を法 m_0 の合同式で考えると, $n^y \equiv -1 \pmod{m_0}$ を得る. これを二乗すると, (4) より, $(-1)^y \equiv 1 \pmod{m_0}$. この合同式から, Lemma 6 の証明と同じようにして, y が偶数であることが結論できる.

次に m が奇数である場合を考える. すると Lemma 8 より, $(1 + m_0 n_0 t)^X = (D - E)/2 = m^y - 2^{y-2}n^y$ がわかる. この式を法 n_0 の合同式で考えると, $m^y \equiv 1 \pmod{n_0}$. ここで仮に y を奇数であると仮定する. これより矛盾を導く. いま, (3) より, $m \equiv 1 \pmod{n_0}$ を得る. このことと, (1) および t, m の両方が奇数であるこ

とを用いると次のように矛盾を導くことが出来る：

$$\begin{aligned}\mathrm{ord}_2(n_0) &\le \mathrm{ord}_2(m-1)\\ &< \mathrm{ord}_2(m^2-1)\\ &= \mathrm{ord}_2(n^2+m_0n_0t)\\ &= \mathrm{ord}_2(n_0)+\mathrm{ord}_2(n^2/n_0+m_0t)=\mathrm{ord}_2(n_0).\end{aligned}$$

よって y が偶数であると結論出来る. (証明終わり)

Lemma 9 から, $y=2Y$ (Y は自然数) と書ける. すると, Lemma 8 および Proposition 2 から, $X=Y=Z=1$ を得る. (証明終わり)

5 対数一次形式

この節では, $\epsilon=-1$ の場合に必要となる Baker の手法について述べる. $\epsilon=-1$ の証明は $\epsilon=1$ の場合と方針は同じである. すなわち, 「解 x,y,z がすべて偶数であること」を示し, 「Proposition 2 を適用する」ことである. $\epsilon=-1$ の場合には, 前者を示すためにある特殊な場合を扱う必要が生ずる. それは, $y=1$ の場合である.

$y=1$ のときには, 方程式は

$$a^x+b=c^z$$

となる. a,b は大きさはほとんど同じ (例えば, $1/2<\frac{\log a}{\log b}<2$ の意味で) ことから, 上式における左辺の大きさは a^x であると思える. 従って, 上式においては, 二つの累乗数 a^x, c^z は大きさがほとんど同じであるといえる. 言い換えれば, 対数の一次形式 $z\log c-x\log a$ は "小さい". このとき, 指数変数 x,z の上界を得るために Baker の手法が有効であることが知られている. 実際, $\max\{x,z\}$ は $(\log c)(\log\log c)$ の定数倍で抑えることが出来る. 以下では, Baker の手法がどのように適用されるかをみる. (x,z が小さすぎる状況は考えなくてよいことに注意する.)

Baker 理論は, 対数の一次形式に関する理論である. いま, γ_1,γ_2 を 1 より大の有理数とし, b_1,b_2 を自然数とする. 次の対数の線形形式を考える：

$$\Lambda=b_2\log\gamma_2-b_1\log\gamma_1\quad(>0).$$

いま, この値がとても小さい正数であるとする. すると, $\log\Lambda$ は負である. Baker 理論は, この値の下界を次の形で与える：

$$\log\Lambda>-\mathcal{C}\cdot\mathrm{h}(\gamma_1)\cdot\mathrm{h}(\gamma_2)\cdot\log\max\{x,z\}.$$

ここで, $\mathcal{C}$ は正の明示的な絶対定数であり, h は (ナイーブな) 高さ関数で, 互いに素な自然数 P,Q に対して, $\mathrm{h}(P/Q)=\log\max\{P,Q\}$ と定められる ([4] を参照). これを, 我々の場合に当てはめると, $(\gamma_1,\gamma_2)=(a,c)$ かつ $(b_1,b_2)=(x,z)$ と置くとき,

$$\log(z\log c-x\log a)>-\mathcal{C}\cdot(\log a)(\log c)\cdot\log\max\{x,z\}$$

を得る.

一方で, 前に述べたように, $z\log c-x\log a$ は "小さい"はずであるから, その上界を見つけることが出来るはずである. いま, 我々の方程式の両辺を a^x で割ると,

$1+\frac{b}{a^x}=\frac{c^z}{a^x}$ となるので,

$$z\log c - x\log a = \log\left(\frac{c^z}{a^x}\right) = \log\left(1+\frac{b}{a^x}\right) < \frac{b}{a^x} < \frac{a^2}{a^x} = a^{-(x-2)}.$$

よって,

$$\log(z\log c - x\log a) < -(x-2)\log a$$

を得る. これを Baker 理論で得られた下界と比べることによって,

$$\frac{x-2}{\log\max\{x,z\}} < \mathcal{C}\log c$$

となる. いま, a, c および a^x, c^z はそれぞれ大きさがほとんど同じであることから, x, z もほとんど大きさが同じであることがわかる. したがって, 上記の不等式の左辺の分母はだいたい $\log x$ に等しく, それによって, x の (よって z の)c を用いたバウンドが得られる. この様にして得られる解のバウンドを用いて, $y=1$ の場合を処理することができる. (特に, Lemma 2 が使える.)

6 一つの拡張

この最後の節では, Theorem 1 に関連ある結果について述べる. Theorem 1 の証明と同様にして次を示すことが出来る :

Theorem 2. b_0 を b の正の約数とする. b_0 は $\mathrm{rad}(b)$ で割り切れると仮定する. さらに, b_0 はあまり小さくないと仮定する. A, ϵ は Proposition 1 と同様であるとする. いま, Conjecture は, 次の合同式 :

$$A \equiv \epsilon \mod b_0$$

が成り立つときに, 成立すると仮定する. このとき, 合同式

$$A \equiv \epsilon \mod b_0/2$$

が成り立つならば, Conjecture は正しい.

上記の b_0 の仮定 :「b_0 はあまり小さくない」は, $\epsilon=-1$ かつ n が 2 のベキの場合に必要で, 「不等式 $b_0 > \frac{4m}{\mathrm{p}(m)}$ が成り立つこと」であると述べられる. ここで $\mathrm{p}(m)$ は m の最小の素因数を表す.

Theorem 1 は, Proposition 1 と Theorem 2 ($b_0 = b, b/2, \ldots, b/2^{\mathrm{ord}_2(b)-1}$ に適用) から従うことがわかる.

Theorem 2 の証明の方針は Theorem 1 と同じであるが, $\epsilon=-1$ の場合には, 前節でみた Baker の手法を $y=1$ とは異なる場面で使う部分が生ずる. 詳細は省略するが, それは, x, z が偶数とわかっているときに小さい一次形式をみつけ (Lemma 8 を使う), それに Baker 理論を適用し処理している.

References

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

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

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

[4] M. Laurent, 'Linear forms in two logarithms and interpolation determinants II', *Acta Arith.* **133** (2008), 325–348.

[5] 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).

[6] F. Luca, 'On the system of Diophantine equations $a^2+b^2=(m^2+1)^r$ and $a^x+b^y=(m^2+1)^z$', *Acta Arith.* **153** (2012), 373–392.

[7] T. Miyazaki, Jeśmanowicz' conjecture on exponential Diophantine equations, *Funct. Approx. Comment. Math.* **45** (2011), 207–229.

[8] T. Miyazaki, 'Upper bounds for solutions of an exponential Diophantine equation', to appear in Rocky Mountain Journal of Mathematics.

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

[10] T. Miyazaki, 'A note on the article of F. Luca "On the system of Diophantine equations $a^2+b^2=(m^2+1)^r$ and $a^x+b^y=(m^2+1)^z$" (Acta Arith. 153 (2012), 373-392)', *Acta Arith.* **164** (2014), 31–42.

[11] T. Miyazaki and A. Togbé, 'The Diophantine equation $(2am-1)^x+(2m)^y=(2am+1)^z$', *Int. J. Number Theory* **8** (2012), 2035–2044.

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

[13] N. Terai, 'On Jeśmanowicz' conjecture concerning primitive Pythagorean triples', *J. Number Theory* **141** (2014), 316–323.

Department of Mathematics College of Science and Technology, Nihon University 1-8-14 Kanda-Surugadai, Chiyoda-ku, Tokyo 101-8308, Japan

E-mail address: miyazaki-takafumi@math.cst.nihon-u.ac.jp