

Euler 商に関する指数型不定方程式

寺井 伸浩 (大分大学)

概要

整数論において重要な Fermat 商, Euler 商, Wilson 商などの“商”を含む指数型不定方程式の正の整数解について研究する. 一般化された Fermat 予想や Catalan 予想などの最先端の指数型不定方程式に関するいろいろな結果を用いて, “商”を含む方程式の解を決定し, 関係する予想についても述べる.

1 序論

整数論において何々商と言われるものはいくつかあるが, Fermat 予想や単数・類数との関係で次の2つの商は特に重要である.

定義 1. p を奇素数, a を p で割り切れない正の整数とする. そのとき, 商

$$Q_p(a) = \frac{a^{p-1} - 1}{p}$$

は a を底とする p の **Fermat 商** と呼ばれる.

定義 2. $a (> 1)$ を正の整数, $m (> 2)$ を a と互いに素な正の整数とする. そのとき, 商

$$E_m(a) = \frac{a^{\varphi(m)} - 1}{m}$$

は a を底とする m の **Euler 商** と呼ばれる.

Fermat の小定理より, $Q_p(a)$ は整数である. Fermat 商を拡張したものが Euler 商であり, Euler の定理より $E_m(a)$ は整数である. $m = p$ が奇素数のとき $E_m(a) = Q_p(a)$ である.

著者は 1990 年前後に Fermat 商に関する指数型不定方程式

$$Q_p(a) = x^l$$

(ここで x は正の整数, l は素数) を考察していくつか結果を得ていた. 方法は合同式や 2 次体の結果を用いる初等的なものだった. 当時はまだ, Fermat 予想や Catalan 予想は証明されていなかった. Fermat 予想は Wiles [Wi] により 1995 年に, Catalan 予想は Mihailescu [Mi] により 2004 年にそれぞれ解決された. それ以降, 指数型不定方程式の研究は飛躍的に進展した.

本稿では, まず, Fermat 商に関する上の指数型不定方程式について Osada-Terai [OT], Terai [T1], Le [Le1], Cao [Ca] の結果を紹介し, 証明の概略を与える. 次に, 最近の一般化された Fermat 予想や Catalan 予想などのいろいろな結果を用いることにより, Euler 商に関する指数型不定方程式

$$E_m(a) = x^l$$

について Terai [T2] のいくつかの結果を証明し, 関係する予想を紹介する. 最後に, Wilson 商, Fermat-Wilson 商, Fibonacci 商を定義し, これら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.

2 補題

本稿で述べる定理を証明するために、多くの補題を準備する.

補題 1 (Cohn [Co]). 不定方程式

$$x^4 - Dy^2 = 1 \quad (D = 5, 10, 15, 30)$$

の正の整数解は次の通りである:

$D = 5$ なら $(x, y) = (3, 4)$, $D = 15$ なら $(x, y) = (2, 1)$, $D = 10, 30$ なら解なし.

次の結果はよく知られている. (cf. Nagell [N], Chapter VII, pp.229–230.)

補題 2 (Nagell [N]). 不定方程式

$$x^4 \pm 1 = 2y^2$$

は正の整数解 x, y ($xy > 1$) を持たない.

次の Lemma 3 において, $l > 4$ の場合は [BVY] の Theorem 1.5 から従う. $l = 3, 4$ の場合は Magma [BC] により容易に解ける.

補題 3 (Bennett-Vatsal-Yazdani [BVY]). l を $l \geq 3$ である正の整数とする. そのとき, 不定方程式

$$|x^l - 3y^l| = 2$$

は正の整数解 x, y ($|xy| > 1$) を持たない.

次の結果は数論における有名な未解決問題の一つであった Catalan 予想を解決している.

補題 4 (Mihailescu [Mi]). x, y, m, n を $x, y, m, n > 1$ である正の整数とする. そのとき, 不定方程式

$$x^m - y^n = 1$$

の正の整数解は $(x, y, m, n) = (3, 2, 2, 3)$ だけである.

補題 5 (Benett-Skinner [BS]). l を $l \geq 3$ である正の整数とする.

(i) 不定方程式

$$x^l + 1 = 2y^2$$

の正の整数解は $(x, y, l) = (1, 1, l), (23, 78, 3)$ だけである.

(ii) 不定方程式

$$x^l - 1 = 2y^2$$

の正の整数解は $(x, y, l) = (3, 11, 5)$ だけである.

補題 6. (i) (Störmer [S]) x, y を $x > 1, y \geq 1$ である正の整数, l を $l \geq 3$ である奇数とする. そのとき, 不定方程式

$$x^2 + 1 = 2y^l$$

は正の整数解 x, y, l を持たない.

(ii) (Ljunggren [Lj]) 不定方程式

$$x^2 + 1 = 2y^4$$

の正の整数解は $(x, y) = (1, 1), (239, 13)$ だけである.

(iii) (Ribet [Ri]) α を 2 以上の正の整数とする. そのとき, 不定方程式

$$a^p + 2^\alpha b^p + c^p = 0$$

は正の整数解 x, y, l を持たない.

3 Fermat 商に関する指数型不定方程式

この節では, Fermat 商に関する指数型不定方程式

$$Q_p(a) = x^l \tag{1}$$

を考える. ここで x は正の整数, l は素数とする.

(1) に関する最初の結果は Lucas による次の結果である.

定理 1 (Lucas [Lu]). $Q_p(2) : \text{平方数} \iff p = 3, 7$.

この結果を一般化するために, 著者は Osada-Terai [OT], Terai [T1] においていくつかの結果を得た.

注意 1. Fermat 商に関する次の入試問題 (2015 年九州大学) はとても興味深い!

(文系問題)

(1) n が正の偶数のとき, $2^n - 1$ は 3 の倍数であることを示せ.

(2) p を素数とし, k を 0 以上の整数とする. $2^{p-1} - 1 = p^k$ を満たす p, k の組をすべて求めよ.

解: $(p, k) = (2, 0), (3, 1)$.

(理系問題)

(1) n が正の偶数のとき, $2^n - 1$ は 3 の倍数であることを示せ.

(2) n を自然数とする, $2^n + 1$ と $2^n - 1$ は互いに素であることを示せ.

(3) p, q を異なる素数とする. $2^{p-1} - 1 = pq^2$ を満たす p, q の組をすべて求めよ.

解: $(p, q) = (7, 3)$.

3.1 指数型不定方程式 $Q_p(a) = x^l$ の解法

まず, (1) に関する一般的解法を述べる.

$Q_p(a) = x^l$ より $a^{p-1} - 1 = px^l$ となる.

(i) a : 偶数のとき,

$$\begin{cases} a^{(p-1)/2} \pm 1 = px_1^l \\ a^{(p-1)/2} \mp 1 = x_2^l. \end{cases} \quad (\text{Catalan 方程式})$$

ここで $x = x_1 x_2$ である.

(ii) a : 奇数のとき,

$$\begin{cases} a^{(p-1)/2} \pm 1 = 2px_1^l \\ a^{(p-1)/2} \mp 1 = 2^{l-1}x_2^l, \end{cases}$$

または

$$\begin{cases} a^{(p-1)/2} \pm 1 = 2^{l-1}px_1^l \\ a^{(p-1)/2} \mp 1 = 2x_2^l. \end{cases}$$

ここで $x = 2x_1 x_2$ である.

3.2 指数型不定方程式 $Q_p(a) = x^2$ に関する結果

特に, $l = 2$ のとき指数型不定方程式 $Q_p(a) = x^2$ を考える. $Q_p(a) = x^2$ より

$$a^{p-1} - 1 = px^2$$

となる.

$p = 3$ のとき $a^2 - 3x^2 = 1$: Pell 方程式となり無数の整数解をもつ. 以後, $p > 3$ とする.

定理 2 (Osada-Terai [OT], Terai [T1]). $Q_p(a) = x^2 \iff (a, p, x) = (2, 7, 3), (3, 5, 4)$.

Proof. (i) a : 偶数のとき,

$$a^{(p-1)/2} \mp 1 = x_2^2 \text{ (Catalan 方程式, 補題 4)} \implies x = 3, a = 2, p = 7.$$

(ii) a : 奇数のとき.

- $p \equiv 1 \pmod{4}$ のとき,

$$(a^{(p-1)/4})^4 - px^2 = 1 \text{ (Ljunggren, 1965)} \implies x = 4, a = 3, p = 5.$$

- $p \equiv 3 \pmod{4}$ のとき,

$$px^2 + 1 = (a^2)^{(p-1)/2} \text{ (Nagell, 1951): 解なし.}$$

□

3.3 指数型不定方程式 $Q_p(a) = x^l$ に関する結果

次の定理は Le [Le1], Cao [Ca] において Baker 理論を用いて示されたが³, Mihailescu の結果 (補題 4) と Ribet の結果 (補題 6(iii)) を用いると簡単に示される.

定理 3 (Le [Le1], Cao [Ca]). l を奇素数, $p \equiv 1 \pmod{4}$ とする. そのとき, $Q_p(a) = x^l$ は解なし.

Proof. (1) (i) a : 偶数のとき,

$$a^{(p-1)/2} \mp 1 = x_2^l \text{ (Catalan 方程式, 補題 4): 解なし.}$$

(ii) a : 奇数のとき. $p \equiv 1 \pmod{4}$ より, $a^{(p-1)/4} = A$ とおくと

$$A^4 - 1 = px^l$$

となる. p は素数なので, 次の 2 通りが起こる:

$$\begin{cases} A^2 + 1 = 2x_1^l \text{ (Störmer, 1899): 解なし} \\ A^2 - 1 = 2^{l-1}px_2^l, \end{cases}$$

または

$$\begin{cases} A^2 + 1 = 2px_1^l \\ A^2 - 1 = 2^{l-1}x_2^l \implies x_3^l - 2^{l-3}x_4^l = \pm 1 \text{ (Ribet, 補題 6): 解なし.} \end{cases}$$

ここで $x = 2x_1x_2 = 2x_1x_3x_4$ である.

□

4 Euler 商に関する指数型不定方程式

Fermat 商に関する指数型不定方程式 $Q_p(a) = x^l$ の結果を拡張するために、もっと一般的な指数型不定方程式

$$E_m(a) = x^l \quad (2)$$

を考える。ここで x は正の整数, l は素数とする。

4.1 指数型不定方程式 $E_m(a) = x^l$ に関する予想

$E_m(a) = x^l$ より $a^{\varphi(m)} - 1 = mx^l$ となる。

$(m, l) = (3, 2), (6, 2)$ のとき, 上の式は Pell 方程式

$$a^2 - 3x^2 = 1, \quad a^2 - 6x^2 = 1$$

となり無数の正の整数解 a, x をもつ。以後, これらを “exceptional cases” として除外する。また, $(a, m) = (2, 3)$ のとき $2^2 - 1 = 3 \cdot 1^l$ となるため, $x > 1$ としてこれも除外する。

予想 1 (指数型不定方程式 $E_m(a) = x^l$ の整数解). 指数型不定方程式 $E_m(a) = x^l$ のすべての整数解 (a, m, x, l) は次で与えられる:

$$(a, m, x, l) = (2, 7, 3, 2), (3, 5, 4, 2), (3, 10, 2, 3), (5, 3, 2, 3), (7, 6, 2, 3).$$

上記の解で $(m, l) = (3, 3), (6, 3), (10, 3)$ のときは, 楕円曲線の整数点から導かれるのが Magma によりすぐに分かる。

- $(m, l) = (3, 3)$ のとき, (2) は次の楕円曲線に帰着される:

$$E_9 : Y^2 = X^3 + 9.$$

ここで $X = 3x, Y = 3a$ である。Magma より $\text{rank } E_9(\mathbb{Q}) = 1$,

$$E_9(\mathbb{Z}) = (-2, \pm 1), (0, \pm 3), (3, \pm 6), (6, \pm 15), (40, \pm 253).$$

よって (2) の整数解 $(a, m, x, l) = (5, 3, 2, 3)$ を得る。

- $(m, l) = (6, 3)$ のとき, (2) は次の楕円曲線に帰着される:

$$E_{36} : Y^2 = X^3 + 36.$$

ここで $X = 6x, Y = 6a$ である。Magma より $\text{rank } E_{36}(\mathbb{Q}) = 1$,

$$E_{36}(\mathbb{Z}) = (-3, \pm 3), (0, \pm 6), (4, \pm 10), (12, \pm 42).$$

よって (2) の整数解 $(a, m, x, l) = (7, 6, 2, 3)$ を得る。

- $(m, l) = (10, 3)$ のとき, (2) は次の楕円曲線に帰着される:

$$E_{100} : Y^2 = X^3 + 100.$$

ここで $X = 10x, Y = 10a^2$ である。Magma より $\text{rank } E_{100}(\mathbb{Q}) = 1$,

$$E_{100}(\mathbb{Z}) = (-4, \pm 6), (0, \pm 10), (5, \pm 15), (20, \pm 90), (24, \pm 118), (2660, \pm 137190).$$

よって (2) の整数解 $(a, m, x, l) = (3, 10, 2, 3)$ を得る。

4.2 指数型不定方程式 $E_m(a) = x^l$ に関する結果

指数型不定方程式 $E_m(a) = x^l$ に関する著者の最近の結果を紹介する.

定理 4 (Terai [T2]). (1) a を偶数とする. そのとき, $E_m(a) = x^l \iff (a, m, x, l) = (2, 7, 3, 2)$.

(2) $E_m(a) = x^2 \iff (a, m, x, l) = (2, 7, 3), (3, 5, 4)$.

(3) $m \equiv 0 \pmod{4}$ または m は少なくとも 2 つの異なる奇素数を因数として持つとする. そのとき, $E_m(a) = x^l$ は解をもたない.

系 1. $E_m(a) = x^l$ が解をもつならば, $m = p$ または $m = 2p$ である. ここで p は奇素数である.

Proof. (1) $E_m(a) = x^l$ より $a^{\varphi(m)} - 1 = mx^l$ (a は偶数).

$m = 3$ のとき,

$$a^2 - 1 = 3x^l \implies X^l - 3X^l = \pm 2: \text{解なし (補題 3)}.$$

ここで $x = XY > 1$ である. 以後, $m > 3$ とする.

奇数 m の素因数分解を

$$m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

とする. ここで, p_1, \dots, p_r は異なる奇素数である. このとき

$$\varphi(m) = p_1^{e_1-1} p_2^{e_2-1} \cdots p_r^{e_r-1} (p_1 - 1)(p_2 - 1) \cdots (p_r - 1),$$

$$\varphi(m) \equiv 0 \pmod{2^r},$$

$$\varphi(m)/2^r > 1 \iff m > 3$$

となる. いま $A = a^{\varphi(m)/2^r}$ (: 冪) とおくと

$$(A^{2^{r-1}} + 1)(A^{2^{r-2}} + 1) \cdots (A^2 + 1)(A + 1)(A - 1) = mx^l$$

となる. したがって, 両辺の (素) 因数を数えることにより,

$$A^{2^k} + 1 = x_0^l \text{ または } A - 1 = x_0^l.$$

ここで $0 \leq k \leq r - 1$, $x_0 \mid x$ である. よって, 補題 4 (Catalan) より求める解を得る.

(2) (1) と同様にして, 指数型不定方程式

$$A^{2^k} + 1 = 2^s x_0^2 \text{ または } A - 1 = 2^s x_0^2$$

に帰着できる. ここで $0 \leq k \leq r - 1$, $x_0 \mid x$, $s = 0, 1$ である. よって, 補題 2, 4, 5 より求める解を得る.

(3) 省略する. □

5 他の商に関する指数型不定方程式

この節では, Wilson 商, Fermat-Wilson 商, Fibonacci 商を定義し, これら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.

5.1 Wilson 商

定義 3. 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.

定理 5 (Wilson 商の Fermat 商と Bernoulli 数との関係).

$$(1) \text{ (Lerch, 1905) } W_p \equiv \sum_{a=1}^{p-1} Q_p(a) \pmod{p}.$$

$$(2) \text{ (Lehmer, 1938) } W_p \equiv B_{2p-2} - B_{p-1} \pmod{p}.$$

次の定理は平方剰余の相互法則等を用いて初等的に示される.

定理 6 (平方数となる Wilson 商).

$$(1) W_p = x^2 \iff p = 3.$$

$$(2) W_p = px^2 \iff p = 5.$$

l 乗に関する次の予想は難しい.

予想 2 (Wilson 商に関する指数型不定方程式).

$$(1) W_p = x^l \iff (p, l) = (3, 2).$$

$$(2) W_p = px^l \iff (p, l) = (5, 2).$$

階乗に関しては, 次の予想は有名であるが, 未解決である.

予想 3 (Brocard-Ramanujan 予想, cf. [BG], [DU], [KF], [Ra]). $n! + 1 = m^2 \iff (n, m) = (4, 5), (5, 11), (7, 71)$.

Dabrovski [Da] は, もっと一般的な不定方程式

$$n! + A = m^2 \tag{3}$$

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) 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)

5.2 Fermat-Wilson 商

定義 4. p を奇素数, a を p で割り切れない正の整数とする. そのとき, 商

$$Fw_p(a) = \frac{(p-1)! + a^{p-1}}{p}$$

は a を底とする p の **Fermat-Wilson 商** と呼ばれる.

Fermat の小定理と Wilson の定理より, $Fw_p(a)$ は整数である.
指数型不定方程式

$$Fw_p(a) = x^l \tag{4}$$

を考える. $p = 3$, $l = 2$ のとき, (4) は Pell 方程式

$$a^2 - 3x^2 = -2$$

となり無数の正の整数解を持つ:

$$(a, x) = (1, 1), (5, 3), (19, 11), (71, 41), (265, 153), \\ (989, 571), (3691, 2131), (13775, 7953), \dots$$

(4) を一般の l 乗で解くのは難しいが, $p = x$ のとき整数解は完全に決定されている:

定理 7 (Le [Le2], Yu-Liu [YL]). l を正の整数とする. そのとき,

$$Fw_p(a) = p^l \iff (a, p, l) = (1, 3, 1), (1, 5, 2), (5, 3, 3).$$

この定理は Baker 理論を用いて証明される.

5.3 Fibonacci 商

F_n を次で定義される n 番目の Fibonacci 数とする:

$$F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n \quad (n = 0, 1, 2, 3, \dots).$$

任意の奇素数 p に対し,

$$F_{p - \left(\frac{5}{p}\right)} \equiv 0 \pmod{p}$$

が成り立つことはよく知られている. ここで, $\left(\frac{*}{*}\right)$ は Jacobi symbol を表す. 1960 年に Wall [Wa] は任意の奇素数 p に対し

$$F_{p - \left(\frac{5}{p}\right)} \not\equiv 0 \pmod{p^2}$$

が成り立つと予想したが, まだこれは未解決の難問である.

定義 5. p を奇素数, F_n を n 番目の Fibonacci 数とする. そのとき, 商

$$F(p) = \frac{F_{p - \left(\frac{5}{p}\right)}}{p}$$

は p の **Fibonacci 商** と呼ばれる.

定理 8. $F(p) = x^2 \iff p = 3, 5$.

この定理は Fibonacci 数のいろいろな性質を用いて示される.

参考文献

- [ADS] T. Agoh, K. Dilcher and L. Skula, *Fermat quotients for composite moduli*, J. Number Theory **66** (1997), 29–50.
- [BC] W. Bosma and J. Cannon, Handbook of magma functions, Department of Math., University of Sydney, available at <http://magma.maths.usyd.edu.au/magma/>.
- [BG] B. C. Berndt and W. Galway, *The Brocard-Ramanujan diophantine equation $n!+1 = m^2$* , Ramanujan J. **4** (2000), 41–42.
- [BS] M. A. Bennett and C. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), 23–54.
- [BVY] M. A. Bennett, V. Vatsal and S. Yazdani, *Ternary Diophantine equations of signature $(p, p, 3)$* , Compositio Math. **140** (2004), 1399–1416.
- [Ca] Z. Cao, *The Diophantine equations $x^4 - y^4 = z^p$ and $x^4 - 1 = dy^q$* , C. R. Math. Acad. Sci. Soc. R. Can. **21** (1999), 23–27.
- [Co] J. H. E. Cohn, *The Diophantine equations $x^4 - Dy^2 = 1$. II*, Acta Arith. **78** (1997), 401–403.
- [Da] A. Dabrowski, *On the Diophantine equation $n! + A = y^2$* , Nieuw Arch. Wisk. **14** (1996), 321–324.
- [Di] L. E. Dickson, History of the Theory of Numbers. Vol. I: Divisibility and primality, Chelsea Publishing Co., New York, 1966
- [DU] A. Dabrowski and M. Ulas, *Variations on the Brocard-Ramanujan equation*, J. Number Theory **133** (2013), 1168–1185.
- [KF] O. Kihel and F. Luca, *Variants of the Brocard-Ramanujan equation*, J. Théor. Nombres Bordeaux **20** (2008), 353–363.
- [KL] O. Kihel and C. Levesque, *On a few Diophantine equations related to Fermat’s last theorem*, Canad. Math. Bull. **45** (2002), 247–256.
- [Le1] M.-H. Le, *A note on the Diophantine equation $x^{p-1} - 1 = py^q$* , C. R. Math. Acad. Sci. Soc. R. Can. **15** (1993), 121–124.
- [Le2] M.-H. Le, *On the Diophantine equation $x^{p-1} + (p-1)! = p^n$* , Publ. Math. Debrecen **48** (1996), 145–149.
- [Lj] W. Ljunggren, *Zur Theorie der Gleichung $x^2 + 1 = Dy^4$* , Avh. Norske Vid. Akad. Oslo, I, (1942), 1–27.
- [Lu] E. Lucas, Théorie des nombre. Tome I: Le calcul des nombres entiers, le calcul des nombres rationnels, la divisibilité arithmétique, Nouveau tirage augmenté d’un avant-propos de Georges Bouligand, Librairie Scientifique et Technique Albert Blanchard, Paris, 1961

- [Mi] P. Mihailescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. **572** (2004), 167–195.
- [N] T. Nagell, *Introduction to Number Theory*. Second Edition, Chelsea Publishing Co., New York, 1964 .
- [OT] H. Osada and N. Terai, *Generalization of Lucas' theorem for Fermat's quotient*, C. R. Math. Acad. Sci. Soc. R. Can. **11** (1989), 115–120.
- [Ra] S. Ramanujan, *Question 469*, J. Indian Math. Soc. **5** (1913), 59.
- [Ri] K. Ribet, *On the equation $a^p + 2^\alpha b^p + c^p = 0$* , Acta Arith. **79** (1997), 7–16.
- [S] C. Störmer, *Solution complète en nombres entiers de l'équation $m \arctan \frac{1}{x} + n \arctan \frac{1}{y} = k \frac{\pi}{4}$* , Bull. Soc. Math. France, **27**(1899), 160–170.
- [SS] Z.-H. Sun and Z.-W. Sun, *Fibonacci numbers and Fermat's last theorem*, Acta Arith. **60** (1992), 371–388.
- [T1] N. Terai, *Generalization of Lucas' Theorem for Fermat's quotient. II*, Tokyo J. Math. **13** (1990), 277–287.
- [T2] N. Terai, *On exponential Diophantine equations containing the Euler quotient*, Bull. Australian Math. Soc. **91** (2015), 11–18.
- [Wa] D. D. Wall, *Fibonacci series modulo m* , Amer. Math. Monthly **67** (1960), 525–532.
- [Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), 443–551.
- [YL] K. Yu and D. Liu, *A complete resolution of a problem of Erdős and Graham*, Rocky Mountain J. Math. **26** (1996), 1235–1244.