

整数環内のパラメータを用いたディオファントス方程式の解法

遠藤 優斗

2025 年 2 月 22 日

要旨

$x^3 + y^3 = u^3 + v^3$ の互いに素な整数解を $\mathbb{Z}[\sqrt{-3}]$ 内の 2 変数を用いて表現する方法を用いて、いくつかのディオファントス方程式について、いくらでも大きな互いに素な整数解を得られることを示した。

1 はじめに

1.1 先行研究

ディオファントス方程式 $x^3 + y^3 = u^3 + v^3$ について, S.Ramanujan による無限個の整数解を与える公式[1], L.Euler による一般有理数解を与える公式[2]が知られているが, すべての整数解を与える公式は知られていない[3]. John C. Butcher (2022) では, $x = a + b$, $y = a - b$, $u = c + d$, $v = c - d$ と置換すると,

$$a(a^2 + 3b^2) = c(c^2 + 3d^2) \quad (1)$$

となり, 両辺の因子に $\mathbb{Z}[\sqrt{-3}]$ 内でのノルムの形が表れることから, 次の定理を示している[4].

定理 1.1. $x^3 + y^3 = u^3 + v^3$ の互いに素な整数解 (x, y, u, v) は, $\mathbb{Z}[\sqrt{-3}]$ 内の 2 変数を用いて表現することができる.

定理 1.1 では,(1)の互いに素な整数解 (a, b, c, d) を求めるときに,

$$a'(a^2 + 3b^2) = c'(c^2 + 3d^2)$$

の一般解が, $\zeta = \alpha + \beta\sqrt{-3}, \eta = \gamma + \delta\sqrt{-3}, \xi = s + t\sqrt{-3}$ として $X = \xi\bar{\xi}, Y = \eta\bar{\eta}, Z = \zeta\bar{\zeta}$ とおくと,

$$\begin{cases} a' = rY \\ a^2 + 3b^2 = XZ \\ c' = rX \\ c^2 + 3d^2 = YZ \end{cases}$$

と表せることを用いた後,

$$a' = a, \quad c' = c$$

の条件を用いて変数を減らす方法を用いている.

1.2 ルジャンドル記号

定義 1.2. 奇素数 p と, p と互いに素な整数 a に対して, 記号

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \exists x \in \mathbb{Z}[x^2 \equiv a \pmod{p}] \\ -1, & \forall x \in \mathbb{Z}[x^2 \not\equiv a \pmod{p}] \end{cases}$$

をルジャンドル記号とよぶ. この記号について, 次の定理が成り立つ[5].

定理 1.3. a, b を, 素数 p と互いに素な整数として,

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \quad (2)$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad (3)$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \quad (4)$$

p, q を相異なる奇素数として,

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \times \frac{q-1}{2}} \quad (5)$$

2 異なる環への応用

2.1 応用できる条件

$$a(a^2 + nb^2) = c(c^2 + nd^2)$$

の互いに素な整数解を同様の方法で求めることを考える.

$$a'(a^2 + nb^2) = c'(c^2 + nd^2)$$

の一般解を, $\gcd(a', c') = r$, $\gcd(a^2 + nb^2, c^2 + nd^2) = Z'$ として,

$$\begin{cases} a' = rY' \\ a^2 + nb^2 = X'Z' \\ c' = rX' \\ c^2 + nd^2 = Y'Z' \end{cases} \quad (6)$$

と表したときに, X', Y', Z' が $\mathbb{Z}[\sqrt{-n}]$ におけるノルムの形で表せなければならない.
この解法を応用できる環について, 次の定理が成り立つ.

定理 2.1. 条件 (*) を満たす n であれば (6) の表現をすることができる.

(*) : 「 n は素数または 2 の累乗である自然数であり, $e^2 + nf^2$ ($e, f \in \mathbb{N}$) で表せるすべての数について, 素因数 2 の個数を g とすると, その数の約数のうち e, f の約数でない奇素数と, 2^g がすべて $e_k^2 + nf_k^2$ ($e_k, f_k \in \mathbb{N}$) で表せる. 」

証明. n を条件 (*) を満たす自然数とする. (6) の左辺において, $a^2 + nb^2$ の約数に, a の約数であり n と異なる奇素数 p があるとき, b は p の倍数となり $a^2 + nb^2$ は p^2 の倍数である. このとき, X', Z' がともに p の倍数とすると, a, b, c, d がすべて p の倍数となり不適. よって, X', Z' のいずれかのみが p の倍数でありさらにその数の素因数 p の個数は偶数個となる. n, p^2 は $\mathbb{Z}[\sqrt{-n}]$ におけるノルムの形で表せることを考えると, ブラーマグプタの恒等式

$$(a^2 + nb^2)(c^2 + nd^2) = (ac \pm nbd)^2 + n(ad \mp bc)^2 \quad (7)$$

より, X', Y', Z' は $\mathbb{Z}[\sqrt{-n}]$ におけるノルムの形で表せるから, (6) の表現をすることができる.

2.2 応用できる環の例

p を $p \nmid n$ である奇素数, e, f を $p \nmid e, f$ である整数とする.

$$e^2 + nf^2 \equiv 0 \pmod{p}$$

に対し, $fh \equiv 1 \pmod{p}$ である整数 h をとり, 両辺に h^2 を掛けて $i = eh$ とすると,

$$i^2 \equiv -n \pmod{p}$$

とできることから, 次の定理が成り立つ.

定理 2.2. $n = 1, 2, 3, 4, 7$ は条件(*)を満たす.

証明. $\left(\frac{-n}{p}\right) = 1$ となる p と 2^g がすべて, $e_k^2 + nf_k^2$ で表せることを確認すればよい. $2^0 = 1^2 + n \times 0^2$ より以下 $g \in \mathbb{N}$ とする.

(i) $n = 1$ のとき

(3)より, $\left(\frac{-1}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod{4}$ となり, また, $e_k^2 + f_k^2 = p \Leftrightarrow p \equiv 1 \pmod{4}$ であることが知られている[6].

次に, $1^2 + 1 \times 1^2 = 2$ より, $e_k^2 + f_k^2 = 2$ なる e_k, f_k が存在するから, (7) を繰り返し用いることによりすべての g が $e_k^2 + f_k^2$ で表せることがわかる.

以上の2点から, $n = 1$ は条件(*)を満たす.

(ii) $n = 2$ のとき

(2), (3), (4)より,

$$\begin{aligned} \left(\frac{-2}{p}\right) = 1 &\Leftrightarrow \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1 \\ &\Leftrightarrow (-1)^{\frac{p-1}{2}} \frac{p^2-1}{8} = 1 \\ &\Leftrightarrow p \equiv 1, 3 \pmod{8} \end{aligned}$$

となり, また, $e_k^2 + 2f_k^2 = p \Leftrightarrow p \equiv 1, 3 \pmod{8}$ であることが知られている[6].

次に, $0^2 + 2 \times 1^2 = 2$ より, (7) を繰り返し用いることによりすべての g が $e_k^2 + 2f_k^2$ で表せることがわかる.

以上の2点から, $n = 2$ は条件(*)を満たす.

(iii) $n = 3$ のとき

(2), (3), (5)より,

$$\begin{aligned} \left(\frac{-3}{p}\right) = 1 &\Leftrightarrow \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = 1 \\ &\Leftrightarrow (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) = 1 \\ &\Leftrightarrow p \equiv 1 \pmod{6} \end{aligned}$$

となり, また, $e_k^2 + 3f_k^2 = p \Leftrightarrow p \equiv 1 \pmod{6}$ であることが知られている[6].

次に, $e_k^2 + 3f_k^2 = 2$ なる e_k, f_k は存在しないが, 必ず $g = 2g' (g' \in \mathbb{N})$ と表せることが知られている[6]. よって, $1^2 + 3 \times 1^2 = 2^2$ より, (7) を繰り返し用いることによりすべての g が $e_k^2 + 3f_k^2$ で表せることがわかる.

以上の2点から, $n = 3$ は条件(*)を満たす.

(iv) $n = 4$ のとき

(2), (3), (4)より,

$$\begin{aligned} \left(\frac{-4}{p}\right) = 1 &\Leftrightarrow \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{2}{p}\right) = 1 \\ &\Leftrightarrow (-1)^{\frac{p-1}{2}} \frac{p^2-1}{8} \frac{p^2-1}{8} = 1 \end{aligned}$$

$$\Leftrightarrow p \equiv 1 \pmod{4}$$

となり, また, $e_k^2 + 4f_k^2 = p \Leftrightarrow p \equiv 1 \pmod{4}$ であることが知られている[6].

次に, $e_k^2 + 4f_k^2 = 2$ なる e_k, f_k は存在しないが, $e_k^2 + 4f_k^2 \equiv 0, 1 \pmod{4}$ より, $g \geq 2$ である. ここで, $0^2 + 4 \times 1^2 = 2^2$, $2^2 + 4 \times 1^2 = 2^3$ より, (i) と同様に考えると, $2^g = (2^2)^j \times (2^3)^m$ (j, m は 0 以上の整数) と表せるとき, $2^g = e_k^2 + 4f_k^2$ と表せる. $2j + 3m$ は, $m = 0$ のとき 0 以上の偶数, $m = 1$ のとき 3 以上の奇数を表せるから 2 以上のすべての自然数を表せる. よって $2^g = (2^2)^j \times (2^3)^m$ と表せる g は 2 以上の自然数だから, すべての g が $e_k^2 + 4f_k^2$ で表せることがわかる.

以上の 2 点から, $n = 4$ は条件 (*) を満たす.

(v) $n = 7$ のとき

(2), (3), (5)より,

$$\begin{aligned} \left(\frac{-7}{p}\right) = 1 &\Leftrightarrow \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right) = 1 \\ &\Leftrightarrow (-1)^{\frac{p-1}{2}}(-1)^{\frac{3(p-1)}{2}}\left(\frac{p}{7}\right) = 1 \\ &\Leftrightarrow p \equiv 1, 2, 4 \pmod{7} \end{aligned}$$

となり, また, $e_k^2 + 7f_k^2 = p \Leftrightarrow p \equiv 1, 2, 4 \pmod{7}$ であることが知られている[6].

次に, $e_k^2 + 7f_k^2 = 2$ なる e_k, f_k は存在しないが, $e_k^2 + 7f_k^2 \equiv 0, 1, 3 \pmod{4}$ より, $g \geq 2$ である. ここで, $2^2 + 7 \times 0^2 = 2^2$, $1^2 + 7 \times 1^2 = 2^3$ より, (iv) と同様にしてすべての g が $e_k^2 + 7f_k^2$ で表せることがわかる.

以上の 2 点から, $n = 7$ は条件 (*) を満たす.

(i)~(v)より, 定理 3 は示された.

3 得られる恒等式

[4] では, 解を $\alpha + \beta\sqrt{-3}, \gamma + \delta\sqrt{-3}$ の 2 変数で表しているため, $(\alpha, \beta, \gamma, \delta) = (n, 1, n, 0)$ などを代入することで, n についての恒等式をつくることができ, いくらでも大きな値を生成できることを示している. $n = 1, 2, 4, 7$ の場合についても適切な値を代入することで恒等式をつくることができ, 次の定理が成り立つ.

定理 3.1. ディオファントス方程式

$$x^3 + x^2y + xy^2 + y^3 = u^3 + u^2v + uv^2 + v^3$$

$$3x^3 + x^2y + xy^2 + 3y^3 = 3u^3 + u^2v + uv^2 + 3v^3$$

$$5x^3 + x^2y + xy^2 + 5y^3 = 5u^3 + u^2v + uv^2 + 5v^3$$

$$2x^3 - x^2y - xy^2 + 2y^3 = 2u^3 - u^2v - uv^2 + 2v^3$$

$$x^3 - x^2y + xy^2 - y^3 = u^3 - u^2v + uv^2 - v^3$$

$$3x^3 - 5x^2y + 5xy^2 - 3y^3 = 3u^3 - 5u^2v + 5uv^2 - 3v^3$$

$$x^3 - 2x^2y + 2xy^2 - y^3 = u^3 - 2u^2v + 2uv^2 - v^3$$

$$5x^3 - 11x^2y + 11xy^2 - 5y^3 = 5u^3 - 11u^2v + 11uv^2 - 5v^3$$

$$2x^3 - 5x^2y + 5xy^2 - 2y^3 = 2u^3 - 5u^2v + 5uv^2 - 2v^3$$

について, $\max(x, y, u, v)$ がいくらでも大きな互いに素な整数解を生成することができる.

証明. n を条件 (*) を満たす自然数とする. ディオファントス方程式 $a(a^2 + nb^2) = c(c^2 + nd^2)$ の互いに素な整数解は, 定理 2.1 より, (6) のように表現することができる. a, c の値としてそれぞれ $\operatorname{Re} \xi\zeta, \operatorname{Re} \eta\zeta$ を採用すると, 条件 $a' = a, c' = c$ より,

$$\begin{cases} r(\gamma^2 + n\delta^2) = s\alpha - nt\beta \\ r(\alpha^2 + n\beta^2) = s\gamma - nt\delta \end{cases}$$

これを r, s, t について解くと,

$$\begin{pmatrix} r \\ s \\ t \end{pmatrix} = G^{-1} \begin{pmatrix} n(\beta\gamma - \alpha\delta) \\ n^2(\beta^3 - \delta^3) + n(\alpha^2\beta - \gamma^2\delta) \\ \alpha^3 - \gamma^3 + n(\alpha\beta^2 - \gamma\delta^2) \end{pmatrix}$$

となる. ただし, G^{-1} は $\gcd(r, s, t) = 1$ にするための定数である.

ここで, m を $n \nmid m$ である整数として $(\alpha, \beta, \gamma, \delta) = (m, 1, m, 0)$ を選ぶと,

$$\begin{pmatrix} r \\ s \\ t \end{pmatrix} = \begin{pmatrix} m \\ m^2 + n \\ m \end{pmatrix}$$

となり m の値によらずつねに互いに素な (r, s, t) を得ることができ, $a(a^2 + nb^2) = c(c^2 + nd^2)$ の互いに素な整数解

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} m^3 \\ 2m^2 + n \\ m^3 + nm \\ m^2 \end{pmatrix}$$

が得られる. さらに置換を施す前の方程式

$$(n+1)x^3 + (3-n)xy(x+y) + (n+1)y^3 = (n+1)u^3 + (3-n)uv(u+v) + (n+1)v^3 \quad (8)$$

の互いに素な整数解

$$\begin{pmatrix} x \\ y \\ u \\ v \end{pmatrix} = \begin{pmatrix} m^3 + 2m^2 + n \\ m^3 - 2m^2 - n \\ m^3 + m^2 + nm \\ m^3 - m^2 + nm \end{pmatrix}$$

が得られる.

また, 同様の方法をディオファントス方程式 $b(a^2 + nb^2) = d(c^2 + nd^2)$ にも適用することができる. 定理 2.1 より,

$$b'(a^2 + nb^2) = d'(c^2 + nd^2)$$

の一般解を, $\gcd(b', d') = r$, $\gcd(a^2 + nb^2, c^2 + nd^2) = Z'$ として,

$$\begin{cases} b' = rY' \\ a^2 + nb^2 = X'Z' \\ d' = rX' \\ c^2 + nd^2 = Y'Z' \end{cases}$$

と表現することができる. b, d の値としてそれぞれ $\text{Im } \xi\zeta, \text{Im } \eta\zeta$ を採用すると, 条件 $b' = b, d' = d$ より,

$$\begin{cases} r(\gamma^2 + n\delta^2) = t\alpha + s\beta \\ r(\alpha^2 + n\beta^2) = t\gamma + s\delta \end{cases}$$

これを r, s, t について解くと,

$$\begin{pmatrix} r \\ s \\ t \end{pmatrix} = G^{-1} \begin{pmatrix} ad - bc \\ \alpha^3 - \gamma^3 + n(\alpha\beta^2 - \gamma\delta^2) \\ n(\delta^3 - \beta^3) + \gamma^2\delta - \alpha^2\beta \end{pmatrix}$$

となる. ただし, G^{-1} は $\gcd(r, s, t) = 1$ にするための定数である.

ここで, m を $n \nmid m$ である整数として $(\alpha, \beta, \gamma, \delta) = (1, m, 0, m)$ を選ぶと,

$$\begin{pmatrix} r \\ s \\ t \end{pmatrix} = \begin{pmatrix} m \\ nm^2 + 1 \\ -m \end{pmatrix}$$

となり m の値によらずつねに互いに素な (r, s, t) を得ることができ, $b(a^2 + nb^2) = d(c^2 + nd^2)$ の互いに素な整数解

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 2nm^2 + 1 \\ nm^3 \\ nm^2 \\ nm^3 + m \end{pmatrix}$$

が得られる. さらに置換を施す前の方程式

$$(n+1)x^3 + (1-3n)xy(x-y) - (n+1)y^3 = (n+1)u^3 + (1-3n)uv(u-v) - (n+1)v^3 \quad (9)$$

の互いに素な整数解

$$\begin{pmatrix} x \\ y \\ u \\ v \end{pmatrix} = \begin{pmatrix} nm^3 + 2nm^2 + 1 \\ -nm^3 + 2nm^2 + 1 \\ nm^3 + nm^2 + m \\ -nm^3 + nm^2 - m \end{pmatrix}$$

が得られる.

(8), (9) において x, u は $m \geq 0$ で単調増加だから, m を大きくすることで $\max(x, y, u, v)$ がいくらでも大きな互いに素な整数解を生成できることがわかる.(8) に $n = 1, 2, 4, 7$, (9) に $n = 1, 2, 3, 4, 7$ をそれぞれ代入すると定理 3.1 の方程式となることより, 定理 3.1 は示された.

4 謝辞

本研究を行うにあたり指導していただいた, 秋葉先生, 河端先生, 松本先生をはじめとした数学科の先生方に感謝申し上げます.

5 参考文献

- [1] B. C. Berndt & S. Bhargava, “Ramanujan—for Lowbrows.” *Amer. Math. Monthly* 100.7. 1993. 644-656
- [2] H. L. Keng. *Introduction to Number Theory*. New York: Springer. 1982
- [3] L. E. Dickson. *History of the Theory of Numbers, Vol.2: Diophantine Analysis*. New York: Dover. 2005. 550-561
- [4] John C. Butcher. A New Solution to a Cubic Diophantine Equation. *Aioms*. 2022
- [5] 高木貞治. 初等整数論講義. 共立出版. 1971
- [6] David A. Cox. Primes of the Form $x^2 + ny^2$. Wiley. 1989