Jeśmanowicz予想について

樋口　勇気

平成19年1月31日

目 次

1 Introduction

Jeśmanowicz 予想は 1956 年にポーランド人数学者 L. Jeśmanowicz により提出された、ある種の指数型不定方程式に関する未解決問題である. この予想は次のように簡潔に述べられる.

予想 1.0.1 (L. Jeśmanowicz(1956)). (a,b,c) を $a^2+b^2=c^2$ を満たす正の整数の組としたとき、$a^x+b^y=c^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである.

この種の Diophantus 問題は主張の簡潔さに反して、その証明はしばしば大変複雑になるが、Jeśmanowicz 予想についても、現在までのところ様々な条件を付けた上での部分的な結果しか得られていない. 本修士論文では、その中で興味深い結果をいくつか紹介する. この問題は 1956 年の W. Sierpiński による次の定理にさかのぼる.

定理 1.0.2. (Sierpiński [13]). $3^x+4^y=5^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである.

これを受けて、Jeśmanowicz は同年、次の結果を得た.

定理 1.0.3. (Jeśmanowicz [7]). $(a,b,c)=(5,12,13)$, $(7,24,25)$, $(9,40,41)$, $(11,60,61)$ のとき、$a^x+b^y=c^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである.

これらの結果から、Jeśmanowicz は冒頭の予想を提出した. 上の二人の結果は、1965 年に Dem′janenko により次のように一般化された.

定理 1.0.4. (Dem′janenko [2]). n を任意の正の整数とし、$a=2n+1$, $b=2n(n+1)$, $c=2n(n+1)+1$ とする. このとき、$a^x+b^y=c^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである.

さらに、1984 年には Grytczuk と Grelak によって、次の結果が得られた.

定理 1.0.5. (Grytczuk , Grelak [4] Th.1) m を任意の正の整数とし、$a=4m^2-1$, $b=4m$, $c=4m^2+1$ とする. このとき、$a^x+b^y=c^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである.

不定方程式 $a^2+b^2=c^2$ の任意の整数解は、整数 s,t を用いて、$a=s^2-t^2$, $b=2st$, $c=s^2+t^2$ と表すことができる. 定理 1.0.4 は $s>t>0$, $\gcd(s,t)=1$, $2\mid st$, $s-t=1$ の場合に対応し、定理 1.0.5 は $s>t>0$, $\gcd(s,t)=1$, $2\mid st$, $t=1$ の場合に対応している. 1993 年には K. Takakuwa と Y. Asaeda によって、次の結果が得られた.

定理 1.0.6. (Takakuwa , Asaeda [16] Th.1). m を奇数とし、p は奇素数で、$p\equiv 3 \pmod 4$ とする. このとき、$y\neq 1$ ならば、$(4m^2-p^2)^x+(4mp)^y=(4m^2+p^2)^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである.

また、同年に Takakuwa は次の結果も得ている.

定理 1.0.7. (Takakuwa [15] Th.1). m を奇数とし、p は奇素数で、$p \equiv 5 \pmod 8$ とする. このとき、y が偶数ならば、$(4m^2-p^2)^x+(4mp)^y=(4m^2+p^2)^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである.

1995 年には、Le が Pell 方程式の性質を利用した次の結果を得た.

定理 1.0.8. (Le [9]). (a,b,c) を $a^2+b^2=c^2$ かつ $\gcd(a,b,c)=1$ であるような正の整数の組とする. このとき、$4 \parallel ab$ かつ $c=p^n$（ p：奇素数 , $n \geq 1$ ）を満たすならば、$a^x+b^y=c^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである.

Le は翌年、Baker の手法を用いることで、次のような結果を得ている.

定理 1.0.9. (Le [10]) s,t を $s>t$, $\gcd(s,t)=1$, かつ $2 \mid st$ を満たす正の整数とし、$a=s^2-t^2$, $b=2st$, $c=s^2+t^2$ とする. このとき、$2 \parallel s$, $t \equiv 3 \pmod 4$, かつ $s \geq 81t$ ならば、$a^x+b^y=c^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである.

さらに Le は 1999 年には、$\gcd(a,b,c)$ が 1 とは限らない場合に対する、以下の重要な結果も得ている.

定理 1.0.10. (Le [11] Cor.1) s,t を $s>t$, $\gcd(s,t)=1$, かつ $2 \mid st$ を満たす正の整数とし、$a=s^2-t^2$, $b=2st$, $c=s^2+t^2$ とする. n を任意の正の整数とし、(x,y,z) を $(an)^x+(bn)^y=(cn)^z$ の $(2,2,2)$ ではない正の整数解とする. このとき、x,y,z はそれぞれ互いに異なる.

定理 1.0.11. (Le [11] Cor.1) n を正の整数とする. $n>1$ のとき、$n=\prod_{i=1}^{l} {p_i}^{e_i}$ と書けた場合、$C(n)=\prod_{i=1}^{l} p_i$ とする. $n=1$ のときは $C(1)=1$ とする. s,t を $s>t$, $\gcd(s,t)=1$, かつ $2 \mid st$ を満たす正の整数とし、$a=s^2-t^2$, $b=2st$, $c=s^2+t^2$ とする. このとき、$C(n) \nmid a,b,c$ ならば、$(an)^x+(bn)^y=(cn)^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである.

これらの結果の証明をこれから見ていくことにする.

末筆になりましたが、担当教官として三年間御指導して下さった雪江明彦教授には大変感謝しております. また、数学に関することから、TEX の使い方、発表の仕方など様々なことで御世話になった、早坂紀彦先輩、森本聡先輩にも感謝しております. そして、セミナーにおいて共に学んだ酒井祐貴子さん、曽根浩圭君、福井邦彦君、八木勇磨君、渡邉崇君にも感謝しています.

2　初等的アプローチ

ここでは初等的アプローチで示されたいくつかの結果を紹介する.

2.1　Sierpiński と Jeśmanowicz の結果

まず、この予想をたてるきっかけになった Sierpiński と Jeśmanowicz 自身の結果を紹介する.

定理 2.1.1. (Sierpiński [13]). $3^x + 4^y = 5^z$ の正の整数解 (x, y, z) は $(2, 2, 2)$ のみである.

定理 2.1.2. (Jeśmanowicz [7]). $(a, b, c) = (5, 12, 13)$, $(7, 24, 25)$, $(9, 40, 41)$, $(11, 60, 61)$ のとき、$a^x + b^y = c^z$ の正の整数解 (x, y, z) は $(2, 2, 2)$ のみである.

証明は少し複雑だが同様なので、定理 2.1.1 のみ証明する.

定理 2.1.1 の証明. $3^x+4^y = 5^z$ より、$3^x \equiv 1 \pmod 4$ であるので、x は偶数である. また、$1 \equiv 2^z \pmod 3$ より、z も偶数である. $x = 2x'$, $z = 2z'$ とおくと、$9^{x'}+4^y = 25^{z'}$ と書けるので、$1 + 4^y \equiv 1 \pmod 8$ となる. よって、$y \geq 2$ が得られる. また、$3^{2x'} + 4^y = 5^{2z'}$ より、$2^{2y} = (5^{z'} + 3^{x'})(5^{z'} - 3^{x'})$ と書ける. $\gcd(5^{z'} + 3^{x'}, 5^{z'} - 3^{x'}) = 2$ かつ $5^{z'} + 3^{x'} > 5^{z'} - 3^{x'}$ より、

$$\begin{cases} 5^{z'} + 3^{x'} &= 2^{2y-1} & \cdots (1) \\ 5^{z'} - 3^{x'} &= 2 & \cdots (2) \end{cases}$$

を解けばよい. $(1) + (2)$ より、$2 \cdot 5^{z'} = 2^{2y-1} + 2$ となるので、$5^{z'} = 2^{2y-2} + 1$ である.

(i) $y = 2$ の場合. $5^{z'} = 2^2 + 1 = 5$ より、$z' = 1$ となる. $y = z = 2$ より、$x = 2$ が得られる. したがって、$(x, y, z) = (2, 2, 2)$ となる.

(ii) $y \geq 3$ の場合. $2^{2y-2} \equiv 0 \pmod 8$ より、$5^{z'} \equiv 1 \pmod 8$ なので、z' は偶数である. 一方、(2) より $2^{z'} \equiv 2 \pmod 3$ となるので、z' は奇数となり矛盾する.

したがって、$3^x + 4^y = 5^z$ を満たす正の整数の組 (x, y, z) は $(x, y, z) = (2, 2, 2)$ のみである.

□

2.2　a, b, c を一つのパラメーターで表せる場合

この節では a, b, c を一つのパラメーターで表せる場合の結果を紹介する.

定理 2.2.1. (Dem′janenko [2]). n を任意の正の整数とし、$a = 2n + 1$, $b = 2n(n + 1)$, $c = 2n(n+1)+1$ とする. このとき、$a^x + b^y = c^z$ の正の整数解 (x, y, z) は $(2, 2, 2)$ のみである.

定理 2.2.2. (Grytczuk , Grelak [4] Th.1) m を任意の正の整数とし、$a = 4m^2 - 1$, $b = 4m$, $c = 4m^2 + 1$ とする. このとき、$a^x + b^y = c^z$ の正の整数解 (x, y, z) は $(2, 2, 2)$ のみである.

注 2.2.3. 定理 2.1.1 は定理 2.2.1 における $n = 1$ の場合であり、定理 2.1.2 は $n = 2, 3, 4, 5$ の場合である.

注 2.2.4. a, b, c を $s > t$, $\gcd(s, t) = 1$, かつ $2 \mid st$ を満たす正の整数 s, t を用いて、$a = s^2 - t^2$, $b = 2st$, $c = s^2 + t^2$ と表したとき、定理 2.2.1 は $s - t = 1$ の場合であり、定理 2.2.2 は $t = 1$ の場合である.

証明はほぼ同様であるので、定理 2.2.2 のみ証明する.

定理 2.2.2 **の証明.**

$$(4m^2 - 1)^x + (4m)^y = (4m^2 + 1)^z \tag{2.2.5}$$

より、$(-1)^x \equiv 1 \pmod 4$. したがって、x は偶数である. また、$(-1)^x + (4m)^y \equiv 1 \pmod{4m^2}$ であり、x は偶数であるので、$(4m)^y \equiv 0 \pmod{4m^2}$ となる. ここで、$y = 1$ と仮定する. $4m^2 \mid 4m$ より、$m = 1$ となり (2.2.5) に代入すると、$3^x + 4 = 5^z$ となるが、定理 2.1.1 よりこの式を満たす (x, z) は存在しない. したがって、$y \geq 2$ となる. x は偶数、$y \geq 2$ であり、$(4m^2 - 1)^2 \equiv (4m^2 + 1)^2 \equiv 1 \pmod{8m^2}$ であるので、(2.2.5) より $(4m^2 + 1)^z \equiv 1 \pmod{8m^2}$. したがって、$z$ は偶数である. ここで、$x = 2x', z = 2z', A = (4m^2 + 1)^{z'}, B = (4m^2 - 1)^{x'}$ とおくと (2.2.5) は $(4m)^y = (A + B)(A - B)$ となる. また、$m = 2^{k-1}m'$（$k \geq 1$, m'：奇数）とおくと $(A + B)(A - B) = 2^{(k+1)y}m'^y$ と書ける. A, B は奇数であり、$\gcd(A, B) = 1$ であるので、$\gcd(A + B, A - B) = 2$ となる. ここで、x'：偶数と仮定する. m' の任意の素因子 p (p：奇素数) に対して、$A + B \equiv 1^{z'} + (-1)^{x'} \equiv 2 \pmod p$ であるので、$p \nmid A + B$ となる. したがって、$\gcd(A + B, m') = 1$ である. また、$A + B \equiv 1^{z'} + (-1)^{x'} \equiv 2 \pmod 4$ より、$4 \nmid A + B$ も分かる. したがって、$\gcd(A + B, A - B) = 2$ より、

$$\begin{cases} A + B &= 2 \\ A - B &= 2^{(k+1)y-1}m'^y \end{cases}$$

であるが、$A + B < A - B$ となるので矛盾する. したがって、x' は奇数である. 今と同様の議論により、$\gcd(A - B, m') = 1$, $4 \nmid A - B$ が分かる. したがって、

$$\begin{cases} A + B &= 2^{(k+1)y-1}m'^y \\ A - B &= 2 \end{cases}$$

となり、上下の式の和と差を考えると、

$$\begin{cases} A &= (4m^2 + 1)^{z'} = 2^{(k+1)y-2}m'^y + 1 \\ B &= (4m^2 - 1)^{x'} = 2^{(k+1)y-2}m'^y - 1 \end{cases}$$

が得られる. $m = 2^{k-1}m'$ より、

$$(4m^2-1)^{x'} = 2^{(k+1)y-2}m'^y - 1 = 2^{2(y-1)}m^y - 1$$

となる. ここで、$y \geq 3$ と仮定すると、$8m^2 \mid 2^{2(y-1)}m^y$ より、$(4m^2-1)^{x'} \equiv -1 \pmod{8m^2}$ となる. mod $8m^2$ における $4m^2-1$ の位数は 2 であり、x' は奇数であるので、$(4m^2-1)^{x'} \equiv 4m^2-1 \equiv -1 \pmod{8m^2}$. したがって、$4m^2 \equiv 0 \pmod{8m^2}$ となり、$8m^2 \mid 4m^2$ となるので矛盾する. したがって、$y < 3$ が得られる. $y \geq 2$ であったので、$y = 2$ となる. 代入すると、$(4m^2-1)^{x'} = 4m^2-1$ となり、$x' = 1$ であるので、$x = 2$ となる. $x = y = 2$ より、$z = 2$ となる. したがって、(2.2.5) の正の整数解 (x, y, z) は $(2, 2, 2)$ のみである.

□

2.3 パラメーター s, t に条件を与えた場合

$\gcd(a, b, c) = 1$ である場合には $s > t$, $\gcd(s, t) = 1$, かつ $2 \mid st$ を満たす正の整数 s, t を用いて、$a = s^2 - t^2$, $b = 2st$, $c = s^2 + t^2$ と表せることはよく知られている. この節では $s = 2m$：偶数 , $t = p$：素数として、m, p にいくつか条件をつけた場合、

$$(4m^2-p^2)^x + (4mp)^y = (4m^2+p^2)^z \tag{2.3.1}$$

の正の整数解は $(x, y, z) = (2, 2, 2)$ のみであることを示した結果をいくつか紹介する. s を偶数とするのは、(2.3.1) より、$(-1)^x \equiv 1 \pmod 4$ が得られるので、x が偶数であることがすぐに分かるためである.

定理を紹介する前に、Legendre 記号と Jacobi 記号を定義しておく.

定義 2.3.2 (Legendre 記号). a を零でない整数とし、p を奇素数とする. このとき、Legendre 記号 (a/p) を以下で定義する. a が mod p における平方剰余であるとき、すなわち合同方程式 $x^2 \equiv a \pmod p$ が可解であるとき、$(a/p) = 1$ とし、a が mod p における平方非剰余であるとき、すなわち合同方程式 $x^2 \equiv a \pmod p$ が非可解であるとき、$(a/p) = -1$ とする. また、$p \mid a$ のとき、$(a/p) = 0$ とする.

定義 2.3.3 (Jacobi 記号). a を零でない整数とし、b を正の整数でかつ奇数とする. b が素数の積で $b = p_1 p_2 \cdots p_l$ と書けるとき (ただし、全てが異なる必要はない)、Jacobi 記号 (a/b) を Legendre 記号を用いて、

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_l}\right)$$

と定義する.

まず、$p \equiv 3 \pmod 4$ である場合の結果を紹介する.

定理 2.3.4. (Takakuwa , Asaeda [16] Th.1). m を奇数とし、p は奇素数で、$p \equiv 3 \pmod 4$ とする. このとき、$y \neq 1$ ならば、$(4m^2-p^2)^x+(4mp)^y=(4m^2+p^2)^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである.

定理 2.3.5. (Takakuwa , Asaeda [16] Th.3). m を奇数とし、p は奇素数で、$p \equiv 3 \pmod 4$ とする. このとき、m の素因子 q で $q \equiv 1 \pmod 4$ かつ

$$\left(\frac{p}{q}\right)=-1 \qquad \left(\left(\frac{*}{*}\right) \text{は Legendre 記号}\right)$$

を満たすものが存在するならば、$(4m^2-p^2)^x+(4mp)^y=(4m^2+p^2)^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである.

定理 2.3.6. (Takakuwa , Asaeda [16] Th.2). m を偶数とし、p は奇素数で、$p \equiv 3 \pmod 8$ とする. このとき、$2m+p$ が素数で、かつ $2m-p$ が素数、もしくは 1 であるならば、$(4m^2-p^2)^x+(4mp)^y=(4m^2+p^2)^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである.

定理 2.3.4 は後に記す補題の系として得られるので、ここでは証明しないことにする. 定理 2.3.5 を証明するため、次の命題を示す.

命題 2.3.7. m が奇数であり、かつ $p \equiv 3 \pmod 4$ ならば、次の (1), (2) が成り立つ.

(1) $y \equiv z \pmod 2$.

(2) $y \neq 1 \Leftrightarrow z$：偶数.

証明. (1) (2.3.1) より、$(4mp)^y \equiv (2p^2)^z \pmod{4m^2-p^2}$ となる. m と p の仮定より、Jacobi 記号を用いて、

$$\left(\frac{2^{2y}m^yp^y}{4m^2-p^2}\right)=(-1)^y=\left(\frac{2^zp^{2z}}{4m^2-p^2}\right)=(-1)^z$$

と書ける. したがって、$y \equiv z \pmod 2$ となる.

(2) (1) より、z が偶数であるならば、$y \neq 1$ である. また、z が奇数であると仮定すると、$(4m^2+p^2)^z \equiv 5 \pmod 8$ となる. x は偶数であるので、$(4m^2-p^2)^x \equiv 1 \pmod 8$ となり、(2.3.1) より、$(4mp)^y \equiv 4 \pmod 8$ が得られる. したがって、$y=1$ であるので、対偶をとれば、$y \neq 1$ ならば、z は偶数である. よって、$y \neq 1 \Leftrightarrow z$：偶数が示された. □

定理 2.3.5 の証明. r を $\bmod q$ における原始根とし、d を $p \equiv r^d \pmod q$ となる正の整数とする. 条件より、

$$-1=\left(\frac{p}{q}\right)=\left(\frac{r}{q}\right)^d$$

となるので、d は奇数であることが分かる．そのとき、mod q における p の位数は $\dfrac{q-1}{\gcd(t,q-1)}$ と等しくなり、また、$\dfrac{q-1}{\gcd(t,q-1)} \equiv 0 \pmod 4$ となる．(2.3.1) より、$(-p^2)^x \equiv p^{2z} \pmod q$ であるので、$p^{2|x-z|} \equiv 1 \pmod q$ となる．したがって、mod q における p の位数は $2|x-z|$ を割り切る．mod q における p の位数は 4 で割り切れるので、$|x-z|$ は偶数である．x は偶数であるので、z も偶数となる．命題 2.3.7 より、$y \neq 1$ が得られる．したがって、定理 2.3.4 より、(x,y,z) は $(2,2,2)$ のみである． □

次に定理 2.3.6 を証明するため、以下の命題を証明する．

命題 2.3.8. m が偶数であり、かつ $p \equiv 3 \pmod 4$ ならば、y は偶数である．

証明. (2.3.1) より、$(4mp)^y \equiv (2p^2)^z \pmod{4m^2-p^2}$ となる． m と p の仮定より、Jacobi 記号を用いて、

$$\left(\frac{2^{2y}m^yp^y}{4m^2-p^2}\right) = (-1)^y = \left(\frac{2^zp^{2z}}{4m^2-p^2}\right) = 1$$

となる．したがって、y は偶数である． □

命題 2.3.9. m が偶数であり、かつ $p \equiv 3 \pmod 8$ ならば、z は偶数である．

証明. 命題 2.3.7 より、y は偶数である．(2.3.1) より、$1 \equiv 9^z \pmod{16}$ となるので、z は偶数である． □

次の補題は今後用いることになる．

補題 2.3.10. 方程式 $X^4+Y^2=Z^4$ に正の整数解 (X,Y,Z) は存在しない．

証明は [14, Ch.2 Cor.1] でなされている．

定理 2.3.6 の証明. 命題 2.3.8 , 2.3.9 より、y と z はともに偶数である．$x=2x'$, $z=2z'$, $A=(4m^2+p^2)^{z'}+(4m^2-p^2)^{x'}$, $B=(4m^2+p^2)^{z'}-(4m^2-p^2)^{x'}$ とおく．ここで、$\gcd(A,B)=2$ であることに注意しておく．(2.3.1) より、

$$2^{2y}m^yp^y = AB \tag{2.3.11}$$

が得られる．ここで、$p \mid A$ と仮定すると、$(2m)^{2z'}+(2m)^{2x'} \equiv 0 \pmod p$ となるので、$(2m)^{2|z'-x'|} \equiv -1 \pmod p$ となる．したがって、mod 4 における $(2m)^{|z'-x'|}$ の位数は 4 であり、これは $p \equiv 3 \pmod 4$ であることに反する．よって、$p \nmid A$ が分かり、$p \mid B$ となる．$m=2^rm'$（$r \geq 1$, m'：奇数）とおくと、(2.3.11) より A,B は $m'=kl$, $\gcd(k,l)=1$ であるような正の整数 k,l を用いて、次の 2 つのどちらかの形で表すことが出来る．

(1) $A=2k^y$, $\quad B=2^{y(2+r)-1}l^yp^y$

(2) $A=2^{y(2+r)-1}k^y$, $B=2l^yp^y$

(1) の場合. $B \equiv 1-(-1)^{x'} \equiv 0 \pmod 4$ より、x' は偶数であるので、$(4m^2-p^2)^{x'} \equiv 1 \pmod{16}$ となる. したがって、$B \equiv 9^{z'}-1 \equiv 0 \pmod{16}$ となるので、z' は偶数である. よって、$4 \mid x$, $2 \mid y$, $4 \mid z$ となり、これは補題 2.3.10 に反する. したがって、(1) の場合はあり得ない.

(2) の場合. $A \equiv 1+(-1)^{x'} \equiv 0 \pmod 4$ より、x' は奇数である. $y = 2y'$ とおくと、

$$\frac{A-B}{2} = (4m^2-p^2)^{x'} = (2^{y'(2+r)-1}k^{y'})^2 - (l^{y'}p^{y'})^2$$

となるので、

$$(2m+p)^{x'}(2m-p)^{x'} = (2^{y'(2+r)-1}k^{y'} + l^{y'}p^{y'})(2^{y'(2+r)-1}k^{y'} - l^{y'}p^{y'})$$

と書ける. 条件より $2m+p$ は素数であり、$2m-p$ は素数、もしくは 1 である. また、

$$\gcd(2a+p\ ,\ 2a-p) = \gcd(2^{y'(2+r)-1}k^{y'} + l^{y'}p^{y'}\ ,\ 2^{y'(2+r)-1}k^{y'} - l^{y'}p^{y'}) = 1$$

であるので、

(2-1) $2^{y'(2+r)-1}k^{y'} + l^{y'}p^{y'} = (4m^2-p^2)^{x'}$, $2^{y'(2+r)-1}k^{y'} - l^{y'}p^{y'} = 1$

(2-2) $2^{y'(2+r)-1}k^{y'} + l^{y'}p^{y'} = (2m+p)^{x'}$, $2^{y'(2+r)-1}k^{y'} - l^{y'}p^{y'} = (2m-p)^{x'}$

のどちらかの形になる.

(2-1) の場合. 2 つの式を足すと、x' は奇数であるので、

$$2l^{y'}p^{y'} = (4m^2-p^2)^{x'} - 1 \equiv 7^{x'} - 1 \equiv 6 \pmod{16}$$

となる. したがって、$l^{y'}p^{y'} \equiv 3 \pmod{16}$ であるので、

$$1 = 2^{y'(2+r)-1}k^{y'} - l^{y'}p^{y'} \equiv 2^{y'(2+r)-1}k^{y'} - 3 \pmod 8$$

となり、$2^{y'(2+r)-1}k^{y'} \equiv 4 \pmod 8$ が分かる. k が奇数であることと、$y'(2+r)-1 \geq 2$ であることより、$y'(2+r)-1 = 2$ が得られる. したがって、$y' = 1, r = 1$ となるので、

$$\begin{aligned} 4k+lp &= (2m+p)^{x'}(2m-p)^{x'} \\ 4k-lp &= 1 \end{aligned}$$

となる. よって、$8k-1 = (2m+p)^{x'}(2m-p)^{x'}$ が得られる. この式は、$2m-p = 1$ のときのみ成り立つ可能性がある. したがって、(2-1) は (2-2) の場合に含まれている.

(2-2) の場合. 上の式から下の式を引くと、$(2m+p)^{x'} - (2m-p)^{x'} = 2l^{y'}p^{y'}$ となり、x' は奇数であるので、$2p^{x'} \equiv 0 \pmod l$ が分かる. $\gcd(p,l) = \gcd(2,l) = 1$ より、$l = 1$ となる. したがって、$k = m'$ より、

$$\begin{aligned} 2^{y'(2+r)-1}m'^{y'} + p^{y'} &= (2m+p)^{x'} \\ 2^{y'(2+r)-1}m'^{y'} - p^{y'} &= (2m-p)^{x'} \end{aligned}$$

となる. 上下の式を足すと、$2^{y'(2+r)}m'^{y'} = (2m+p)^{x'} + (2m-p)^{x'}$ となる. ここで、x' は奇数であることより、

$$d = (2m+p)^{x'-1} - (2m+p)^{x'-2}(2m-p) + \cdots + (2m-p)^{x'-1}$$

とすると、

$$(2m+p)^{x'} + (2m-p)^{x'} = 4md = 2^{2+r}m'd$$

と書ける. したがって、$y' = 1$ である. 代入すると、$2m+p = (2m+p)^{x'}$ となるので、$x' = 1$ となり、このとき $z' = 1$ である. したがって、正の整数解 (x, y, z) は $(2, 2, 2)$ のみである. □

次に、$p \equiv 1 \pmod 4$ である場合の結果を紹介する.

定理 2.3.12. (Takakuwa [15] Th.1). m を奇数とし、p は奇素数で、$p \equiv 5 \pmod 8$ とする. このとき、y が偶数ならば、$(4m^2-p^2)^x + (4mp)^y = (4m^2+p^2)^z$ の正の整数解 (x, y, z) は $(2, 2, 2)$ のみである.

定理 2.3.13. (Takakuwa [15] Th.2). m を奇数とし、p は奇素数で、$p \equiv 1 \pmod 8$ とする. また、次の (1) もしくは (2) が成り立つとする.

(1) y は偶数

(2) $m = m_1 m_2$, $\gcd(m_1, m_2) = 1$, かつ $m_1 \equiv 5 \pmod 8$ となるような正の整数 m_1, m_2 は存在しない.

このとき、$(4m^2-p^2)^x + (4mp)^y = (4m^2+p^2)^z$ の正の整数解 (x, y, z) は $(2, 2, 2)$ のみである.

系 2.3.14. (Takakuwa [15] Cor.1). m を奇数とし、p は奇素数で、$p \equiv 1 \pmod 4$ とする. このとき、$m \not\equiv 0 \pmod 3$ かつ $a \not\equiv p \pmod 3$ ならば、$(4m^2-p^2)^x + (4mp)^y = (4m^2+p^2)^z$ の正の整数解 (x, y, z) は $(2, 2, 2)$ のみである.

系 2.3.15. (Takakuwa [15] Cor.2). p を奇素数で、$p \equiv 5 \pmod 8$ とする. このとき、$m \equiv 1 \pmod 4$ ならば、$(4m^2-p^2)^x + (4mp)^y = (4m^2+p^2)^z$ の正の整数解 (x, y, z) は $(2, 2, 2)$ のみである.

系 2.3.16. (Takakuwa [15] Cor.3). p を奇素数で、$p \equiv 1 \pmod 8$ とする. このとき、$m \equiv 3 \pmod 4$ ならば、$(4m^2-p^2)^x + (4mp)^y = (4m^2+p^2)^z$ の正の整数解 (x, y, z) は $(2, 2, 2)$ のみである.

定理 2.3.17. (Takakuwa [15] Th.3). m を偶数とし、 $m = 2^s m_0$ $(s \geq 1$, $(2, m_0) = 1)$ とおく. p を奇素数で、$p \equiv 5 \pmod 8$ とする. $2m+p$, $2m-p$ はそれぞれ素数であると仮定する. また、$m \equiv 2 \pmod 4$ のときは、さらに次の (1) もしくは (2) が成り立つと仮定する.

(1) y は偶数

(2) $y \neq 1$ かつ $m_0 = m_1 m_2$, $\gcd(m_1, m_2) = 1$, $m_1 \equiv 1 \pmod 4$, かつ $m_1 \neq 1$ となるような正の整数 m_1, m_2 は存在しない

このとき、$(4m^2 - p^2)^x + (4mp)^y = (4m^2 + p^2)^z$ の正の整数解 (x, y, z) は $(2, 2, 2)$ のみである.

まず、定理 2.3.12 を証明する. その証明に必要な次の命題を示す.

命題 2.3.18. m が奇数であり、かつ $p \equiv 1 \pmod 4$ ならば、z は偶数である.

証明. (2.3.1) より、$(4mp)^y \equiv (2p^2)^z \pmod{4m^2 - p^2}$ となる. m と p の仮定より、Jacobi 記号を用いて、

$$\left(\frac{2^{2y} m^y p^y}{4m^2 - p^2}\right) = 1 = \left(\frac{2^z p^{2z}}{4m^2 - p^2}\right) = (-1)^z$$

となる. したがって、z は偶数である. □

定理 2.3.12 の証明. 命題 2.3.18 より、z は偶数である. $x = 2x', z = 2z', A = (4m^2 + p^2)^{z'} + (4m^2 - p^2)^{x'}, B = (4m^2 + p^2)^{z'} - (4m^2 - p^2)^{x'}$ とおくと、(2.3.1) より、

$$2^{2y} m^y p^y = AB \tag{2.3.19}$$

と書ける. $\gcd(A, B) = 2$ であることと (2.3.19) より A, B は $m = kl$, $\gcd(k, l) = 1$ であるような正の整数 k, l を用いて、次の 4 つのいずれかの形で表すことが出来る.

(1) $A = 2k^y p^y \quad , \quad B = 2^{2y-1} l^y$

(2) $A = 2k^y \quad , \quad B = 2^{2y-1} l^y p^y$

(3) $A = 2^{2y-1} k^y p^y$, $B = 2l^y$

(4) $A = 2^{2y-1} k^y \quad , \quad B = 2l^y p^y$

(1) の場合. $B \equiv 1 - (-1)^{x'} \equiv 0 \pmod 4$ より、x' は偶数であるので、

$$B \equiv -(-2p^2)^{x'} \equiv 2^{2y-1} l^y \pmod{4m^2 + p^2}$$

となる. ここで、Jacobi 記号を用いると、

$$\left(\frac{-(-2p^2)^{x'}}{4m^2 + p^2}\right) = \left(\frac{2^{2y-1} l^y}{4m^2 + p^2}\right)$$

となるが、それぞれを計算すると m と p の仮定より、左辺は 1、右辺は -1 となり矛盾である. したがって、(1) の場合は起こりえない.

(2) の場合. (1) の場合と同様の方法で起こりえないことが分かる.

(3) の場合. $A \equiv 1 + (-1)^{x'} \equiv 0 \pmod 4$ より、x' は奇数である. $A \equiv 5^{z'} + 3^{x'} \equiv 0 \pmod 8$ と x' は奇数であることより、z' も奇数である.

$$A = (4m^2 + p^2)^{z'} + (4m^2 - p^2)^{x'} \equiv 0 \pmod p$$

より、$(2m)^{|x-z|} \equiv -1 \pmod p$ である. x' と z' は奇数であるので、$4 \mid |x - z|$ となり、ある正の整数 r を用いて、$|x - z| = 4r$ と書ける. すると、mod p における $(2m)^r$ の位数は 8 となるが、これは、$p \equiv 5 \pmod 8$ に反する.

(4) の場合. (3) の場合と同様の方法で x', z' は奇数であることが分かる. ここで、$y \geq 4$ と仮定すると、$A \equiv 13^{z'} - 5^{x'} \equiv 0 \pmod{16}$ が得られる. $13^1 \equiv 13 \pmod{16}, 13^3 \equiv 5 \pmod{16}, 5^1 \equiv 5 \pmod{16}, 5^3 \equiv 13 \pmod{16}$ であるので、$z' \equiv x' + 2 \pmod 4$ であることが分かる. したがって、次の 2 つの場合が考えられる.

(4-1) $x' \equiv 1 \pmod 4$, $z' \equiv 3 \pmod 4$

(4-2) $x' \equiv 3 \pmod 4$, $z' \equiv 1 \pmod 4$

(4-1) の場合. $(4m^2 \pm p^2)^4 \equiv (4 \pm 9)^4 \equiv 1 \pmod{16}$ であるので、

$$B = 2l^y p^y \equiv (4m^2 + p^2)^3 - (4m^2 - p^2) \equiv 13^3 + 5 \equiv 10 \pmod{16}$$

となる. したがって、$l^y p^y \equiv 5 \pmod 8$ が得られる.

(4-2) の場合. (4-1) の場合と同様の方法で、$l^y p^y \equiv 5 \pmod 8$ が得られる.

したがって、y は奇数であることになるが、これは、定理の仮定に矛盾する. よって、$y = 2$ が得られる. $m = kl$ より、

$$A = (4m^2 + p^2)^{z'} + (4m^2 - p^2)^{x'} = 2^3 k^2 = 8k^2 \leq 8m^2 = (4m^2 + p^2) + (4m^2 - p^2)$$

であるので、$x' = z' = 1$ となる. したがって、(2.3.1) の正の整数解 (x, y, z) は $(2, 2, 2)$ のみである.

□

次に、定理 2.3.13 を証明する. まず、必要な命題を示す.

命題 2.3.20. m が奇数であり、かつ $p \equiv 1 \pmod 4$ ならば、$y \neq 1$ である.

証明. x は偶数であるので、$(4m^2 - p^2)^x \equiv 1 \pmod 8$ となる. また、m が奇数かつ $p \equiv 1 \pmod 4$ あるので、命題 2.3.18 より、z は偶数となり、$(4m^2 + p^2)^z \equiv 1 \pmod 8$ である. したがって、(2.3.1) より、$(4mp)^y \equiv 0 \pmod 8$ となるので、$y \neq 1$ である. □

定理 2.3.13 の証明. 命題 2.3.18 , 2.3.20 より、z は偶数かつ $y \neq 1$ である. x', z', A, B, k, l を定理 2.3.12 の証明と同様のものとすると、A, B は次の 4 つのいずれかの形で表すことが出来る.

(1) $A = 2k^y p^y$, $B = 2^{2y-1} l^y$

(2) $A = 2k^y \quad , \quad B = 2^{2y-1}l^y p^y$

(3) $A = 2^{2y-1}k^y \quad , \quad B = 2l^y p^y$

(4) $A = 2^{2y-1}k^y p^y \ , \ B = 2l^y$

(1)、(2) の場合. 定理 2.3.12 の証明における (1) の場合と同様の方法で起こりえないことが示される.

(3) の場合. $y \geq 3$ と仮定すると、定理 2.3.12 の証明における (4) の場合と同様の方法で $l^y p^y \equiv 5 \pmod 8$ が得られる. $p \equiv 1 \pmod 8$ であるので、$l^y \equiv 5 \pmod 8$ となる. したがって、y が奇数かつ $l \equiv 5 \pmod 8$ であるので、定理の仮定に矛盾する. よって、$y = 2$ であることが分かる. $m = kl$ より、

$$A = (4m^2 + p^2)^{z'} + (4m^2 - p^2)^{x'} = 2^3 k^2 = 8k^2 \leq 8m^2 = (4m^2 + p^2) + (4m^2 - p^2)$$

であるので、$x' = z' = 1$ となる. したがって、$(x, y, z) = (2, 2, 2)$ が得られる.

(4) の場合. 定理 2.3.12 の証明における (4) の場合と同様の方法で x', z' : 奇数、$y = 2$ が得られる. このとき、

$$\frac{A + B}{2} = (4m^2 + p^2)^{z'} = 4k^2 p^2 + l^2 \leq 4m^2 p^2 + m^2$$

となる. また、

$$(4m^2 + p^2)^3 = 64m^6 + 48m^4 p^2 + 12m^2 p^4 + p^6 > 4m^2 p^2 + m^2$$

である. したがって、$(4m^2 + p^2)^{z'} < (4m^2 + p^2)^3$ となり、z' は奇数より、$z' = 1$ となる. そのとき、$4m^2 + p^2 = 4k^2 l^2 + p^2 = 4k^2 p^2 + l^2$ となり、$4k^2(l^2 - p^2) = l^2 - p^2$ が得られる. よって、$4k^2 = 1$ となるが、このような正の整数 k は存在しない. したがって、(4) は起こり得ない.

□

次に系 2.3.14 , 2.3.15 をそれぞれ証明する. 系 2.3.16 の証明は系 2.3.15 の証明と同様にして出来るので、ここでは省略する.

系 2.3.14 の証明. $p \equiv 1 \pmod 4$ より、$p \neq 3$ である. したがって、$m \not\equiv 0 \pmod 3$ より、$m^2 \equiv p^2 \equiv 1 \pmod 3$ となる. また、$a \not\equiv p \pmod 3$ より、$ap \equiv -1 \pmod 3$ である. したがって、(2.3.1) より、$(-1)^y \equiv (-1)^z$ となるので、$y \equiv z \pmod 2$ となる. 命題 2.3.9 より、z は偶数なので、y も偶数となる. したがって、定理 2.3.12 , 2.3.13 より、正の整数解 (x, y, z) は $(2, 2, 2)$ のみである. □

系 2.3.15 の証明. (2.3.1) より、$(2p^2)^y \equiv (2p^2)^z \pmod{2m - p}$ となる. $2m - p \equiv 5 \pmod 8$ より、

$$\left(\frac{2}{2m - p}\right) = -1$$

となる. したがって、

$$\left(\frac{(2p^2)^y}{2m-p}\right) = (-1)^y = \left(\frac{(2p^2)^z}{2m-p}\right) = (-1)^z$$

が得られる. 命題 2.3.18 より、z は偶数なので、y も偶数となる. したがって、定理 2.3.12 より、正の整数解 (x, y, z) は $(2, 2, 2)$ のみである. □

定理 2.3.17 を証明する. まず、その証明に必要な 2 つの命題を示す.

命題 2.3.21. $m \equiv 2 \pmod 4$ であるとする. そのとき、

(1) $p \equiv 1 \pmod 8$ ならば、$y \neq 1$.

(2) $p \equiv 5 \pmod 8$ ならば、$y \neq 1 \Leftrightarrow z$：偶数.

証明. (1) (2.3.1) より、$(4mp)^y \equiv 0 \pmod{16}$ が得られる. $4 \nmid mp$ より、$y \neq 1$ となる.
(2) $y^2 \equiv 9 \pmod{16}$ より、$(4mp)^y \equiv 9^z - 1 \pmod{16}$ が得られる. そのとき、$y \neq 1 \Leftrightarrow (4mp)^y \equiv 0 \pmod{16} \Leftrightarrow 9^z \equiv 1 \pmod{16} \Leftrightarrow z$：偶数. □

命題 2.3.22. $m \equiv 0 \pmod 4$ かつ $p \equiv 5 \pmod 8$ ならば、y, z は偶数である.

証明. (2.3.1) より、$1 \equiv 9^z \pmod{16}$ であるので、z は偶数である. また、(2.3.1) より、$(2p^2)^y \equiv (2p^2)^z \pmod{2m-p}$ が分かる. $2m - p \equiv 3 \pmod 8$ であるので、

$$\left(\frac{2}{2m-p}\right) = -1$$

となるから、$(-1)^y = 1$ が得られる. したがって、y も偶数である. □

定理 2.3.17 の証明. 命題 2.3.21, 2.3.22 より、z は偶数である. x', z', A, B, k, l を定理 2.3.12 の証明と同様のものとすると、A, B は次の 4 つのいずれかの形で表すことが出来る.

(1) $A = 2k^y \quad , \quad B = 2^{y(2+s)-1} l^y p^y$

(2) $A = 2^{y(2+s)-1} k^y \quad , \quad B = 2l^y p^y$

(3) $A = 2^{y(2+s)-1} k^y p^y \ , \ B = 2l^y$

(4) $A = 2k^y p^y \quad , \quad B = 2^{y(2+s)-1} l^y$

(1) の場合. $B \equiv 1 - (-1)^{x'} \equiv 0 \pmod 4$ であるので、x' は偶数である. そのとき、$B \equiv 9^{z'} - 1 \equiv 0 \pmod 4$ となるので、z' も偶数である. また、$m \equiv 0 \pmod 4$ とすると、命題 2.3.22 より、y は偶数である. $m \equiv 2 \pmod 4$ とすると、$A \equiv 2 \equiv 2k^y \pmod{16}$ となるので、$k^y \equiv 1 \pmod 8$ が得られる. y：奇数と仮定すると、$k \equiv 1 \pmod 8$ となり、この場合 $b \neq 1$ であるので、定理の仮定に反する. したがって、y は

偶数である. よって、$4 \mid x$, $2 \mid y$, $4 \mid z$ となり、これは補題 2.3.10 に反する. したがって、(1) は起こりえない.

(2) の場合. $A \equiv 1 + (-1)^{x'} \equiv 0 \pmod 4$ であるので、x' は奇数である. そのとき、$A \equiv 9^{z'} - 9 \equiv 0 \pmod 4$ となるので、z' も奇数である. また、$m \equiv 0 \pmod 4$ とすると、命題 2.3.22 より、y は偶数である. $m \equiv 2 \pmod 4$ とすると、$B \equiv 2 \equiv 2l^y p^y \pmod{16}$ となるので、$l^y p^y \equiv 1 \pmod 8$ が得られる. y：奇数と仮定すると、$l \equiv 5 \pmod 8$ となり、定理の仮定に反する. したがって、y は偶数である. $y = 2y'$ とおく.

$$\frac{A-B}{2} = (4m^2 - p^2)^{x'} = (2^{y'(2+s)-1}k^{y'})^2 - (l^{y'}p^{y'})^2$$

であるので、

$$(2a+p)^{x'}(2a-p)^{x'} = (2^{y'(2+s)-1}k^{y'} + l^{y'}p^{y'})(2^{y'(2+s)-1}k^{y'} - l^{y'}p^{y'}) \tag{2.3.23}$$

となる. $2a+p$, $2a-p$ はそれぞれ素数であり、

$$\gcd(2a+p, 2a-p) = \gcd(2^{y'(2+s)-1}k^{y'} + l^{y'}p^{y'}, 2^{y'(2+s)-1}k^{y'} - l^{y'}p^{y'}) = 1$$

であるので、次の 2 つのうち、どちらかの形になる.

$$\begin{aligned} 2^{y'(2+s)-1}k^{y'} + l^{y'}p^{y'} &= (4m^2 - p^2)^{x'} \\ 2^{y'(2+s)-1}k^{y'} - l^{y'}p^{y'} &= 1 \end{aligned} \tag{2.3.24}$$

$$\begin{aligned} 2^{y'(2+s)-1}k^{y'} + l^{y'}p^{y'} &= (2m+p)^{x'} \\ 2^{y'(2+s)-1}k^{y'} - l^{y'}p^{y'} &= (2m-p)^{x'} \end{aligned} \tag{2.3.25}$$

(2.3.24) の場合. $2l^{y'}p^{y'} \equiv (4m^2 - p^2)^{x'} - 1 \equiv -1 \pmod{4m^2 - p^2}$ であるので、m と p の仮定より、

$$\left(\frac{-1}{4m^2 - p^2}\right) = \left(\frac{2l^{y'}p^{y'}}{4m^2 - p^2}\right)$$

となるが、両辺をそれぞれ計算すると、左辺は -1 となり、右辺は 1 となるので矛盾する. したがって、(2.3.24) は起こりえない.

(2.3.25) の場合. $(2m+p)^{x'} + (2m-p)^{x'} = 2^{y'(2+s)}k^{y'}$ となる. x' は奇数であるので、

$$\begin{aligned} &(2m+p)^{x'} + (2m-p)^{x'} \\ &\quad = ((2m+p) + (2m-p))((2a+p)^{x'-1} - \cdots + (2a-p)^{x'-1}) \\ &\quad = 4aC_1 = 2^{2+s}C_2 \end{aligned}$$

と書ける. ただし、C_1, C_2 はこの式を満たすような奇数である. したがって、$2^{2+s}C_2 = 2^{y'(2+s)}k^{y'}$ であるので、$2+s = y'(2+s)$ となる. よって、$y' = 1$ となり、$y = 2$ が得られる. そのとき、

$$A = (4m^2 + p^2)^{z'} + (4m^2 - p^2)^{x'} = 2^{3+2s}k^2 \leq 8m^2 = (4m^2 + p^2) + (4m^2 - p^2)$$

であるので、$x' = z' = 1$ となり、$(x, y, z) = (2, 2, 2)$ が得られる.

(3) の場合. (2) の場合と同様の方法で x', z' は奇数であることが分かる. したがって、$4 \mid |x - z|$ が得られるので、ある正の整数 r を用いて、$|x - z| = 4r$ と書ける. $A \equiv (2m)^z + (2m)^x \equiv 0 \pmod{p}$ であるから、$(2m)^{|x-z|} \equiv -1 \pmod{p}$ となる. そのとき、$((2m)^r)^4 \equiv -1 \pmod{p}$ となり、mod p における $(2m)^r$ の位数は 8 であることが分かる. しかし、これは $p \equiv 5 \pmod{8}$ であることに矛盾する. したがって、(3) は起こりえない.

(4) の場合. (1) の場合と同様の方法で x', z' は偶数であることが分かる. あとは、(3) の場合と同様の方法で (4) は起こりえないことがわかる.

□

2.4 $c = p^n$ の場合

ここでは、Pell 方程式の性質を利用して得られた結果を紹介する.

まず、記号 $\|$ について定義する.

定義 2.4.1. m を零でない整数とし、p を素数とする. このとき、ある正の整数 l に対し、$p^l \mid m$ かつ $p^{l+1} \nmid m$ であるならば、$p^l \parallel m$ と書く.

定理 2.4.2. (Le [9]). s, t を $s > t$, $\gcd(s, t) = 1$, かつ $2 \mid st$ を満たす正の整数とし、$a = s^2 - t^2$, $b = 2st$, $c = s^2 + t^2$ とする. このとき、$2 \parallel st$ かつ $c = p^n$ （ p：奇素数 , $n \geq 1$ ）を満たすならば、$a^x + b^y = c^z$ の正の整数解 (x, y, z) は $(2, 2, 2)$ のみである.

定理を証明するための準備をする. まず、$k > 1$ かつ $4 \nmid k$ であるような整数 k に対して、$V(k)$ を

$$V(k) = \prod_{q \mid k} (1 + \chi(q))$$

と定める. ただし、q は k の全ての素因子を走り、$\chi(q)$ は以下で定まるものとする.

$$\chi(q) = \begin{cases} 0 & (q = 2) \\ (-1)^{\frac{q-1}{2}} & (q \neq 2). \end{cases}$$

次に、ある種の Pell 方程式に関する、4 つの補題を紹介する.

補題 2.4.3. k を $k > 1$ かつ $4 \nmid k$ であるような整数とする. このとき、方程式

$$X_1{}^2 + Y_1{}^2 = k \ , \ X_1, Y_1 \in \mathbb{Z} \ , \ \gcd(X_1, Y_1) = 1 \tag{2.4.4}$$

の解 (X_1, Y_1) の個数はちょうど $4V(k)$ 個である.

補題 2.4.5. k を $k>1$, $4\nmid k$, かつ $2\nmid k$ であるような整数とする. このとき、方程式

$$X^2+Y^2=k^Z\ ,\ X,Y,Z\in\mathbb{Z}\ ,\ \gcd(X,Y)=1\ ,\ Z>0$$

の全ての解 (X,Y,Z) は以下のように与えることができる.

$$Z\in\mathbb{N}\ ,\ X+Y\sqrt{-1}=(X_1+Y_1\sqrt{-1})^Z \text{ もしくは } Y+X\sqrt{-1}=(X_1+Y_1\sqrt{-1})^Z$$

ただし、(X_1,Y_1) は (2.4.4) の全ての解を走るものとする.

補題 2.4.6. $D>1$ を整数とし、p を $p\nmid D$ であるような素数とする. このとき、方程式

$$X^2+DY^2=p^Z\ ,\ X,Y,Z\in\mathbb{Z}\ ,\ \gcd(X,Y)=1\ ,\ Z>0 \tag{2.4.7}$$

が解をもつならば、$X_1>0$, $Y_1>0$ かつ $Z_1\le Z$（Z は (2.4.7) の全ての解を走る）であるような唯一の解 (X_1,Y_1,Z_1) が存在する. 解 (X_1,Y_1,Z_1) を (2.4.7) の最小解とよぶ. さらに、(2.4.7) の全ての解は以下のように与えることができる.

$$Z=Z_1r\ ,\ X+Y\sqrt{-D}=\lambda_1(X_1+\lambda_2Y_1\sqrt{-D})^r\ ,\ r\in\mathbb{N}\ ,\ \lambda_1,\lambda_2\in\{-1,1\}.$$

補題 2.4.8. $c=p^n$ とする. このとき、$(X_1,Y_1,Z_1)=(s-t,1,n)$ は方程式

$$X^2+bY^2=p^Z\ ,\ X,Y,Z\in\mathbb{Z}\ ,\ \gcd(X,Y)=1\ ,\ Z>0 \tag{2.4.9}$$

の最小解である.

補題 2.4.8 のみ証明する. 補題 2.4.3 は [6, Ch.6 Th.7.1,7.4]、補題 2.4.5 は [12, Ch.15]、補題 2.4.6 は [1] においてそれぞれ証明がなされている.

補題 2.4.8 の証明. 明らかに、$(X,Y,Z)=(s-t,1,n)$ は (2.4.9) の解である. 補題 2.4.6 より、$(X_1,Y_1,Z_1)\neq(s-t,1,n)$ と仮定すると、$n=Z_1r$ となるようなある整数 $r>1$ が存在する. ${X_1}^2+b{Y_1}^2=p^{Z_1}$ より、

$$s^2+t^2=c=p^n\ge p^{2Z_1}\ge(1+b)^2=(1+2st)^2>4(s^2+t^2)$$

となるので、矛盾する. したがって、$(s-t,1,n)$ は (2.4.9) の最小解である. □

定理 2.4.2 の証明. (x,y,z) を $a^x+b^y=c^z$ の正の整数解とする. 以下、次のように場合分けをして考える.

(1) $2\nmid x$ かつ $2\mid y$

(2) $2\nmid x$ かつ $2\nmid y$

(3) $2\mid x$ かつ $2\mid y$

(4) $2 \mid x$ かつ $2 \nmid y$

(1) の場合. $\left(\frac{*}{*}\right)$ を Jacobi 記号とすると、$2 \nmid x$ かつ $2 \mid y$ より、$\left(\frac{-a}{c}\right) = 1$ が得られる. 一方 $2 \parallel st$ より、$c \equiv 5 \pmod 8$ となる. したがって、

$$\left(\frac{-a}{c}\right) = \left(\frac{t^2 - s^2}{s^2 + t^2}\right) = \left(\frac{2t^2}{s^2 + t^2}\right) = \left(\frac{2}{s^2 + t^2}\right) = \left(\frac{2}{c}\right) = -1$$

となり、矛盾する. よって、(1) の場合は起こりえない.

(2) の場合. $\left(\frac{*}{*}\right)$ を Jacobi 記号とすると、$2 \nmid x$ かつ $2 \nmid y$ より、$\left(\frac{-ab}{c}\right) = 1$ が得られる. 一方 $c \equiv 5 \pmod 8$ より、

$$\begin{aligned}\left(\frac{-ab}{c}\right) &= \left(\frac{2st(t^2 - s^2)}{s^2 + t^2}\right) = \left(\frac{4st^2}{s^2 + t^2}\right) = \left(\frac{4st}{s^2 + t^2}\right) \\ &= \left(\frac{2(s+t)^2}{s^2 + t^2}\right) = \left(\frac{2}{s^2 + t^2}\right) = \left(\frac{2}{c}\right) = -1\end{aligned}$$

となるので、矛盾する. よって、(2) の場合は起こりえない.

(3) の場合. $2 \mid x$ かつ $2 \mid y$ より、$a^x + b^y \equiv 1 \pmod 8$ となる. また、$c \equiv 5 \pmod 8$ であるので、$5^z \equiv 1 \pmod 8$ より、z は偶数である. $x = 2x', y = 2y', z = 2z'$ とおくと、$(X, Y, Z) = (a^{x'}, b^{y'}, z')$ は方程式

$$X^2 + Y^2 = c^{2Z} \ , \ X, Y, Z \in \mathbb{Z} \ , \ \gcd(X, Y) = 1 \ , \ Z > 0$$

の解である. c は奇素数のべきであるので、補題 2.4.3 , 2.4.5 より、次の 4 つの場合が得られる.

$$\begin{aligned} a^{x'} + b^{y'}\sqrt{-1} &= \lambda_1(a + \lambda_2 b\sqrt{-1})^{z'} \\ a^{x'} + b^{y'}\sqrt{-1} &= \lambda_1(b + \lambda_2 a\sqrt{-1})^{z'} \\ b^{y'} + a^{x'}\sqrt{-1} &= \lambda_1(a + \lambda_2 b\sqrt{-1})^{z'} \\ b^{y'} + a^{x'}\sqrt{-1} &= \lambda_1(b + \lambda_2 a\sqrt{-1})^{z'} \end{aligned} \tag{2.4.10}$$

ただし、$\lambda_1, \lambda_2 \in \{-1, 1\}$ である.

$z' = 1$ とすると、(2.4.10) より、$x' = y' = 1$ となるので、$(x, y, z) = (2, 2, 2)$ が得られる.

$z' > 1$ かつ $2 \mid z'$ と仮定すると、$a, b > 1$ かつ $\gcd(a, b) = 1$ より、(2.4.10) はありえない.

$z' > 1$ かつ $2 \nmid z'$ と仮定すると、(2.4.10) より、

$$a^{x'} + b^{y'}\sqrt{-1} = \lambda_1(a + \lambda_2 b\sqrt{-1})^{z'} \ , \ \lambda_1, \lambda_2 \in \{-1, 1\}$$

となるので、次の 2 つの式を得る.

$$a^{x'} = \lambda_1 a \sum_{i=0}^{(z'-1)/2} \binom{z'}{2i+1} a^{2i}(-b^2)^{(z'-1)/2-i}, \tag{2.4.11}$$

$$b^{y'} = \lambda_1\lambda_2 b \sum_{i=0}^{(z'-1)/2} \binom{z'}{2i+1} a^{z'-2i-1}(-b^2)^i. \tag{2.4.12}$$

$2 \nmid a$, $2 \mid b$, $2 \nmid z'$ であるから、(2.4.12) から $y = 2$ を得る. さらに $z > 2$ ゆえ、$a^2 + b^2 = c^2$ から $x > 2$ であり、(2.4.11) から $z' \equiv 0 \pmod{a}$ である. q を a の素因子として、任意の $i \in \mathbb{N}$ に対し、$q^\alpha \parallel a$, $q^\beta \parallel z'$ かつ $q^{\gamma_i} \parallel (2i+1)$ とする. $q \geq 3$ かつ任意の $i \in \mathbb{N}$ に対し、

$$\gamma_i \leq \frac{\log(2i+1)}{\log q} < 2i$$

であるから、$i = 1, \cdots, (z'-1)/2$ に対して、

$$\binom{z'}{2i+1} a^{2i} = z' \binom{z'-1}{2i} \frac{a^{2i}}{2i+1} \equiv 0 \pmod{q^{\beta+1}} \tag{2.4.13}$$

が成り立つ. (2.4.11) , (2.4.13) から、a の任意の素因子 q に対して $\beta = \alpha(x'-1)$ をえるが、これは、

$$z' \equiv 0 \pmod{a^{x'-1}} \tag{2.4.14}$$

を意味する. $a^x + b^y = c^z$ と (2.4.14) から、

$$c^{x+2} > a^x + b^2 = a^x + b^y = c^z \geq c^{2a^{x'-1}}$$

であるので、

$$x + 2 > 2a^{x'-1}$$

を得る. しかし、$a \geq 3$ かつ $x > 2$ であるから、これは不可能である.

(4) の場合. $2 \mid x$ かつ $2 \nmid y$ より、 $(X, Y, Z) = (a^{x/2}, b^{(y-1)/2}, nz)$ は (2.4.9) の整数解である. 補題 2.4.6 , 2.4.8 から次式をえる.

$$a^{x/2} + b^{(y-1)/2}\sqrt{-b} = \lambda_1((s-t) + \lambda_2\sqrt{-b})^z. \tag{2.4.15}$$

ただし、$\lambda_1, \lambda_2 \in \{-1, 1\}$ である.

z が偶数のとき、(2.4.15) から $b^{(y-1)/2} \equiv 0 \pmod{s-t}$ である. すると $a^2 + b^2 = c^2$, $a = s^2 - t^2$, $b = 2st$, $c = s^2 + t^2$ から $s - t = 1$ とわかる. 定理 2.2.1 より、この場合は定理が成立することが分かる.

z が奇数のとき、$c \equiv 5 \pmod 8$ より $a^x \equiv 1 \pmod 8$ かつ $c^z \equiv 5 \pmod 8$ であり、$a^x + b^y = c^z$ から $y = 1$ を得る. 一方で (2.4.15) から次の式が成立する.

$$\frac{a^x}{s-t} = (s-t)^{(x/2)-1}(s+t)^{x/2} = \lambda_1 \sum_{i=0}^{(z-1)/2} \binom{z}{2i+1} (s-t)^{2i}(-b)^{(z-1)/(2-i)}. \tag{2.4.16}$$

$x = 2$ なら、$c = s^2 + t^2 < (s^2 - t^2)^2 + 2st = a^2 + b = c^z < c^2$ となり、これは矛盾である. $x > 2$ なら、$z \equiv 0 \pmod{s-t}$ である. q を $s - t$ の素因子として、任意の

$i \in \mathbb{N}$ に対し、$q^{\alpha} \parallel s-t, q^{\beta} \parallel z$ かつ $q^{\gamma_i} \parallel (2i+1)$ とする．$2 \nmid (s-t), q \geq 3$ かつ任意の $i \in \mathbb{N}$ に対して、$\gamma_i \leq (\log(2i+1))/(\log q) < 2$ であるから、(2.4.16) および $i = 1, \cdots, (z-1)/2$ に対して、

$$\binom{z}{2i+1}(r-s)^{2i} = z\binom{z-1}{2i}\frac{(r-s)^{2i}}{2i+1} \equiv 0 \pmod{q^{\beta+1}}$$

が成り立つから、$\beta = \alpha\left(\frac{x}{2}-1\right)$ と分かる．このことは、

$$z \equiv 0 \pmod{(s-t)^{(x/2)-1}} \tag{2.4.17}$$

を意味する．$y=1$ であったから、$a^x + b^y = c^z$ と (2.4.17) より任意の奇数 z_1 に対して、

$$c^x > a^x + b = c^z = c^{(s-t)^{(x/2)-1}z_1} \tag{2.4.18}$$

が成り立つ．$s-t \geq 3$ かつ $x \geq 4$ であるから、(2.4.18) より $s-t=3$, $x=4$, $z_1 = 1$, $z=3$ である．この場合、(2.4.16) は $(s+t)^2 = b-3 = 2st-3$ となるが、これは矛盾である．したがって、証明が完了したことになる．

□

2.5 $\gcd(a,b,c)=1$ を仮定しない場合

今までは、$\gcd(a,b,c)=1$ であるような結果を見てきた．ここでは、$\gcd(a,b,c)=1$ を仮定しない結果をいくつか紹介する．

$N>1$ を整数とし、$N = \prod_{i=1}^{l} {p_i}^{e_i}$ と素因数分解されるとする．このとき、$C(N) = \prod_{i=1}^{l} p_i$ とする．また、$C(1)=1$ とする．

定理 2.5.1. (M. Deng , G. L. Cohen [3] Th.1) k を任意の正の整数とし、$a = 2k+1$, $b = 2k(k+1)$, $c = 2k(k+1)+1$ とする．a を素数のべきと仮定し、n を $C(b) \mid n$ もしくは $C(n) \nmid b$ を満たす正の整数であるとする．このとき、$(an)^x + (bn)^y = (cn)^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである．

定理 2.5.2. (M. Deng , G. L. Cohen [3] Th.2) n を任意の正の整数としたとき、$(a,b,c) = (3,4,5)$, $(5,12,13)$, $(7,24,25)$, $(9,40,41)$, $(11,60,61)$ に対して、$(an)^x + (bn)^y = (cn)^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである．

定理 2.5.1 は Dem′janenko の結果を部分的に拡張したものと言え、定理 2.5.2 は Sierpiński と Jeśmanowicz の結果の一般化と言える．

まず、定理 2.5.1 を証明する．その前に証明に必要な 2 つの補題を示す．

補題 2.5.3. (a,b,c) を $a^2 + b^2 = c^2$ を満たす正の整数の組とする．このとき、$z \geq \max(x,y)$ ならば、$a^x + b^y = c^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである．

証明. $z=1$ と仮定すると、条件より $x=y=1$ となる. しかし、$(a+b)^2 > a^2+b^2 = c^2$ より、$a+b>c$ となるので $(x,y,z)=(1,1,1)$ は解ではない. したがって、$z \geq 2$ が分かる. ここで、$x \leq y$ としても一般性を失わないので、$x \leq y$ とする. $y=1$ のとき、$x=1$ となり、$a^x+b^y = a+b < a^2+b^2 = c^2 \leq c^z$ より、$(1,1,z)$ という解は存在しない. $y \geq 2$ のとき、

$$\begin{aligned} a^x + b^y &= (a^2)^{\frac{x}{2}} + (b^2)^{\frac{y}{2}} \\ &\leq (a^2)^{\frac{y}{2}} + (b^2)^{\frac{y}{2}} \qquad (2.5.4) \\ &\leq (a^2+b^2)^{\frac{y}{2}} \qquad (2.5.5) \\ &= c^y \\ &\leq c^z \qquad (2.5.6) \end{aligned}$$

となる. ここで、(2.5.4) の等号成立条件は $x=y$ であり、(2.5.5) の等号成立条件は $y=2$ であり、(2.5.6) の等号成立条件は $y=z$ であるので、$a^x+b^y=c^z$ となるのは (x,y,z) は $(2,2,2)$ のときのみである.

□

補題 2.5.7. p を奇素数とし、a,b を互いに素であるような整数とする. このとき $a+b$ と $\dfrac{a^p+b^p}{a+b}$ の最大公約数は 1 または p である.

証明. q を $a+b$ の素因子とすると、$q \nmid a$ かつ $b \equiv -a \pmod{q}$ となる. したがって、

$$\frac{a^p+b^p}{a+b} = a^{p-1} - a^{p-2}b + \cdots + b^{p-1} \equiv pa^{p-1} \pmod{q}.$$

が得られる. よって、q が $\dfrac{a^p+b^p}{a+b}$ の素因子ならば、$q \mid p$ であるから補題は示された. □

定理 2.5.1 の証明. 定理 2.2.1 , 補題 2.5.3 から、$n>1$ かつ $z < \max(x,y)$ のときを考えればよい. 仮定により $a^2+b^2=c^2$ かつ $a^2 = b+c$, $c=b+1$, $b=k(a+1)$, $c=k(a-1)+a$ が成立しているから、a,b,c はどの 2 つも互いに素である. さらに $(an)^x+(bn)^y=(cn)^z$ の成立を仮定することで矛盾を導く. 証明は n と c が互いに素である場合とそうでない場合の 2 つに大きく分かれており、各場合に対してさらにいくつかの場合分けを行う.

(1) $\gcd(n,c)=1$ の場合.

$x=y$ ならば $z<x$ であり、 $(an)^x+(bn)^y=(cn)^z$ から $n^{x-z}(a^x+b^x)=c^z$ ゆえ $\gcd(n,c)>1$ となり矛盾する. よって $x \neq y$ のときを考える.

(1-1) $x>y$ の場合.

$n^y(n^{x-y}a^x+b^y)=n^zc^z$ より、$z \geq y$ かつ $z<x$ である.

(1-1-1) $n \nmid b^y$ の場合.

$n^{x-y}a^x+b^y=n^{z-y}c^z$ であるから $z>y$ はあり得ず、$z=y$ であり、$n^{x-z}a^x+b^z=c^z$ である. $k^z \equiv (-k)^z \pmod{a}$ かつ $\gcd(a,k)=1$ より、z は偶数である. $z=2z_1$ とすると、

$$n^{x-z}a^x = c^z - b^z = (c^{z_1}+b^{z_1})(c^{z_1}-b^{z_1})$$

である. 右辺の 2 つの因子の両方が同時に a で割り切れることはないので、片方が a^x で割り切れることになる. しかし、

$$a^x > a^z = a^{2z_1} = (c+b)^{z_1} \geq c^{z_1} + b^{z_1} > c^{z_1} - b^{z_1}$$

であるので、矛盾が生じる.

(1-1-2) $n \mid b^y$ の場合.

$C(n) \nmid b$ であるから $C(b) \mid n$ である. b の素因数分解を $b = \prod_{i=1}^{s} r_i^{\gamma_i}$ とすると、各 $i = 1, \cdots, s$ に対して、$\nu_i \geq 1$ となるような ν_i を用いて、$n = \prod_{i=1}^{s} r_i^{\nu_i}$ と表せる. すると、任意の $i = 1, 2, \cdots, s$ に対して、$t_i \geq 1$, $0 \leq l_i < \nu_i$ であるような整数 t_i , l_i を用いて、$\gamma_i y = t_i \nu_i + l_i$ と表すことができる.

(1-1-2-1) 任意の $i = 1, 2, \cdots, s$ に対して、$x > y + t_i$ の場合.

$$\prod_{i=1}^{s} r_i^{\nu_i(y+t_i)} \left(\prod_{i=1}^{s} r_i^{\nu_i(x-y-t_i)} \cdot a^x + \prod_{i=1}^{s} r_i^{l_i} \right) = \prod_{i=1}^{s} r_i^{\nu_i z} \cdot c^z \tag{2.5.8}$$

であり、 $\gcd(n, c) = 1$ かつ任意の $i = 1, 2, \cdots, s$ に対し、$l_i < \nu_i$ であるから $r_i \mid c$ である. したがって、$z = y + t_1 = \cdots = y + t_s$ であり、$t_1 = \cdots = t_s = t$ であるから (2.5.8) より、

$$\prod_{i=1}^{s} r_i^{\nu_i(x-y-t_i)} \cdot a^x + \prod_{i=1}^{s} r_i^{l_i} = c^z$$

が分かる. よって任意の $i = 1, \cdots, s$ に対して、$l_i = 0$ であり、次式を満たす.

$$\frac{\nu_1}{\gamma_1} = \cdots = \frac{\nu_s}{\gamma_s} = \frac{y}{t} = \frac{y'}{t'}. \tag{2.5.9}$$

ただし、ここで y' と t' は互いに素である. 同様にして (2.5.8) から次式を得る.

$$n^{x-z} a^x + 1 = c^z. \tag{2.5.10}$$

z が偶数なら、$z = 2z_1$ とおけば $n^{x-z} a^x = (c^{z_1} + 1)(c^{z_1} - 1)$ を得る. 右辺の 2 つの因子の両方が同時に a で割り切れることはないので、片方が a^x で割り切れることになる. しかし、

$$a^x > a^z = a^{2z_1} = (b+c)^{z_1} > c^{z_1} + 1 > c^{z_1} - 1$$

であるので、これは不可能である.

z を奇数とする. (2.5.10) から $b^{y'(x-z)} a^{xt'} = (c^z - 1)^{t'} = ((b+1)^z - 1)^{t'}$ であるから、(2.5.9) を用いて $n = b^{y'/t'}$ を得ることができる. b は偶数であるから $b \nmid z$ であり、したがって $(b+1)^z - 1$ はちょうど b で割り切れる. よって $y'(x-z) = t'$ である. y' と t' は互いに素であるから、$y' = 1$ かつ $x = z + t'$ であり、また (2.5.9) から $yt' = t$ である. さらに $z = y + t = y(1 + t')$ であることから、t' は偶数であり、x は奇数である. $x = 2x_1 + 1$ と書くと、(2.5.10) から $n^{x-z} = n^{t'} = b^{y'} = b$ であるから、

$$c^z - 1 = ba^x = a(c-1)(b+c)^{x_1} = a(c-1)(2c-1)^{x_1}$$

が得られる. したがって、$a(-1)^{x_1} \equiv 1 \pmod{c}$ となるので、$c \mid (a+1)$ または $c \mid (a-1)$ であるから、$c > a+1$ より、これは不可能である.

(1-1-2-2) 少なくとも 1 つの $i = 1, \cdots, s$ に対して、$x \leq y + t_i$ である場合.

この場合は簡単に矛盾を導くことができる. $x \leq y + t_1$ かつ $i = 2, \cdots, s$ ($i \geq 2$ である場合) に対して、$x > y + t_i$ であるとする. このとき (2.5.8) より、

$$r_1^{\nu_1 x} \prod_{i=2}^{s} r_i^{\nu_i(y+t_i)} \left(\prod_{i=2}^{s} r_i^{\nu_i(x-y-t_i)} \cdot a^x + r_1^{\nu_1(y+t_1-x)} \prod_{i=1}^{s} r_i^{l_i} \right) = \prod_{i=1}^{s} r_i^{\nu_i z} \cdot c^z$$

を得る. しかし $x > z$ であるので、これは $r_1 \mid \prod_{i=2}^{s} r_i^{\nu_i z} \cdot c^z$ を意味し、矛盾である.

(1-2) $x < y$ の場合.

この時、$(an)^x + (bn)^y = (cn)^z$ は $n^x(a^x + n^{y-x}b^y) = n^z c^z$ となる. したがって、$y > z \geq x$ である.

(1-2-1) $n \nmid a^x$ の場合.

$z > x$ はあり得ないから $z = x$ であり、$n^{y-z}b^y = c^z - a^z$ を得る. $k = 1$ なら $a = 3$, $b = 4$, $c = 5$ であり、この等式を mod 4 で考える. $k > 1$ なら、mod $(k+1)$ で考える. どちらの場合も z が偶数でなければならないことが分かるので、$z = 2z_1$ と書くことができる.

$k = 1$ のとき、$n^{y-z}4^y = 5^z - 3^z = (5^{z_1} + 3^{z_1})(5^{z_1} - 3^{z_1})$ である. 右辺の因子は共に偶数であるが、両方が同時に 4 で割り切れることはない. したがって、片方は 2^{2y-1} で割り切れる. しかし、

$$2^{2y-1} > 2^{2z-1} = 2^{4z_1-1} \geq 2^{3z_1} = (5+3)^{z_1} \geq 5^{z_1} + 3^{z_1} > 5^{z_1} - 3^{z_1}$$

であるから、これは矛盾である.

次に $k > 1$ とする. このとき $n^{y-z}b^y = (c^{z_1} + a^{z_1})(c^{z_1} - a^{z_1})$ であり、$b = 2k(k+1)$, $k \mid (c-a) \mid (c^{z_1} - a^{z_1})$ かつ $\gcd(c^{z_1} + a^{z_1}, c^{z_1} - a^{z_1}) = 2$ である. z_1 が偶数であるか、z_1 が奇数かつ k が偶数のとき (このとき $a \equiv c \equiv 1 \pmod{4}$ である)、$c^{z_1} + a^{z_1}$ は偶数であり、4 の倍数ではない. したがって $2^{y-1}k^y \mid (c^{z_1} - a^{z_1})$ である. しかし、

$$2^{y-1}k^y = \frac{(2k)^y}{2} \geq \frac{(2k)^{z+1}}{2} = k(4k^2)^{z_1} > (2k^2 + 2k + 1)^{z_1} = c^{z_1} > c^{z_1} - a^{z_1}$$

であるから矛盾する. もし z_1 と k が共に奇数なら、$c \equiv -a \equiv 1 \pmod{k+1}$ であるから、$(k+1) \mid (c^{z_1} + a^{z_1})$ かつ $4 \nmid (c^{z_1} - a^{z_1})$ である. よって、$2^{y-1}(k+1)^y \mid (c^{z_1} + a^{z_1})$ である. しかし、

$$\begin{aligned} 2^{y-1}(k+1)^y &> \frac{1}{2}(2(k+1))^z = \frac{1}{2}(4k^2 + 8k + 4)^{z_1} \\ &\geq (2k^2 + 4k + 2)^{z_1} = (c+a)^{z_1} \geq c^{z_1} + a^{z_1} \end{aligned}$$

であるから矛盾する.

(1-2-2) $n \mid a^x$ の場合.

定理の仮定より、素数 p を用いて $a=p^{\alpha}$, $n=p^{\nu}$ と表すことができる. このとき、$0\leq l<\nu$ であるような l と正の整数 t、そして α , ν を用いて、$\alpha x=\nu t+l$ と書ける.

$y>x+t$ であるとすると、$(an)^x+(bn)^y=(cn)^z$ から $n^{x+t}(p^l+n^{y-x-t}b^y)=n^zc^z$ が得られる. この式より、$z=x+t$ かつ $l=0$ が分かるので、$n^{y-z}b^y=c^z-1$ となる. z が奇数なら (1-1-2-1) から c^z-1 は b でちょうど割り切れる. しかし $y>z$ であり、したがって $y\geq 2$ かつ $b^2\mid(c^z-1)$ であるから、z は偶数でなければならない. よって $z=2z_1$ とすると、$\gcd(c^{z_1}+1,b)=2$ であることから $c^{z_1}+1\equiv 2 \pmod b$ を得る. さらに $n^{y-z}b^y=(c^{z_1}+1)(c^{z_1}-1)$ であるから、$\dfrac{b^y}{2}\Big|(c^{z_1}-1)$ を得る. しかし、

$$\frac{b^y}{2}>\frac{b^{2z_1}}{2}=\frac{1}{2}(c-a)^{z_1}(c+a)^{z_1}\geq c^{z_1}+a^{z_1}>c^{z_1}-1$$

であるから、これは矛盾である.

$y\leq x+t$ であるとすると、$(an)^x+(bn)^y=(cn)^z$ から $n^y(n^{x+t-y}p^l+b^y)=n^zc^z$ が得られる. $y>z$ であるので、$n\mid c^z$ となり、矛盾する.

(2) $\gcd(n,c)>1$ の場合.

c の素因数分解を $c=\prod_{i=1}^{t}q_i^{\alpha_i}$ とする.

(2-1) $C(n)\mid c$ の場合.

$s\leq t$, $\beta_i\geq 1$ $(i=1,\cdots,s)$ となるような整数 s , β_i を用いて $n=\prod_{i=1}^{s}q_i^{\beta_i}$ と表せる.

(2-1-1) $x=y$ の場合.

$z<x$ であるので、$(an)^x+(bn)^y=(cn)^z$ から

$$(a^x+b^x)\prod_{i=1}^{s}q_i^{\beta_i x}=\prod_{i=1}^{s}q_i^{\beta_i z}\cdot\prod_{i=1}^{s}q_i^{\alpha_i z}\cdot\prod_{i=s+1}^{t}q_i^{\alpha_i z}$$

であるから、

$$a^x+b^x=\prod_{i=1}^{s}q_i^{\alpha_i z-\beta_i(x-z)}\cdot\prod_{i=s+1}^{t}q_i^{\alpha_i z}\tag{2.5.11}$$

が得られる. この式より、任意の $i=1,\cdots s$ に対して、$\alpha_iz-\beta_i(x-z)\geq 0$ が成り立つことが分かる. 次に $\alpha_1z-\beta_1(x-z)>\alpha_1$ を示す. 仮にこれが成り立たないとする. $t=1$ なら、$s=1$ であり、$q_1^{\alpha_1z-\beta_1(x-z)}\leq q_1^{\alpha_1}=c<a^x+b^x$ であるが、これは (2.5.11) に矛盾する. $t>1$ なら、${q_1}^{\alpha_1}\leq\dfrac{c}{q_2}<c-1=b$ かつ $\prod_{i=2}^{t}q_i^{\alpha_i}\leq\dfrac{c}{q_1}<c-1=b$ であるから、

$$\prod_{i=1}^{s}q_i^{\alpha_iz-\beta_i(x-z)}\cdot\prod_{i=s+1}^{t}q_i^{\alpha_iz}<q_1^{\alpha_1}\prod_{i=2}^{t}q_i^{\alpha_iz}<b^{z+1}\leq b^x<a^x+b^x$$

であり、これも矛盾である. したがって、$\alpha_1z-\beta_1(x-z)>\alpha_1$ となる. 同様にして、$i=2,\cdots,s$ に対して、$\alpha_iz-\beta_i(x-z)>\alpha_i$ が成り立つことも示せる. したがって、

(2.5.11) から

$$a^x + b^x \equiv 0 \pmod{c} \tag{2.5.12}$$

が得られる. もし x が奇数ならば、$x = 2x_1 + 1$ とすると、

$$a^x + b^x = aa^{2x_1} + bb^{2x_1} \equiv a(-1)^{x_1} - 1 \pmod{c}$$

であり、(2.5.12) から $c \mid (a-1)$ または $c \mid (a+1)$ となるが、$c > a+1$ ゆえ、これは不可能である. よって x は偶数である. このとき $x = 2x_1$ とおくと (2.5.12) から、$(-1)^{x_1} + 1 \equiv 0 \pmod{c}$ であり x_1 は奇数である. この場合、$a^x + b^x = (a^2)^{x_1} + (b^2)^{x_1}$ は $x^2 + y^2$ で割り切れ、$z < x$ より $x > 2$ であるから、その商は 1 より大きい. さらに (2.5.11) から任意の $j = 1, \cdots, t$ に対して、$\dfrac{a^x + b^x}{a^2 + b^2}$ は q_j で割り切れる. $a^2 \equiv -1 \equiv b^2 \pmod{c}$ であるから、

$$\frac{a^x + b^x}{a^2 + b^2} = a^{2(x_1-1)} - a^{2(x_1-2)}b^2 + \cdots + b^{2(x_1-1)} \equiv x_1 \equiv 0 \pmod{q_j}$$

である. つまり $q_j \mid x_1$ である. したがって、$a^{2q_j} + b^{2q_j}$ は $a^{2x_1} + b^{2x_1}$ を割り切る. さらに、$\dfrac{a^{2q_j} + b^{2q_j}}{a^2 + b^2}$ も $a^{2x_1} + b^{2x_1}$ を割り切る. そして (2.5.11) から、この値は $\{q_1, \cdots, q_t\}$ の元の積になる. よって補題 2.5.7 から $\gcd\left(a^2 + b^2, \dfrac{a^{2q_j} + b^{2q_j}}{a^2 + b^2}\right) = q_j$ となる. しかし、明らかに $\dfrac{a^{2q_j} + b^{2q_j}}{a^2 + b^2} > q_j$ かつ $\prod_{i=1}^{t} q_i^2 \Big| (a^2 + b^2)$ であるから矛盾が生じる.

(2-1-2) $x > y$ の場合.

$(an)^x + (bn)^y = (cn)^z$ から

$$\prod_{i=1}^{s} q_i^{\beta_i y}(n^{x-y}a^x + b^y) = \prod_{i=1}^{s} q_i^{\beta_i z} \cdot \prod_{i=1}^{t} q_i^{\alpha_i z}$$

であり、$z \geq y$ なら $q_1 \mid b$ となり $\gcd(b, c) = 1$ に矛盾する. よって $z < y$ である. このとき、

$$n^{x-y}a^x + b^y = \prod_{i=1}^{s} q_i^{\alpha_i z - \beta_i(y-z)} \cdot \prod_{i=s+1}^{t} q_i^{\alpha_i z} \tag{2.5.13}$$

である. $q_j \mid b$ より $\alpha_j z - \beta_j(y-z) > 0$ となる $j = 1, \cdots, s$ が存在すれば矛盾するので、$\prod_{i=1}^{s} q_i^{\alpha_i z - \beta_i(y-z)} = 1$ である. したがって、$s < t$ となるが、$\prod_{i=s+1}^{t} q_i^{\alpha_i} < \dfrac{c}{q_1} < b$ から、

$$\prod_{i=s+1}^{t} q_i^{\alpha_i z} < b^z < b^y < n^{x-y}a^x + b^y$$

が得られ、これは (2.5.13) に矛盾する. 同様にして $x < y$ もありえない.

(2-2) $C(n) \nmid c$ の場合.

$n_1 > 1$ かつ $\gcd(n_1, n_2) = \gcd(n_1, c) = 1$ であるような n_1, n_2 を用いて $n = n_1 n_2$ とする.

(2-2-1) $x = y$ の場合.

$(an)^x + (bn)^y = (cn)^z$ から $n_1^x n_2^x (a^x + b^x) = n_1^x n_2^x c^z$ である. $z < x$ であるから、これは $n_1 \mid n_2^z c^z$ を意味し、矛盾である.

(2-2-2) $x > y$ の場合.

$(an)^x + (bn)^y = (cn)^z$ より $n_1^y n_2^y (n^{x-y} a^x + b^y) = n_1^z n_2^z c^z$ である. ここで $z \geq y$ なら $\gcd(n, c) > 1$ から $\gcd(b, c) > 1$ となり矛盾である. $z < y$ のとき $n_1 \mid c^z$ となるが、これも不可能である. 同様にして $x < y$ もありえない. これで証明は完了した.

□

定理 2.5.2 の証明. 定理 2.5.1 より、$k = 1$ の場合はよい. $k = 2, 3, 4, 5$ の場合は $C(b) \nmid n$ かつ $C(n) \mid b$ であるような n に対して、$(an)^x + (bn)^y = (cn)^z$ の正の整数解が $(x, y, z) = (2, 2, 2)$ しか存在しないことを示せばよい. 実際、定理 2.5.1 の証明における (1-1-2) の場合だけを考えればよいので、$\gcd(n, c) = 1$, $x > y$, $n \mid b^y$ かつ $C(b) \nmid n$ を仮定する. また、この証明内で用いる l は非負の整数とし、r , r_1 , r_2 , s , t は正の整数とする.

(1) $k = 2$ の場合. このとき $(a, b, c) = (5, 12, 13)$ である. また $x > y$, $n \mid 12^y$, $6 \nmid n$ が仮定であるから、n は 2 または 3 のべき乗である.

(1-1) $n = 3^r$ の場合、$0 \leq l < r$ であるような l と t, r を用いて、$y = tr + l$ と書ける.

$x > y + t$ なら $(an)^x + (bn)^y = (cn)^z$ から $n^{y+t}(n^{x-y-t}5^x + 3^l 4^y) = n^z 13^z$ である. したがって、$z = y + t$, $n^{x-z}5^x + 3^l 4^y = 13^z$ となり、$x > z$ であるから、$l = 0$ である. このとき、$(-1)^y \equiv 3^z \pmod 5$ であるから、z は偶数である. したがって、$z = 2z_1$ とすると、$n^{x-z}5^x = (13^{z_1} + 2^y)(13^{z_1} - 2^y)$ である. 右辺の因子は両方が同時に 5 で割り切れることはなく、また、$z = y + t > y$ に注意すると、

$$5^x > 5^z = 25^{z_1} > 13^{z_1} + 4^{z_1} > 13^{z_1} + 2^y > 13^{z_1} - 2^y$$

であるから、矛盾が生じる.

$x \leq y + t$ なら $(an)^x + (bn)^y = (cn)^z$ から

$$n^x(5^x + 3^l n^{y+t-x} 4^y) = n^z 13^z$$

である. $x > z$ であるから、これは明らかに不可能である.

(1-2) $n = 2^s$ の場合、$0 \leq l < s$ であるような l と t, s を用いて、$2y = ts + l$ と書ける. $x \leq y + t$ はあり得ないから、$x > y + t$ であり、$n^{y+t}(n^{x-y-t}5^x + 2^l 3^y) = n^z 13^z$ である. これは $z = y + t$ を意味し、したがって $l = 0$ であるから、

$$n^{x-z}5^x + 3^y = 13^z \tag{2.5.14}$$

が得られる. よって $3^y \equiv 3^z \pmod 5$ であり、y と z は偶奇が一致する. $4 \mid n^{x-z}$ なら (2.5.14) を mod 4 で考えることにより、y が偶数であると分かる. したがって

$z = 2z_1$, $y = 2y_1$ とおけて $n^{x-z}5^x = (13^{z_1} + 3^{y_1})(13^{z_1} - 3^{y_1})$ となる. (1-1) と同様にしてこれは不可能であることが分かる. したがって、$k = 2$ の場合は示された.

(2) $k = 3$ とすると、$(a, b, c) = (7, 24, 25)$ である. $x > y$ かつ $n \mid 24^y$ かつ $6 \nmid n$ を仮定しているから、n は 3 または 2 のべき乗である.

(2-1) $n = 3^r$ の場合、$0 \leq l < r$ であるような l と t, r を用いて、$y = tr + l$ と書ける. (1-1) と同様にして $x > y + t$ を得て、$z = y + t$ かつ $l = 0$ である. よって、$n^{x-z}7^x + 8^y = 25^z$ となる. この等式を mod 3 で考えることにより $y = 2y_1$ とおけて、$n^{x-z}7^x = (5^z + 8^{y_1})(5^z - 8^{y_1})$ と書けるが、右辺の因子は両方が同時に 7 で割り切れることはなく、また、

$$7^x > 7^z = 7^t 49^{y_1} > 5^t(25^{y_1} + 8^{y_1}) \geq 5^{y+t} + 8^{y_1} = 5^z + 8^{y_1} > 5^z - 8^{y_1}$$

であるから、矛盾が生じる.

(2-2) $n = 2^s$ の場合、(1-2) と同様にして矛盾を導くことができる. したがって、$k = 3$ の場合も示された.

(3) $k = 4$ の場合、$(a, b, c) = (9, 40, 41)$ である. $x > y$, $n \mid 40^y$, $10 \nmid n$ を仮定するから、n は 5 または 2 のべき乗である.

(3-1) $n = 5^r$ のとき、$0 \leq l < r$ である l と t, r を用いて、$y = tr + l$ と書ける. $x > y + t$ なら $(an)^x + (bn)^y = (cn)^z$ から $n^{y+t}(n^{x-y-t}9^x + 5^l 8^y) = n^z 41^z$ である. したがって、$z = y + t$ となり、$l = 0$ である. $n^{x-z}9^x + 8^y = 41^z$ を mod 5 で考えることにより、y が偶数であることが分かり、mod 3 で考えることにより、z が偶数であると分かる. よって、$y = 2y_1$, $z = 2z_1$ とおくと、$n^{x-z}9^x = (41^{z_1} + 8^{y_1})(41^{z_1} - 8^{y_1})$ である. 右辺の因子は両方が同時に 3 で割り切れることはなく、また、

$$9^x > 9^z = 81^{z_1} > 41^{z_1} + 8^{z_1} > 41^{z_1} + 8^{y_1} > 41^{z_1} - 8^{y_1}$$

であるから、矛盾が生じる.

(3-2) $n = 2^s$ の場合、(1-2) と同様にして矛盾が生じる. したがって、$k = 4$ の場合も示された.

(4) $k = 5$ の場合、$(a, b, c) = (11, 60, 61)$ であり、$x > y$, $n \mid 60^y$, $30 \nmid n$ を仮定する. $n = 3^{r_1}$, 5^{r_2} , 2^s , $3^{r_1}5^{r_2}$, $2^s 3^{r_1}$, $2^s 5^{r_2}$ の場合を考える必要があるが、これらについても前述の方法に沿って矛盾を導くことができる. 以上で定理の証明は完了したことになる.

□

また、Le は Deng と Cohen の結果を踏まえて、次の興味深い結果を得ている.

定理 2.5.15. (Le [11] Th.) s, t を $s > t$, $\gcd(s, t) = 1$, かつ $2 \mid st$ を満たす正の整数とし、$a = s^2 - t^2$, $b = 2st$, $c = s^2 + t^2$ とする. n を任意の正の整数とし、(x, y, z) を $(an)^x + (bn)^y = (cn)^z$ の $(2, 2, 2)$ ではない正の整数解とする. このとき、次の条件のうち、いずれか一つが成り立つ.

(1) $\max(x, y) > \min(x, y) > z$, $C(n) \mid c$ かつ $C(n) < C(c)$.

(2) $x > z > y$ かつ $C(n) \mid b$.

(3) $y > z > x$ かつ $C(n) \mid a$.

系 2.5.16. (Le [11] Cor.1) s, t を $s > t$, $\gcd(s,t) = 1$, かつ $2 \mid st$ を満たす正の整数とし、$a = s^2 - t^2$, $b = 2st$, $c = s^2 + t^2$ とする. n を任意の正の整数とし、(x,y,z) を $(an)^x + (bn)^y = (cn)^z$ の $(2,2,2)$ ではない正の整数解とする. このとき、x, y, z はそれぞれ互いに異なる.

系 2.5.17. (Le [11] Cor.1) s, t を $s > t$, $\gcd(s,t) = 1$, かつ $2 \mid st$ を満たす正の整数とし、$a = s^2 - t^2$, $b = 2st$, $c = s^2 + t^2$ とする. このとき、正の整数 n に対して、$C(n) \nmid a, b, c$ ならば、$(an)^x + (bn)^y = (cn)^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである.

2 つの系は定理からすぐに分かるので、定理 2.5.15 を証明する. まず、次の補題を証明する.

補題 2.5.18. l, m を正の整数とし、p を $p \mid l$ かつ $p \mid m$ であるような素数とする. このとき、$p^\alpha \parallel m$ かつ $p^\beta \parallel l$ （α, β：正の整数、$\alpha > 1$）ならば、

$$\binom{l}{k+1} m^k \equiv 0 \pmod{p^{\beta+1}}, \quad k = 1, \ldots, l-1$$

が成り立つ.

証明. $k = 1, \ldots, l-1$ に対して、γ_k を $p^{\gamma_k} \parallel k+1$ で定まる正の整数とする. このとき、

$$\gamma_k \leq \left[\frac{\log(k+1)}{\log p} \right] \leq k, \quad k = 1, \ldots, l-1 \quad ([*] \text{はガウス記号}) \tag{2.5.19}$$

が成り立つ. $(k+1)\binom{l}{k+1} = l\binom{l-1}{k}$ より、$\binom{l}{k+1} m^k = l\binom{l-1}{k}\frac{m^k}{k+1}$ となる. ここで、$p^2 \mid t$ より、$p^{2k} \mid t^k$ であり、また、(2.5.19) より、$\gamma_k < 2k$ であるので、$p \,\Big|\, \frac{m^k}{k+1}$ が分かる. $p^\beta \parallel l$ であったので、$l\binom{l-1}{k}\frac{m^k}{k+1} \equiv 0 \pmod{p^{\beta+1}}$ となり、補題は証明された. □

定理 2.5.15 の証明. (x,y,z) を $(an)^x + (bn)^y = (cn)^z$ の (2,2,2) ではない解とする. 補題 (2.5.7) より、$z < \max(x,y)$ としてよい. まず次の 3 つの場合がありえないことを示す.

(i) $x > y$ かつ $y = z$

(ii) $y > x$ かつ $x = z$

(iii) $x = y$ かつ $y > z$

どの場合もほぼ同様の方法で示すことができるので、(i) の場合のみを示す. $(an)^x + (bn)^y = (cn)^z$, $x > y$ かつ $y = z$ より、

$$a^x n^{x-y} = c^y - b^y \tag{2.5.20}$$

が得られる. 一方、条件より $a^2 = (c+b)(c-b)$ であるので、$c+b \mid a^2$ が分かる. ここで、y:奇数と仮定すると、(2.5.20) より、$c^y - b^y \equiv (-b)^y - b^y \equiv -2b^y \equiv 0 \pmod{c+b}$ となる. したがって、$\gcd(b, c+b) \neq 1$ であるから、$c+b \mid a^2$ より、$\gcd(a,b) \neq 1$ となり、条件に反する. よって、y は偶数である. $y = 2y'$ とおくと、(2.5.20) より、

$$\begin{aligned} a^{x-2} n^{x-y} &= \frac{(c^2)^{y'} - (b^2)^{y'}}{a^2} \\ &= \frac{(a^2+b^2)^{y'} - (b^2)^{y'}}{a^2} \\ &= \sum_{i=0}^{y'-1} \binom{y'}{i+1} a^{2i} b^{2(y'-i-1)} \end{aligned} \tag{2.5.21}$$

と書ける. ここで、p を a の素因子とする. (2.5.21) より、$y' b^{2(y'-1)} \equiv 0 \pmod{p}$ となる. $\gcd(a,b) = 1$ より、$p \mid y'$ が分かる. ここで、α, β を $p^\alpha \parallel a$, $p^\beta \parallel y'$ で定まる正整数とする. 補題 2.5.18 において、$l = y'$, $m = a^2$ とすると、条件を満たすので、

$$\binom{y'}{i+1} (a^2)^i \equiv 0 \pmod{p^{\beta+1}} , \quad i = 1, \ldots, y'-1$$

が得られる. したがって、

$$\sum_{i=0}^{y'-1} \binom{y'}{i+1} a^{2i} b^{2(y'-i-1)} \equiv y' b^{2(y'-1)} \pmod{p^{\beta+1}}$$

となる. ここで、$\gcd(p,b) = 1$ であり、また、$p^\beta \parallel y'$ であるので、$y' b^{2(y'-1)} \not\equiv 0 \pmod{p^{\beta+1}}$ となる. したがって、

$$p^\beta \Big\| \sum_{i=0}^{y'-1} \binom{y'}{i+1} a^{2i} b^{2(y'-i-1)} \tag{2.5.22}$$

が分かる. (2.5.21) と (2.5.22)、$p^\alpha \parallel a$ より、$\alpha(x-2) \leq \beta$ が得られる. p を a の全ての素因子を走らせて、同様の議論をすることにより、$a^{x-2} \mid y'$ が分かる. $y = 2y'$ であったので、$y \geq 2a^{x-2}$ となるが、$x > y$ かつ $a > 1$ であるので、これは成り立たない. したがって、$x > y$ かつ $y = z$ であるような解 (x, y, z) は存在しない.

したがって、(x, y, z) は

(1') $\max(x, y) > \min(x, y) > z$

(2') $x > z > y$

(3') $y > z > x$

のいずれかを満たす.

(1') の場合. $x > y > z$ も $y > x > z$ も同様に示すことができるので、$x > y > z$ のときのみ示す. $x > y > z$ のとき、$(an)^x + (bn)^y = (cn)^z$ より、

$$a^x n^{x-y} + b^y = \frac{c^z}{n^{y-z}} \tag{2.5.23}$$

である. ここで、$\dfrac{c^z}{n^{y-z}}$ は 1 より大きい整数である. したがって、$C(n) \mid c$ が得られる. また、$C(n) = C(c)$ と仮定すると、$p \Big| \dfrac{c^z}{n^{y-z}}$ かつ $p \mid n$ であるような素数 p が存在する. (2.5.23) より、$b^y \equiv 0 \pmod{p}$ となるので、$p \mid b$ であるが、これは $\gcd(b, c) = 1$ であることに矛盾する. よって、$C(n) < C(c)$ が得られる. したがって、(1) が得られる.

(2') の場合. $x > z > y$ のとき、$(an)^x + (bn)^y = (cn)^z$ より、

$$a^x n^{x-z} + \frac{b^y}{n^{z-y}} = c^z$$

が得られるので、$C(n) \mid b$ が分かる. したがって、(2) が得られる.

(3') の場合. (2') の場合と同様にして、(3) が得られる. これで定理は証明された.

□

3　解析的アプローチ

この章では、Baker の手法を用いて得られた結果を紹介する.

定理 3.0.1. (Guo , Le [5]) s を $2 \parallel s$, $s \geq 6000$ を満たす整数としたとき、$(s^2-9)^x + (6s)^y = (s^2+9)^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである.

定理 3.0.2. (Le [10]) s,t を $s > t$, $\gcd(s,t) = 1$, かつ $2 \mid st$ を満たす正の整数とし、$a = s^2 - t^2$, $b = 2st$, $c = s^2 + t^2$ とする. このとき、$2 \parallel s$, $t \equiv 3 \pmod 4$, かつ $s \geq 81t$ ならば、$a^x + b^y = c^z$ の正の整数解 (x,y,z) は $(2,2,2)$ のみである.

注 3.0.3. 定理 3.0.2 において $t = 3$ とすると、$s \geq 243$ となり、定理 3.0.1 を含んでいることが分かる.

定理 3.0.1 と定理 3.0.2 は証明方法がほぼ同じであるので、定理 3.0.2 のみ証明する. まず、この定理の証明の鍵となっている補題を証明する.

補題 3.0.4. s,t を $s > t$, $\gcd(s,t) = 1$, かつ $2 \mid st$ を満たす正の整数とし、$a = s^2 - t^2$, $b = 2st$, $c = s^2 + t^2$ とする. また、(x,y,z) を $a^x + b^y = c^z$ の $(2,2,2)$ ではない正の整数解とする. このとき、$2 \parallel s$ かつ $t \equiv 3 \pmod 4$ ならば、$2 \mid x$, $y = 1$ かつ $2 \nmid z$ である.

証明. $2 \parallel s$ かつ $t \equiv 3 \pmod 4$ より、

$$a \equiv 3 \pmod 8 \ , \ b \equiv 4 \pmod 8 \ , \ c \equiv 5 \pmod 8 \tag{3.0.5}$$

となる. したがって、$3^x + 4^y \equiv 5^z \pmod 8$ となり、$5^z - 4^y \equiv 1, 5 \pmod 8$ より、x は偶数であることが分かる. 補題を証明するためには、次の 3 つの場合がありえないことを示せばよい.

(1) $2 \mid x$ かつ $2 \mid y$.

(2) $2 \mid x$, $2 \nmid y$ かつ $2 \mid z$.

(3) $2 \mid x$, $2 \nmid y$, $y > 1$ かつ $2 \nmid z$.

(1) の場合. $2 \mid x$ かつ $2 \mid y$ と (3.0.5) より、$5^z \equiv 1 \pmod 8$ が得られる. したがって、z は偶数である. $x = 2x'$, $y = 2y'$, $z = 2z'$ とおくと、$(a^{x'})^2 + (b^{y'})^2 = (c^{z'})^2$ と書けるので、u,v を $u > v$, $\gcd(u,v) = 1$, かつ $2 \mid uv$ を満たす正の整数としたとき、

$$a^{x'} = u^2 - v^2 \ , \ b^{y'} = 2uv \ , \ c^{z'} = u^2 + v^2 \tag{3.0.6}$$

と表すことが出来る. ここで、$y' \geq 2$ と仮定すると、$b \equiv 4 \pmod 8$ と $b^{y'} = 2uv$ から、$uv \equiv 0 \pmod 8$ が分かる. $\gcd(u,v) = 1$ より、$8 \mid u$, $2 \nmid v$ もしくは $2 \nmid u$, $8 \mid v$ となる. (3.0.5) と (3.0.6) より、$3^{x'} \equiv \pm 1 \pmod 8$, $5^{z'} \equiv 1 \pmod 8$ となるので、x', z' は

偶数である. したがって、$4 \mid x$, $2 \mid y$, $4 \mid z$ となるが、補題 2.3.10 より、このような (x, y, z) は存在しない. よって、$y' = 1$ であるので、

$$b^2 = c^z - a^x = (c^{z'} + a^{x'})(c^{z'} - a^{x'}) \tag{3.0.7}$$

と書ける. ここで、$z' \geq 2$ と仮定すると、(3.0.7) より、$b^2 > c^{z'} + a^{x'} > c^{z'} \geq c^2$ となり、$b < c$ であることに矛盾する. したがって、$z' = 1$ となり、$z = 2$ が得られる. $y = z = 2$ より、$x = 2$ となる. したがって、$(x, y, z) \neq (2, 2, 2)$ かつ $2 \mid x$ かつ $2 \mid y$ であるような (x, y, z) は存在しない.

(2) の場合. $a^x + b^y = c^z$ かつ $2 \mid x$, $2 \nmid y$ かつ $2 \mid z$ より、$\left(\frac{a}{b}\right) = 1$ ($\left(\frac{*}{*}\right)$ は Jacobi 記号) が得られる. 一方、$s + t \equiv 1 \pmod 4$ より、

$$\left(\frac{a}{b}\right) = \left(\frac{2}{s^2 - t^2}\right)\left(\frac{st}{s^2 - t^2}\right) = -\left(\frac{st}{s+t}\right)\left(\frac{st}{s-t}\right) = -\left(\frac{-s^2}{s+t}\right)\left(\frac{s^2}{s-t}\right) = -1$$

となるので、矛盾する.

(3) の場合. (3.0.5) と $2 \mid x$, $2 \nmid y$, $y > 1$ より、$a^x + b^y \equiv 3^x + 4^y \equiv 1 \pmod 8$ が得られる. 一方、$c \equiv 5 \pmod 8$ と $2 \nmid z$ より、$c^z \equiv 5^z \equiv 5 \pmod 8$ となり、$a^x + b^y \not\equiv c^z \pmod 8$ であるので、$2 \mid x$, $2 \nmid y$, $y > 1$ かつ $2 \nmid z$ であるような (x, y, z) は存在しない.

□

注 3.0.8. 補題 3.0.4 は定理 2.3.4 を含んでいる.

ここで、Weil's height と呼ばれる height function を以下で定義する.
α を定義方程式が

$$a_0 z^n + a_1 z^{n-1} + \cdots + a_n = a_0(z - \sigma_1\alpha) \cdots (z - \sigma_n\alpha)$$

($a_i \in \mathbb{Z}$, $a_0 > 0$, $\sigma_1\alpha, \ldots, \sigma_n\alpha$ は α の全ての共役元) であるような零でない代数的数とする. このとき、α の Weil's height $h(\alpha)$ を

$$h(\alpha) = \frac{1}{n}\left(\log a_0 + \sum_{i=1}^{n} \log \max(1\ ,\ |\sigma_i\alpha|)\right)$$

と定める. このとき、次の補題が成り立つ.

補題 3.0.9. $\alpha_1, \alpha_2 \in \mathbb{R}^+$ を乗法的に一次独立な代数的数とし、$D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$ とする. また $j = 1, 2$ に対し、$\log A_j = \max\left(h(\alpha_j)\ ,\ \frac{|\log \alpha_j|}{D}\ ,\ \frac{1}{D}\right)$ と定める. さらに、正の整数 b_1, b_2 に対して、$\Lambda = b_1 \log \alpha_1 - b_2 \log \alpha_2$ とする. このとき $B = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}$ とすると、次の不等式が成り立つ.

$$\log |\Lambda| \geq -32.31 D^4 (\log A_1)(\log A_2)\left(\max\left(\frac{10}{D}\ ,\ 0.18 + \log B\right)\right)^2.$$

証明は [8, Cor.2] でなされている.

補題 3.0.4 で得た $y = 1$ であるということと、補題 3.0.9 による評価を用いて、定理 3.0.2 を証明する.

定理 3.0.2 の証明. s, t を $2 \parallel s$, $t \equiv 3 \pmod 4$, $s \geq 81t$ を満たすものとする. $(x, y, z) \neq (2, 2, 2)$ を $a^x + b^y = c^z$ の正の整数解とすると補題 3.0.4 から、

$$a^x + b = c^z,\ 2 \mid x,\ 2 \nmid z. \tag{3.0.10}$$

が成り立つ. ここで $x \not\equiv z \pmod 2$ であるから、$z > x$ と仮定すると、$a^x = c^z - b > c^{x+1} - c > c^x$ となり、矛盾する. よって $z < x$ である. また、$c = a + 2t^2$ であることと $a = s^2 - t^2$, $b = 2st$, $c = s^2 + t^2$ から、

$$\log c = \log a + \rho_1 \tag{3.0.11}$$

が得られる. ここで ρ_1 は次の不等式を満たす.

$$0 < \rho_1 = \frac{2t^2}{s^2} \sum_{k=0}^{\infty} \frac{1}{2k+1} \left(\frac{t^2}{s^2} \right)^{2k} \leq \frac{2}{81^2} \sum_{k=0}^{\infty} \frac{81^{-4k}}{2k+1} < 0.003049. \tag{3.0.12}$$

同様に, (3.0.10) から

$$z \log c - x \log a =: \rho_2 \tag{3.0.13}$$

が得られ、ρ_2 は次の不等式を満たす.

$$0 < \rho_2 = \frac{2b}{a^x + c^z} \sum_{k=0}^{\infty} \frac{1}{2k+1} \left(\frac{b}{a^x + c^z} \right)^{2k} < \frac{b}{a^x}. \tag{3.0.14}$$

(3.0.11), (3.0.12), (3.0.13) より、

$$z = \frac{(x - z) \log a + \rho_2}{\rho_1} > \frac{\log a}{\rho_1} > 3279 \log a \tag{3.0.15}$$

が得られる. ここで、$B = \dfrac{z}{\log a} + \dfrac{x}{\log c}$ とおくと、

$$B = \frac{2x}{\log c} + \frac{\rho_2}{(\log a)(\log c)} \tag{3.0.16}$$

となる.

(i) $B \leq e^{9.82}$ のとき. $D = 1$ より、$\max\left(\dfrac{10}{D} ,\ 0.18 + \log B \right) = 10$ となるので、補題 3.0.9 より、

$$\log \rho_2 \geq -3231 (\log a)(\log c) \tag{3.0.17}$$

が得られる. (3.0.14) と (3.0.17) より、

$$\frac{\log b}{\log a} + 3231 \log c > x \tag{3.0.18}$$

であるが、(3.0.15) と (3.0.18) より、

$$1 + 3231 \log c > x > z > 3279 \log a = 3279 \log c - 3279\rho_1 > 3279 \log c - 1.1$$

となり、これは矛盾する.

(ii) $B > e^{9.82}$ のとき. $\max\left(\frac{10}{D}\ ,\ 0.18 + \log B\right) = 0.18 + \log B$ となるので、補題 3.0.9 より、

$$\log \rho_2 \geq -32.31(\log a)(\log c)(0.18 + \log B)^2 \tag{3.0.19}$$

が得られる. (3.0.14),(3.0.16),(3.0.19) より、

$$\begin{aligned} 1 + 64.62(0.18 + \log B)^2 &> \rho_2 + \frac{2 \log b}{(\log a)(\log c)} + 64.42(0.18 + \log B)^2 \\ &> \rho_2 + \frac{2x}{\log c} \\ &> B \end{aligned}$$

となる. 簡単な考察により、$B > e^{9.82}$ ならば、

$$1 + 64.62(0.18 + \log B)^2 < B$$

であることから矛盾が生じる. したがって、定理は証明された.

□

参考文献

[1] Roger Apéry. Sur une équation diophantienne. *C. R. Acad. Sci. Paris*, Vol. 251, pp. 1451–1452, 1960.

[2] V. A. Dem′janenko. On Jeśmanowicz' problem for Pythagorean numbers. *Izv. Vysš. Učebn. Zaved. Matematika*, Vol. 1965, No. 5 (48), pp. 52–56, 1965.

[3] Moujie Deng and G. L. Cohen. On the conjecture of Jesmanowicz concerning Pythagorean triples. *Bull. Austral. Math. Soc.*, Vol. 57, No. 3, pp. 515–524, 1998.

[4] A. Grytczuk and A. Grelak. On the equation $a^x + b^y = c^z$. *Comment. Math. Prace Mat.*, Vol. 24, No. 2, pp. 269–275, 1984.

[5] Yongdong Guo and Maohua Le. A note on Jeśmanowicz' conjecture concerning Pythagorean numbers. *Comment. Math. Univ. St. Paul.*, Vol. 44, No. 2, pp. 225–228, 1995.

[6] Loo Keng Hua. *Introduction to number theory*. Springer-Verlag, Berlin, 1982. Translated from the Chinese by Peter Shiu.

[7] L. Jeśmanowicz. Several remarks on Pythagorean numbers. *Wiadom. Mat. (2)*, Vol. 1, pp. 196–202, 1955/1956.

[8] Michel Laurent, Maurice Mignotte, and Yuri Nesterenko. Formes linéaires en deux logarithmes et déterminants d'interpolation. *J. Number Theory*, Vol. 55, No. 2, pp. 285–321, 1995.

[9] Mao Hua Le. A note on Jeśmanowicz' conjecture. *Colloq. Math.*, Vol. 69, No. 1, pp. 47–51, 1995.

[10] Maohua Le. On Jeśmanowicz' conjecture concerning Pythagorean numbers. *Proc. Japan Acad. Ser. A Math. Sci.*, Vol. 72, No. 5, pp. 97–98, 1996.

[11] Maohua Le. A note on Jeśmanowicz' conjecture concerning Pythagorean triples. *Bull. Austral. Math. Soc.*, Vol. 59, No. 3, pp. 477–480, 1999.

[12] L. J. Mordell. *Diophantine equations*. Pure and Applied Mathematics, Vol. 30. Academic Press, London, 1969.

[13] W. Sierpiński. On the equation $3^x + 4^y = 5^z$. *Wiadom. Mat. (2)*, Vol. 1, pp. 194–195, 1955/1956.

[14] W. Sierpiński. *Elementary theory of numbers*, Vol. 31 of *North-Holland Mathematical Library*. North-Holland Publishing Co., Amsterdam, second edition, 1988. Edited and with a preface by Andrzej Schinzel.

[15] Kei Takakuwa. On a conjecture on Pythagorean numbers. III. *Proc. Japan Acad. Ser. A Math. Sci.*, Vol. 69, No. 9, pp. 345–349, 1993.

[16] Kei Takakuwa and You Asaeda. On a conjecture on Pythagorean numbers. *Proc. Japan Acad. Ser. A Math. Sci.*, Vol. 69, No. 7, pp. 252–255, 1993.