Ramanujan と関係する指数型不定方程式

寺井 伸浩 (大分大学)

概 要

本稿は第 15 回福岡数論研究集会に於いて著者が「Ramanujan と関係する指数型不定方程式」という題目で講演した報告である. 講演中で詳しく述べられなかった証明の詳細や定理・補題・例を纏め, Ramanujan と関係する不定方程式・予想・数について, 指数型不定方程式の観点で深く解説する.

1 序論

整数論, 特に不定方程式論において, Ramanujan を冠した方程式や数は, 次がよく知られている:

- Ramanujan-Nagell 方程式: $x^2 + 7 = 2^n$
- Brocard-Ramanujan 方程式: $x^2 + 1 = n!$
- Ramanujan のタクシー数: 1729

本稿では, これら 3 つの話題について, 知られている定理, 関係する予想・一般化を著者の結果・予想を中心に幅広く紹介する.

2 Ramanujan-Nagell 方程式 $x^2 + 7 = 2^n$

インドの天才数学者 Ramanujan が 1913 年に予想し, Nagell が 1948 年に次の定理を証明した. その証明は虚 2 次体 $\mathbb{Q}(\sqrt{-7})$ の性質を用いるものであった. 他に, 2 次線形数列, 楕円曲線, 超幾何級数等を用いるいろいろな証明がある.

定理 2.1 (Ramanujan-Nagell)**.** 指数型不定方程式

$$x^2 + 7 = 2^n$$

は, 正の整数解 $(n, x) = (3, 1),\ (4, 3),\ (5, 5),\ (7, 11),\ (15, 181)$ だけをもつ.

定理 2.1 の一般化として, 次の 2 つの定理はよく知られている.

定理 2.2 (Tanahashi [Ta], Toyoizumi [To])**.** 指数型不定方程式

$$x^2 + 7^m = 2^n$$

は, 正の整数解 $(x, m, n) = (1, 1, 3),\ (3, 1, 4),\ (5, 1, 5),\ (11, 1, 7),\ (181, 1, 15),\ (13, 3, 9)$ だけをもつ.

定理 2.3 (Bugeaud-Mignotte-Siksek [BMS], 2006)**.** 指数型不定方程式

$$x^2 + 7 = y^n, \quad n \geq 3$$

は, 正の整数解 $(x, y, n) = (1, 2, 3),\ (3, 2, 4),\ (5, 2, 5),\ (11, 2, 7),\ (181, 2, 15)$ だけをもつ.

2.1 Jeśmanowicz 予想

予想 2.1 (Jeśmanowicz [J], 1956)**.** a, b, c を $a^2 + b^2 = c^2$ を満たす固定された互いに素な正の整数とする. このとき, 指数型不定方程式

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

は, ただ一つの正の整数解 $(x, y, z) = (2, 2, 2)$ をもつ.

ピタゴラス数のパラメーター表示により, 指数型不定方程式

$$(m^2 - n^2)^x + (2mn)^y = (m^2 + n^2)^z \tag{2.1}$$

を考えればよい. ここで, m, n は $m > n$, $m \not\equiv n \pmod 2$ である互いに素な正の整数とする. 次の場合に予想 2.1 が成り立つことが示されている.

- $n = 1$ (Lu [Lu], 1959), $m - n = 1$ (Demjanenko [De], 1965)
- $a \equiv \pm 1 \pmod b$, $c \equiv 1 \pmod b$ (Miyazaki [M1], 2013)
- $n = 2$ (Terai [Te2], 2014), $n \equiv 2 \pmod 4$ and $n < 100$ (Miyazaki-Terai [MT], 2015)

最小のピタゴラス数である $(a, b, c) = (3, 4, 5)$ に対し予想 2.1 が成り立つことを示した, 次の Sierpiński の結果の証明を与える. 証明はとても初等的であるが, まず x, z が偶数であることを示し, よく知られた指数型不定方程式に帰着させる点は, 一般の場合にも応用できる.

定理 2.4 (Sierpiński [S], 1956)**.** 指数型不定方程式

$$3^x + 4^y = 5^z$$

は, ただ一つの正の整数解 $(x, y, z) = (2, 2, 2)$ をもつ.

Proof. 方程式を modulo 4 で考えると $(-1)^x \equiv 1 \pmod 4$ である. よって x は偶数である. また, 方程式を modulo 3 で考えると $1 \equiv (-1)^z \pmod 3$ である. よって z は偶数である. いま, $x = 2X$, $z = 2Z$ とおくと, 方程式は

$$2^{2y} = (5^Z + 3^X)(5^Z - 3^X)$$

となる. 右辺の 2 つの因数の最大公約数は 2 であるので,

$$\begin{cases} 5^Z + 3^X = 2^{2y-1} \\ 5^Z - 3^X = 2 \end{cases}$$

を得る. これら 2 式を引くと $2^{2y-2} - 1 = 3^X$ となる. $y \geq 3$ のとき modulo 8 で考えると $-1 \equiv 3^x \pmod 8$ であるが, これは不可能！したがって, $y = 2$, $x = 2$, $z = 2$ を得る. □

2.2 一般化された Ramanujan-Nagell 方程式 $x^2 + b^m = c^n$ (b は奇数)

一般化された Ramanujan-Nagell 方程式 $x^2 + b^m = c^n$ において, b が奇数と偶数の場合で分けて考察する. この節で b が奇数, 次の節で b が偶数である場合をそれぞれ扱う.

予想 2.2 (Terai [Te1], 1993)**.** a, b, c を $a^2 + b^2 = c^2$ を満たす固定された互いに素な正の整数とする. ただし b を奇数とする. このとき, 指数型不定方程式

$$x^2 + b^m = c^n$$

は, ただ一つの正の整数解 $(x, m, n) = (2, 2, 2)$ をもつ.

ピタゴラス数が $(a, b, c) = (4, 3, 5)$ のとき予想 2.2 が成り立つことを確かめる.

定理 2.5 (Terai [Te1], 1993)**.** 指数型不定方程式

$$x^2 + 3^m = 5^n$$

は, ただ一つの正の整数解 $(x, m, n) = (4, 2, 2)$ をもつ.

Proof. 次の補題を用いて示す.

補題 2.1 (Störmer-Ljunggren)**.** 不定方程式

$$X^2 + 1 = 2Y^n, \quad n \geq 3$$

は, 正の整数解 $(X, Y, n) = (1, 1, n),\ (239, 13, 4)$ だけをもつ.

方程式を modulo 3 で考えると $1 \equiv (-1)^n \pmod 3$ である. よって n は偶数である. いま, $n = 2N$ とおくと, 方程式は

$$3^m = (5^N + x)(5^N - x)$$

となる. 右辺の 2 つの因数は互いに素なので,

$$5^N + x = 3^m, \quad 5^N - x = 1$$

が従う. これら 2 式を加えると

$$3^m + 1 = 2 \cdot 5^N$$

となる. m は偶数が modulo 8 で分かるので, 補題 2.1 より $(x, m, n) = (4, 2, 2)$ を得る. □

同様にして次の定理を示すことができる:

定理 2.6 (Terai [Te1], 1993)**.** 指数型不定方程式

$$x^2 + 5^m = 13^n, \quad x^2 + 7^m = 25^n, \quad x^2 + 9^m = 41^n, \quad x^2 + 11^m = 61^n$$

は, それぞれただ一つの正の整数解

$$(x, m, n) = (12, 2, 2),\ (24, 2, 2),\ (40, 2, 2),\ (60, 2, 2)$$

をもつ.

2.3 一般化された Ramanujan-Nagell 方程式 $x^2+b^m=c^n$ (b は偶数)

一方, b が偶数のときの, 一般化された Ramanujan-Nagell 方程式 $x^2+b^m=c^n$ に関する次の予想はとても興味深い:

予想 2.3 (Terai-Fujita [TF], 2022)**.** u, v を互いに素な $u \not\equiv v \pmod 2$, $u>v$ である正の整数とする.
(1) $3u^2-8uv+3v^2 \neq -1$ ならば, 不定方程式

$$x^2+(2uv)^m=(u^2+v^2)^n \tag{2.2}$$

は, 正の整数解

$$(x,m,n)=(u-v,1,1),\ (u^2-v^2,2,2)$$

だけをもつ. ただし, $(u,v)=(244,231)$ の場合を除く:

$$x^2+112728^m=112897^n;\quad (x,m,n)=(13,1,1),\ (6175,2,2),\ (2540161,3,3).$$

(2) $3u^2-8uv+3v^2=-1$ ならば, 不定方程式 (2.2) は正の整数解

$$(x,m,n)=(u-v,1,1),\ (u^2-v^2,2,2),\ ((u-v)(2u^2+2v^2+1),1,3)$$

だけをもつ.

Magma により, 上の予想 2.3 が $1 \le v < u \le 10^5$, $m \le 11$, $n \le 11$ の範囲で成り立つことを確かめた. $u=2, v=1$ のとき, 予想 2.3 が成り立つことを示す.

定理 2.7 (Yuan-Hu [YH], 2005))**.** 指数型不定方程式

$$x^2+4^m=5^n$$

は, 正の整数解 $(x,m,n)=(1,1,1),\ (3,2,2),\ (11,1,3)$ だけをもつ.

Proof. Yuan-Hu [YH] の方法とは違い, 楕円曲線 (整数論計算ソフト Magma) を用いて示す.

補題 2.2 (楕円曲線の整数点)**.** (1) 楕円曲線 $E_1: Y^2=X^3-4$ 上の整数点は, $(X,Y)=(2,\pm 2),(5,\pm 11)$ だけである.
(2) 楕円曲線 $E_2: Y^2=X^3-4\cdot 5^2$ 上の整数点は, $(X,Y)=(5,\pm 5),(10,\pm 30),(34,\pm 198)$ だけである.
(3) 楕円曲線 $E_3: Y^2=X^3-4\cdot 5^4$ 上の整数点は, $(X,Y)=(50,\pm 350)$ だけである.

(i) $m=1$ のとき, 方程式は $x^2+4=5^n$ となる. $n=3N+r$ $(r=0,1,2)$ とおくと

$r=0$ のとき, $E_1: Y^2=X^3-4$ $(X=5^N,\ Y=x)$,
$r=1$ のとき, $E_2: Y^2=X^3-4\cdot 5^2$ $(X=5^{N+1},\ Y=5x)$,
$r=2$ のとき, $E_3: Y^2=X^3-4\cdot 5^4$ $(X=5^{N+2},\ Y=5^2x)$.

補題 2.2 より, 正の整数解 $(x,m,n)=(1,1,1),\ (11,1,3)$ だけを得る.

(ii) $m \ge 2$ のとき, 方程式を modulo 8 で考えると $1 \equiv 5^n \pmod 8$ である. よって n は偶数である. いま, $n=2N$ とおくと, 方程式は

$$2^{2m}=(5^N+x)(5^N-x)$$

となる. 右辺の 2 つの因数の最大公約数は 2 なので,

$$5^N + x = 2^{2m-1}, \quad 5^N - x = 2$$

が従う. これら 2 式を加えると

$$2^{2m-2} + 1 = 5^N$$

となる.

$m = 2$ のとき, $N = 1$, よって $(x, m, n) = (3, 2, 2)$ を得る.

$m \geq 3$ のとき, N は偶数が modulo 8 で分かるので, 上記の議論の因数分解により, 解なしを容易に示せる. □

$u = 3, v = 2$ のとき, 予想 2.3 が成り立つことを示す.

定理 2.8 (Terai-Fujita [TF], 2022)**.** 指数型不定方程式

$$x^2 + 12^m = 13^n$$

は, 正の整数解 $(x, m, n) = (1, 1, 1),\ (5, 2, 2)$ だけをもつ.

Proof. 楕円曲線 (整数論計算ソフト Magma) と Zsigmondy の結果を用いて示す.

補題 2.3 (楕円曲線の整数点)**.** (1) 楕円曲線 $E_1 : Y^2 = X^3 - 12$ 上の整数点 (X, Y) はなし.
(2) 楕円曲線 $E_2 : Y^2 = X^3 - 12 \cdot 13^2$ 上の整数点は, $(X, Y) = (13, \pm 13)$ だけである.
(3) 楕円曲線 $E_3 : Y^2 = X^3 - 12 \cdot 13^4$ 上の整数点 (X, Y) はなし.

補題 2.4 (Zsigmondy [Z])**.** a, b を互いに素で $a > b$ である正の整数とし, 数列 $\{a_n\}$ を $a_n = a^n - b^n$ で定義する. このとき, $n > 1$ ならば, $a_1 a_2 \cdots a_{n-1}$ を割らない a_n の素因数が存在する. ただし, 次の 2 つの場合は除く: (I) $n = 2$, $a + b$ は 2 の冪, (II) $(a, b, n) = (2, 1, 6)$.

(i) $m = 1$ のとき, 方程式は $x^2 + 12 = 13^n$ となる. $n = 3N + r$ $(r = 0, 1, 2)$ とおくと

$r = 0$ のとき, $E_1 : Y^2 = X^3 - 12$ $(X = 13^N,\ Y = x)$,

$r = 1$ のとき, $E_2 : Y^2 = X^3 - 12 \cdot 13^2$ $(X = 13^{N+1},\ Y = 13x)$,

$r = 2$ のとき, $E_3 : Y^2 = X^3 - 12 \cdot 13^4$ $(X = 13^{N+2},\ Y = 13^2 x)$.

補題 2.3 より, 正の整数解 $(x, m, n) = (1, 1, 1)$ だけを得る.

(ii) $m \geq 2$ のとき, 方程式を modulo 8 で考えると $1 \equiv 5^n \pmod 8$ である. よって n は偶数である. いま, $n = 2N$ とおくと, 方程式は

$$2^{2m} 3^m = (13^N + x)(13^N - x)$$

となる. 右辺の 2 つの因数の最大公約数は 2 なので,

$$\begin{cases} 13^N \pm x = 2^{2m-1} 3^m \\ 13^N \mp x = 2 \end{cases}$$

または

$$\begin{cases} 13^N \pm x = 2 \cdot 3^m \\ 13^N \mp x = 2^{2m-1} \end{cases}$$

を得る. これら 2 式をそれぞれ加えると

$$2^{2m-2}3^m + 1 = 13^N \tag{2.3}$$

または

$$2^{2m-2} + 3^m = 13^N \tag{2.4}$$

となる.

まず, 方程式 (2.3) を考える. 数列 $\{a_N\}$ を次のようにおく:

$$a_N = 13^N - 1 = 2^{2m-2}3^m. \tag{2.5}$$

$N = 1$ のとき, (2.3) は解をもたない. $a_1 = 12 = 2^2 \cdot 3$ なので, $N \geq 2$ のとき $\{a_N\}$ は Zsigmondy の補題 2.4 より (2.5) を満たす解 N, m をもたない.

次に, 方程式 (2.4) を考える. $m = 1, 2$ のとき, (2.4) は明らかに $(m, N) = (2, 1)$ だけを解にもつ. このとき, $n = 2, x = 5$ を得る. $m \geq 3$ のとき, (2.4) より

$$3^m \equiv 5^N \pmod 8$$

となる. これは, m と N は偶数であることを示す. よって, $m = 2m_1,\ N = N_1$ とおく. このとき, ピタゴラス数のパラメーター表示より

$$\begin{cases} 2^{m-1} = 2UV \\ 3^{m_1} = U^2 - V^2 \\ 13^{N_1} = U^2 + V^2 \end{cases} \tag{2.6}$$

が従う. ここで, U, V は $U > V$, 反対の偶奇性, 互いに素な整数である. (2.6) の最初の 2 式より

$$U = 2^{m-2}, \quad V = 1, \quad U - V = 1$$

を得る. 上式を満たす m, U, V の値は $m = 3, U = 2, V = 1$ だけである. このとき, (2.6) の最後の式より

$$13^{N_1} = 2^2 + 1^2$$

となるが, これは不可能である. □

Pell 方程式や BHV の深い結果 ([BHV]) を用いて, 次を示すことができる.

定理 2.9 (Fujita-Le-Terai [FLT], 2022)**.** p を奇素数, t を正の整数とする. このとき, 予想 2.3 は $(u, v) \in \{(2p^t, 1), (p^t, 2)\}$ に対し正しい.

3 Brocard-Ramanujan 方程式 $x^2 + 1 = n!$

3.1 Brocard-Ramanujan 予想の一般化

階乗に関しては, 次の予想は有名であるが, 未解決である (cf. [BG], [DU], [KF]).

予想 3.1 (Brocard-Ramanujan [Ra], 1913)**.** 不定方程式

$$n! + 1 = x^2$$

は, 正の整数解 $(n, x) = (4, 5), (5, 11), (7, 71)$ だけをもつ.

注意. $n!-1=x^2 \iff (n,x)=(2,1)$ を示すのは超簡単である.

Dabrovski [Da] は, もっと一般的な不定方程式

$$n!+A=m^2 \tag{3.1}$$

を考察した. ここで A は平方数でない正の整数である. ABC 予想を仮定すれば, (3.1) の正の整数解 n,m は高々有限個がであることが示される. 小さい A の値に関しては次の解が知られている.

A	知られている正の整数解 (n,m)
1	$(4,5),\ (5,11),\ (7,71)$
2	$(2,2)$
3	$(1,2),\ (3,3)$
4	—
5	—
6	—
7	$(2,3)$
8	$(1,3)$
9	$(6,27)$
10	$(3,4)$

Brocard-Ramanujan 予想の一般化として次を提起する:

予想 3.2 (一般化された Brocard-Ramanujan 予想)**.** (1) 不定方程式

$$n!+n^k=x^2$$

は, 正の整数解 $(k,n,x)=(1,2,2),\ (1,3,3),\ (3,9,603)$ だけをもつ.
(2) 不定方程式

$$|n!-n^k|=x^2$$

は, 正の整数解 $(k,n,x)=(4,6,24),\ (5,6,84)$ だけをもつ.

予想 3.2 を一般の場合に示すのは難しいが, n が素数の場合は初等的に示すことができる.

定理 3.1. n が素数ならば, 予想 3.2 は (1), (2) 共に正しい.

Proof. $n=p$ (p : 素数) とする.
(1) $x=pX$ とおき, 方程式の両辺を p で割ると

$$(p-1)!+p^{k-1}=pX^2$$

となる. 明らかに, $p=2$ のとき $k=1$, $X=1$, $x=2$ を得る. 以後, $p>2$ としてよい.
(i) $k>1$ のとき, Wilson の定理より $-1\equiv 0 \pmod p$, 矛盾 !
(ii) $k=1$ のとき,

$$(p-1)!+1=pX^2 \tag{3.2}$$

となる.
$p=3$ ならば, $3=2!+1=3X^2$, よって $X=1$, $x=3$ を得る.

$p>3$ ならば, $\left(\dfrac{m}{p}\right)=-1$ となる奇数 m $(1<m<p)$ を取れる. 何故ならば, $p>3$ と (3.2) より $p\equiv 1 \pmod 4$ であるので, m が偶数ならば, $m_0=p-m$: (奇数) を取ればよい. よって, (3.2) より

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

となり矛盾！

(2) $n!-n^k=\pm x^2$ より, $x=pX$ とおくと,

$$(p-1)!-p^{k-1}=\pm pX^2$$

となる. 明らかに, $p>2$ としてよい.

(i) $k>1$ のとき, Wilson の定理より $-1\equiv 0 \pmod p$, 矛盾！

(ii) $k=1$ のとき, $-1-1\equiv 0 \pmod p$, 矛盾！ □

3.2 Wilson 商との関係

この節では, Wilson 商を定義し, これに関する指数型不定方程式の予想や知られている結果を述べる.

定義 3.1. p を奇素数とする. そのとき, 商

$$W_p=\frac{(p-1)!+1}{p}$$

は p の **Wilson 商**と呼ばれる.

Wilson の定理より, W_p は整数である. Wilson 商が平方数, p 倍の平方数になるかの予想は次である:

予想 3.3 (平方数となる Wilson 商)**.** (1) $W_p=x^2 \iff (p,x)=(3,1)$.
(2) $W_p=px^2 \iff (p-1)!+1=(px)^2 \iff (p,x)=(5,1)$.

注意. 上記予想 3.3 において, (1) は定理 3.1 より正しいが, (2) は難しいようである. これは Brocard-Ramanujan 予想 (予想 3.1) の $n=p-1$ の場合に当たる. $W_p\equiv 0 \pmod p$ (ここで $3\le p<10^{10}$) を満たす p の値は $p=5,13,563$ だけである.

l 乗 $(l\ge 2)$ に関する次の予想は難しい.

予想 3.4 (冪となる Wilson 商)**.** (1) $W_p=x^l \iff (p,l)=(3,2)$.
(2) $W_p=px^l \iff (p,l)=(5,2)$.

4 Ramanujan のタクシー数 1729

4.1 1729 の面白い 4 つの性質

Ramanujan のタクシー数 1729 は, 次のようなとても興味深い性質を持つ:

(1) **正の 2 つの立方数の和として2 通りに表せる最小の正の整数** $1729=12^3+1^3=10^3+9^3$.

「正の 2 つの立方数の和」が「正の 2 つの平方数の和」「(正負の) 2 つの立方数の和」ならば, 最小数はそれぞれ次である:

$$65 = 8^2 + 1^2 = 7^2 + 4^2 \ (= 5 \cdot 13),$$
$$91 = 6^3 + (-5)^3 = 4^3 + 3^3 \ (= 7 \cdot 13).$$

(2) **3 番目のカーマイケル数**

1 番目は $561 = 3 \cdot 11 \cdot 17$, 2 番目は $1105 = 5 \cdot 13 \cdot 17$, 3 番目は $1729 = 7 \cdot 13 \cdot 19$.

(3) $a^2 + ab + b^2$ **の形で 4 通りに表せる最小の正の整数** (ここで a, b は正の整数)

$1729 = a^2 + ab + b^2$, ここで $(a, b) = (3, 40), (8, 37), (15, 32), (23, 25)$.

(4) $a^2 - ab + b^2$ **の形で 8 通りに表せる最小の正の整数**

$a^2 + ab + b^2 = a^2 - a(a + b) + (a + b)^2 = (a + b)^2 - (a + b)b + b^2$ と表せるので (3) の 2 倍の 8 通りある.

1729 の番外編 (Wikipedia)

各位の数字の総和と, その総和の数の数字の並び順を逆にした数との積が元の数に一致するという性質を持つ最大の正の整数. (by 藤原正彦)
上記の性質を持つ正の整数は次の 4 つである (cf. The On-Line Encyclopedia of Integer Sequences (OEIS) (A110921); オンライン整数列大辞典):

$$1729 = 19 \cdot 91, \ 1 + 7 + 2 + 9 = 19 : \text{ハーシャッド数},$$
$$1458 = 18 \cdot 81, \ 1 + 4 + 5 + 8 = 18,$$
$$81 = 9 \cdot 9, \ 8 + 1 = 9,$$
$$1 = 1 \cdot 1.$$

カーマイケル数に関する日本語の本は次を参照せよ:

「発見・予想を積み重ねる — それが整数論」(オーム社　安福 悠 (著))

4.2　指数型不定方程式 $10^x + 9^y = 12^z + 1$ と $(4^x + 1)(12^y + 1) = 8^z + 1$

定理 4.1. 指数型不定方程式

$$10^x + 9^y = 12^z + 1$$

は, ただ一つの正の整数解 $(x, y, z) = (3, 3, 3)$ をもつ.

注意. (1) (Euler の恒等式) $(9m^3 + 1)^3 + (9m^4)^3 = (9m^4 + 3m)^3 + 1^3$.
(2) (一橋大学入試問題, 2009) $x^3 + 1 = y^3 + 10^3 \Longrightarrow (x, y) = (12, 9)$.

Proof. $z \leq 3$ のとき, 明らかに (計算機により) 方程式の解は $(x, y, z) = (3, 3, 3)$ だけである. よって, $z \geq 4$ としてよい.

$x \leq 3$ のとき, $10^x - 1 = 12^z - 9^y$ と変形できるので, 解なしは容易に分かる. よって, $x \geq 4$ としてよい. また, $(-1)^y - 1 \equiv 2^z \pmod 5$ より, y は奇数である. 方程式を modulo 16 で考えると $9^y \equiv 1 \pmod{16}$ である. $9^2 = 81 \equiv 1 \pmod{16}$ かつ y は奇数より $9 \equiv 1 \pmod{16}$ となり矛盾! □

定理 4.2. 指数型不定方程式

$$(4^x+1)(12^y+1)=8^z+1$$

は, ただ一つの正の整数解 $(x,y,z)=(1,1,2)$ をもつ.

注意. $65=5\cdot 13=8^2+1$ を解とする不定方程式 $(4^x+1)(12^y+1)=8^z+1$ を下記のように解くのは容易であるが, $1729=7\cdot 13\cdot 19=12^3+1$ を解とする不定方程式

$$(6^x+1)(12^y+1)(18^z+1)=12^w+1$$

を解くのは容易ではない (cf. 定理 4.4).

Proof. 方程式の左辺を展開し整理すると,

$$4^x\cdot 12^y+4^x+12^y=2^{3z}. \tag{4.1}$$

(i) $x=y$ のとき, (4.1) は

$$2^{2x}(12^x+1+3^x)=2^{3z}$$

となる. $x=1$ のとき, $2^6=2^{3z}$ より $z=2$ を得る.
$x\geq 2$ のとき, $12^x+1+3^x\equiv 2,4 \pmod 8$ より容易に矛盾に至る.
(ii) $x>y$ のとき, (4.1) は

$$2^{2y}(4^x\cdot 3^y+4^{x-y}+3^y)=2^{3z}$$

となる. よって $4^x\cdot 3^y+4^{x-y}+3^y>1$ は奇数より矛盾!
(iii) $y>x$ のとき, (4.1) は

$$2^{2x}(12^y+1+4^{y-x}3^y)=2^{3z}$$

となる. よって $12^y+1+4^{y-x}3^y>1$ は奇数より矛盾! □

4.3 カーマイケル数

合成数 C がカーマイケル数かどうかを判定する方法は次である:

定理 4.3 (コルセルトの判定法)**.** C はカーマイケル数である $\iff$ $C=p_1p_2\cdots p_k$ かつ $(p_i-1)\mid (C-1)$. ただし $i=1,2,\ldots,k$ で, $p_1,p_2,\ldots,p_k$ $(k\geq 3)$ は相異なる奇素数である.

今後, k 個の素因数をもつカーマイケル数を C_k と表す.

予想 4.1 (C_3-1 が冪)**.** C_3-1 が冪, つまり, $C_3=a^n+1$ となる C_3,a,n (>1) の値は次の 2 つだけである:

$$1729=7\cdot 13\cdot 19=12^3+1,\quad 46657=13\cdot 37\cdot 97=6^6+1.$$

注意. 底 a が与えられたとき, Baker 理論より C_3,n は高々有限個存在する.

4.4 $C_3 = a^n + 1$

定理 4.4. a, n を 1 より大きい正の整数とする.
(1) a が奇数ならば, $C_3 = a^n + 1$ は解 a, n を持たない.
(2) $C_3 = 2^{tn} + 1$ は解 a, n を持たない.
(3) $C_3 = 6^n + 1 \iff 46657 = 13 \cdot 37 \cdot 97 = 6^6 + 1$.
(4) $C_3 = 12^n + 1 \iff 1729 = 7 \cdot 13 \cdot 19 = 12^3 + 1$.

Proof. 証明の概略を述べる.

(4) C_3 の素因数を p_i $(i = 1, 2, 3)$ とすると, コルセルトの判定法より, $C_3 - 1 = 12^n = 2^{2n}3^n \equiv 0 \pmod{p_i - 1}$ となる. よって $p_i - 1 = 2^{\alpha_i}3^{\beta_i}$ $(\alpha_i \geq 1,\ \beta_i \geq 0)$ を得る.

(i) n が奇数のとき,

$$C_3 = 12^n + 1 \equiv 0 \pmod{13}$$

となる. “カーマイケル数 C_3 の決定アルゴリズム” より, 13 を素因数にもつ C_3 をすべて決定できる:

$$\begin{aligned}
&C_3 = 1105 = 5 \cdot \mathbf{13} \cdot 17, \quad C_3 - 1 = 2^4 \cdot 3 \cdot 23;\\
&C_3 = 1729 = 7 \cdot \mathbf{13} \cdot 19, \quad C_3 - 1 = 2^6 \cdot 3^3;\\
&C_3 = 2821 = 7 \cdot \mathbf{13} \cdot 31, \quad C_3 - 1 = 2^2 \cdot 3 \cdot 5 \cdot 47;\\
&C_3 = 29341 = \mathbf{13} \cdot 37 \cdot 61, \quad C_3 - 1 = 2^2 \cdot 3^2 \cdot 5 \cdot 163;\\
&C_3 = 46657 = \mathbf{13} \cdot 37 \cdot 97, \quad C_3 - 1 = 2^6 \cdot 3^6;\\
&C_3 = 115921 = \mathbf{13} \cdot 37 \cdot 241, \quad C_3 - 1 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 23;\\
&C_3 = 314821 = \mathbf{13} \cdot 61 \cdot 397, \quad C_3 - 1 = 2^2 \cdot 3^3 \cdot 5 \cdot 11 \cdot 53;\\
&C_3 = 53081 = \mathbf{13} \cdot 97 \cdot 421, \quad C_3 - 1 = 2^6 \cdot 3 \cdot 5 \cdot 7 \cdot 79.
\end{aligned}$$

上記で $C_3 - 1 = 2^{2n}3^n$ となっているものは $C_3 = 1729$ のみ!

(ii) $n = 2k$ (k は奇数) のとき,

$$C_3 = 12^{2k} + 1 \equiv 0 \pmod{12^2 + 1 = 5 \cdot 29}$$

となる. しかし, $p - 1 = 29 - 1 = 2^2 \cdot 7$, 矛盾!

(iii) $n \equiv 0 \pmod 4$ のとき, $C_3 = 12^n + 1$ は次に帰着される:

$$(2^{\alpha_1}3^{\beta_1} + 1)(2^{\alpha_2}3^{\beta_2} + 1)(2^{\alpha_3}3^{\beta_3} + 1) = 2^{2n}3^n + 1.$$

ここで, $\alpha_i \geq 3$, $\beta_i \geq 0$ である. ここから先は少し面倒なので, 詳細は略す!

(3) (4) と同様に示すことができる.

(2) (4) と同様にして, $C_3 = 2^{tn} + 1$ は次に帰着される:

$$(2^{\alpha_1} + 1)(2^{\alpha_2} + 1)(2^{\alpha_3} + 1) = 2^{tn} + 1.$$

ここで, $\alpha_i \equiv tn \equiv 0 \pmod 4$ である. よって, Fermat の小定理 $x^4 \equiv 1 \pmod 5$ より, $(1+1)(1+1)(1+1) \equiv 1 + 1 \pmod 5$, 矛盾!

(1) コルセルトの判定法より明らかである. □

4.5 Eisenstein 数に関する指数型不定方程式

$\{a, b, 1729\}$ は

$$a^2 + ab + b^2 = 1729^2$$

を満たす Eisenstein 数である. ここで

$$\begin{aligned}(a, b) = {} & (96, 1679),\ (209, 1615),\ (249, 1591),\ (299, 1560),\ (361, 1520),\ (455, 1456),\\ & (504, 1421),\ (651, 1309),\ (656, 1305),\ (741, 1235),\ (799, 1185),\ (845, 1144),\\ & (931, 1064)\ \ (a < b)\end{aligned}$$

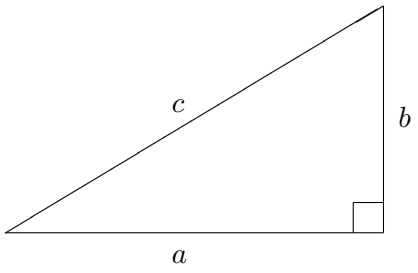
である. 一般に, Eisenstein 数 $\{a, b, c\}$ に関する指数型不定方程式の予想が知られている. この予想はピタゴラス数に関する Jeśmanowicz 予想の類似である (cf. Miyazaki [M2]).

予想 4.2 ([Te2], [TT])**.** $\{a, b, c\}$ を Eisenstein 数, つまり $a^2 + ab + b^2 = c^2$ を満たす正の整数とする. このとき, 指数型不定方程式

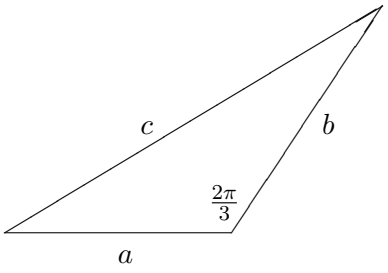
$$a^{2x} + a^x b^y + b^{2y} = c^z$$

は, ただ一つの正の整数解 $(x, y, z) = (1, 1, 2)$ をもつ.

注意. ピタゴラス数と Eisenstein 数は, 余弦定理より次のような図形的特徴をもつ.



ピタゴラス数 $\{a, b, c\} : a^2 + b^2 = c^2$



Eisenstein 数 $\{a, b, c\} : a^2 + ab + b^2 = c^2$

Eisenstein 数はピタゴラス数と類似の媒介変数表示をもつ.

補題 4.1 (Eisenstein 数の媒介変数表示)**.** 原始 Eisenstein numbers$\{a, b, c\}$ は次のように媒介変数表示される. ただし, $\gcd(a,\ b) = 1$, $a - b \equiv 1 \pmod 3$ である.

$$a = u^2 - v^2, \quad b = v(2u + v), \quad c = u^2 + uv + v^2.$$

ここで, u, v は $(u, v) = 1$, $u > v$, $u \not\equiv v \pmod 3$ を満たす正の整数である.

Eisenstein 数 a, b, c がある特別な場合に, 予想 4.2 が正しいことを確かめた.

定理 4.5 ([TT])**.** a, b, c, m を次を満たす正の整数とする:

$$a = m^2 - 1, \quad b = 2m + 1, \quad c = m^2 + m + 1, \quad \text{ここで } b \text{ は冪},$$

または

$$a = 2m + 1, \quad b = 3m^2 + 2m, \quad c = 3m^2 + 3m + 1, \quad \text{ここで } a \text{ は冪}.$$

このとき, 予想 4.2 は正しい.

謝辞

第 15 回福岡数論研究集会において講演する機会を与えて頂いた世話人の金子昌信先生 (九州大学), 権寧魯先生 (九州大学), 岸康弘先生 (愛知教育大学), 高妻倫太郎先生 (立命館アジア太平洋大学), 松坂俊輝先生 (九州大学) に深く感謝いたします. 本研究は科研費 (22K03271) の助成を受けたものである.

参考文献

[BG] B. C. Berndt and W. Galway, On the Brocard-Ramanujan diophantine equation $n! + 1 = m^2$, Ramanujan J. **4** (2000), no. 1, 41–42.

[BHV] Y. Bilu, G. Hanrot and P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, J. Reine Angew. Math. **539** (2001), 75–122.

[BMS] Y. Bugeaud, M. Mignotte and S. Siksek, Classical and modular approaches to exponential Diophantine equations II. The Lebesgue-Nagell equation, Compos. Math. **142**(2006), no. 1, 31–62.

[Da] A. Dąbrowski, On the Diophantine equation $n! + A = y^2$, Nieuw Arch. Wisk. (4) **14** (1996), no. 3, 321–324.

[De] V. A. Dem'janenko, On Jeśmanowicz' problem for Pythagorean numbers, Izv. Vyssˇ. Učebn. Zaved. Matematika**1965** (1965), no. 3, 52–56.

[DU] A. Dąbrowski and M. Ulas, Variations on the Brocard-Ramanujan equation, J. Number Theory **133** (2013), no. 4, 1168–1185.

[FLT] Y. Fujita, M.-H. Le and N. Terai, Some exponential Diophantine equations attached to Pythagorean triples, Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **65(113)** (2022), no. 3, 359–365.

[J] L. Jeśmanowicz, Several remarks on Pythagorean numbers, Wiadom. Mat. (2) **1** (1955), 196–202.

[KF] O. Kihel and F. Luca, Variants of the Brocard-Ramanujan equation, J. Théor. Nombres Bordeaux **20** (2008), no. 2, 353–363.

[Lu] W. Lu, On the Pythagorean numbers $4n^2 - 1, 4n$ and $4n^2 + 1$, Acta Sci. Nat. Univ. Szechuan **2** (1959), 39–42.

[M1] T. Miyazaki, Generalizations of classical results on Jeśmanowicz' conjecture concerning primitive Pythagorean triples, J. Number Theory **133** (2013), no. 2, 583–595.

[M2] T. Miyazaki, Application of cubic residue theory to an exponential equation concerning Eisenstein triples, Bull. Math. Soc. Sci. Math. Roumanie (N.S.) **62(110)** (2019), no. 3, 305–312.

[MT] T. Miyazaki and N. Terai, On Jeśmanowicz' conjecture concerning primitive Pythagorean triples II, Acta Math. Hungar. **147** (2015), no. 2, 286–293.

[Ra] S. Ramanujan, Question 469, J. Indian Math. Soc. **5** (1913), 59.

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

[Ta] K. Tanahashi, On the Diophantine equations $x^2 + 7^m = 2^n$ and $x^2 + 11^m = 3^n$, J. Predent. Fac. Gifu College Dent. (1977), no. 3, 77–79.

[Te1] N. Terai, The Diophantine equation $x^2 + q^m = p^n$, Acta Arith. **63** (1993), no. 4, 351–358.

[Te2] N. Terai, A remark on a conjecture concerning Eisenstein numbers, C. R. Math. Acad. Sci. Soc. R. Can. **22** (2000), no. 3, 105–110.

[Te3] N. Terai, On Jeśmanowicz' conjecture concerning primitive Pythagorean triples, J. Number Theory **141** (2014), 316–323.

[TF] N. Terai and Y. Fujita, On exponential Diophantine equations concerning Pythagorean triples, Publ. Math. Debrecen **101** (2022), no. 1-2, 147–168.

[TT] N. Terai and K. Takakuwa, On a Diophantine equation concerning Eisenstein numbers, Tokyo J. Math. **24** (2001), no. 2, 429–439.

[To] M. Toyoizumi, On the diophantine equation $y^2 + D^m = 2^n$, Comment. Math. Univ. St. Paul. **27** (1978), no. 2, 105–111.

[YH] P. Yuan and Y. Hu, On the diophantine equation $x^2 + D^m = p^n$, J. Number Theory **111** (2005), no. 1, 144–153.

[Z] K. Zsigmondy, Zur Theorie der Potenzreste, Monatsh. Math. Phys. **3** (1892), no. 1, 265–284.