

# 方程式 $3x^4 + 3x^2 + 1 = y^2$ の整数解について

大塚美紀生

本稿では，方程式

$$3x^4 + 3x^2 + 1 = y^2 \quad (1)$$

の整数解を考える。[4]において，方程式

$$3x^2 + 3x + 1 = y^2$$

の整数解を完全に求めたものの， $x$  が平方数という条件で一般項を抜き出すのは困難である。(1)をうまく変数変換すると，よく知られた定理に帰着される。

定理 0 方程式

$$y^2 = x^3 - 1 \quad (2)$$

の整数解は  $(x, y) = (1, 0)$  のみである。

これを用いることにより，次の定理が得られる。

定理 1 方程式

$$3x^4 + 3x^2 + 1 = y^2 \quad (1)$$

の整数解は  $(x, y) = (0, \pm 1)$  のみである。

この定理と [4] の内容を組み合わせると，[1] のような数列の一般項の平方数問題について，一つの結果が得られる。

定理 2 漸化式

$$a_1 = 0, \quad a_2 = 7, \quad a_{n+2} = 14a_{n+1} - a_n + 6 \quad (n = 1, 2, 3, \dots)$$

で定義される数列  $\{a_n\}$  において，平方数となるのは  $a_1 = 0$  のみである。

## $Z[i]$ の整数論

代数的整数に馴染みのない人のために、2次体の整数論について少し解説しておく。とはいっても、代数的整数論の一般論まで述べるのは避け、本稿に必要な

$$Z[i] = \{a + bi \mid a, b \in Z\} \quad (i \text{は虚数単位})$$

を解説する程度にとどめることにする。代数的整数論に興味を持たれた方は、[3]や数論序説(小野孝著 裳華房発行)など代数的整数論の教科書を読まれることをおすすめする。なお、代数的整数論の知識のある方は、この章はとばされても差し支えない。

$i$ を虚数単位とするとき、 $a + bi$  ( $a, b \in Z$ )と表される数の集合  $Z[i]$  は(通常の)和、差、積について閉じており、あとで述べるように倍数・約数も定義できるので、有理整数(高校までで扱う通常の整数)と同様の議論が期待できる。 $Z[i]$ に属する数を、2次体  $Q(i)$ の整数と呼ぶ。<sup>注1</sup>

$\alpha = a + bi$  ( $a, b$ は有理数)に対して、

$$\bar{\alpha} = a - bi$$

を(有理数体上) $\alpha$ と共役な数<sup>注2</sup>であるといい、

$$N(\alpha) = \alpha \bar{\alpha} = a^2 + b^2$$

で定まる量を( $Q(i)$ における) $\alpha$ のノルム<sup>注2</sup>という。本稿では混同の恐れがないので、それぞれ略して共役な数、ノルムとだけ呼ぶことにする。

**命題1**  $N(\alpha) = 0 \iff \alpha = 0$

(証明)  $\alpha = \frac{a}{c} + \frac{b}{d}i$  ( $a, b, c, d$ は整数,  $c > 0, d > 0$ )とおくと、

$$N(\alpha) = \left(\frac{a}{c}\right)^2 + \left(\frac{b}{d}\right)^2 = \frac{a^2d^2 + b^2c^2}{c^2d^2}$$

$N(\alpha) = 0$ ならば  $a^2d^2 = -b^2c^2$ であるが、ここで  $a^2d^2 = -b^2c^2 \neq 0$ であるとすれば、左辺は正、右辺は負となって矛盾するから、 $a^2d^2 = -b^2c^2 = 0$ である。

$cd \neq 0$ であるから、

$$N(\alpha) = 0 \implies a = b = 0 \implies \alpha = 0$$

逆に、 $\alpha = 0$ ならば、 $N(0) = 0 \times \bar{0} = 0$ である。

(おわり)

**命題2**  $N(\alpha\beta) = N(\alpha)N(\beta)$

(証明)  $\alpha = a + bi, \beta = c + di$  ( $a, b, c, d$ は有理数)とおくと、

$$\alpha\beta = ac - bd + (ad + bc)i$$

であるから、

$$\begin{aligned} N(\alpha\beta) &= (ac - bd)^2 + (ad + bc)^2 \\ &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 \\ &= a^2(c^2 + d^2) + b^2(d^2 + c^2) \end{aligned}$$

$$\begin{aligned}
&= (a^2 + b^2)(c^2 + d^2) \\
&= N(\alpha)N(\beta) \qquad \qquad \qquad (\text{おわり})
\end{aligned}$$

$\mathbb{Z}[i]$ ではなく、 $\mathbb{Q}(i)$ の範囲で示したのは、少し広い範囲で示しておく方がこのあとの議論で都合が良いからである。 $\alpha, \beta \in \mathbb{Z}[i]$ に限定すると、命題1、命題2より

$$\beta \neq 0 \text{ ならば } N(\beta) \geq 1, N(\alpha\beta) \geq N(\alpha) \geq 0$$

が成り立つ。

有理整数のときと同様に、 $\mathbb{Z}[i]$ においても除法の基本定理が成り立つ。このことが有理整数と同様に扱える最大の理由である。

**命題3**  $\alpha, \beta \in \mathbb{Z}[i], \beta \neq 0$  に対して

$$\alpha = \beta\kappa + \rho, \quad 0 \leq N(\rho) < N(\beta)$$

を満たす  $\kappa, \rho \in \mathbb{Z}[i]$  が存在する。

(証明)  $\alpha = a + bi, \beta = c + di$  ( $a, b, c, d \in \mathbb{Z}$ ) とすると

$$\frac{\alpha}{\beta} = \frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{ac + bd + (bc - ad)i}{c^2 + d^2}$$

ここで、

$$\left| \frac{ac + bd}{c^2 + d^2} - m \right| \leq \frac{1}{2}, \quad \left| \frac{bc - ad}{c^2 + d^2} - n \right| \leq \frac{1}{2}$$

を満たす有理整数  $m, n$  が存在することに注意して、この  $m, n$  を用いて

$$\kappa = m + ni$$

とおくと、

$$\begin{aligned}
N\left(\frac{\alpha}{\beta} - \kappa\right) &= \left(\frac{ac + bd}{c^2 + d^2} - m\right)^2 + \left(\frac{bc - ad}{c^2 + d^2} - n\right)^2 \\
&\leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 < 1
\end{aligned}$$

命題2より

$$N\left(\frac{\alpha}{\beta} - \kappa\right)N(\beta) = N\left(\left(\frac{\alpha}{\beta} - \kappa\right)\beta\right) = N(\alpha - \beta\kappa)$$

であり、 $\beta \neq 0$  より  $N(\beta) > 0$  であるから

$$N(\alpha - \beta\kappa) < N(\beta)$$

よって、

$$\rho = \alpha - \beta\kappa$$

とおくと、

$$\alpha = \beta\kappa + \rho, \quad 0 \leq N(\rho) < N(\beta)$$

である。

(おわり)

命題3のような性質はユークリッド的 (euclidean) であるといい、ユークリッド的な環をユークリッド環という。 $Z[i]$ はユークリッド環であるが、2次体の整数環がすべてユークリッド的というわけではない。

$\varepsilon (\in Z[i])$  の逆数がまた  $Z[i]$  に属するとき、 $\varepsilon$  を  $Z[i]$  における単数という。これは、有理整数における単数が  $\pm 1$  であることの定義と同じである。単数であるかどうかの判定には、ノルムを用いればよい。

命題4  $\alpha \in Z[i]$  に対して、

$$\alpha \text{ が単数} \iff N(\alpha) = 1$$

(証明)  $\alpha$  が単数ならば、 $\beta = \frac{1}{\alpha} \in Z[i]$  であるから

$$\alpha\beta = 1$$

命題2より

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(1) = 1$$

であり、 $N(\alpha)$  は0以上の有理整数であるから、

$$N(\alpha) = 1$$

逆に、 $N(\alpha) = \alpha\bar{\alpha} = 1$  ならば、 $\alpha^{-1} = \bar{\alpha} \in Z[i]$  であるから、 $\alpha$  は単数である。

(おわり)

ここで注意すべきことは、 $Z[i]$  の要素を前提としていることである。例えば、

$$N\left(\frac{3}{5} + \frac{4}{5}i\right) = \left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1$$

ではあるが、 $\frac{3}{5} + \frac{4}{5}i$  は単数ではない。

命題5  $Z[i]$  における単数は  $\pm 1, \pm i$  である。

(証明)  $N(a + bi) = a^2 + b^2 = 1$  を満たす有理整数  $a, b$  を求めると、

$$(a, b) = (\pm 1, 0), (0, \pm 1)$$

に定まる。

(おわり)

有理整数のときと同じように、 $\alpha, \beta \in Z[i]$  ( $\beta \neq 0$ ) に対して

$$\alpha = \beta\gamma$$

となる  $\gamma \in Z[i]$  があるとき、 $\alpha$  は  $\beta$  の倍数、 $\beta$  は  $\alpha$  の約数であるという。また、 $\gamma$  が単数であるとき、 $\alpha$  と  $\beta$  は同伴であるという。特に、 $\alpha$  と  $\alpha$  は同伴である。最小公倍数や最大公約数についても、ノルム(の絶対値)<sup>注3</sup>が最小・最大であることをもって定義することができる。

0でも単数でもない整数  $\pi \in \mathbb{Z}[i]$  が、同様な約数と単数以外に約数をもたないとき、 $\mathbb{Z}[i]$ における素数という。  $2 = (1+i)(1-i)$  のように、有理整数において素数であっても、 $\mathbb{Z}[i]$ において素数であるとは限らないので注意を要する。

**命題 6**  $\mathbb{Z}[i]$ の素数  $\pi$  と同様な数  $\pi'$  および共役な数  $\bar{\pi}$  もまた素数である。

(証明)  $\pi$  と同様な数  $\pi'$  は

$$\pi' = \pi\varepsilon \quad (\varepsilon \text{ は単数})$$

と表され、 $\pi' = \alpha\beta$  ( $\alpha, \beta \in \mathbb{Z}[i]$ ) であるとすると、

$$\pi = \pi'\varepsilon^{-1} = \alpha(\beta\varepsilon^{-1})$$

より  $\alpha$  は  $\pi$  の約数であるから、 $\alpha$  は  $\pi$  に同伴または単数である。命題 2, 4 より単数の積も単数であるから、 $\alpha$  は  $\pi'$  に同伴または単数となって、 $\pi'$  も素数である。

$\bar{\pi}$  の約数の一つを  $\alpha$  とすると、

$$\bar{\pi} = \alpha\beta \quad (\alpha, \beta \in \mathbb{Z}[i])$$

と表される。両辺共役をとると

$$\pi = \bar{\alpha}\bar{\beta}$$

となり、 $\pi$  は素数であるから、

$$\bar{\alpha} = \pi\varepsilon \quad (\varepsilon \text{ は単数}) \text{ または } \bar{\alpha} \text{ は単数}$$

である。もう一度、両辺共役をとると(命題 4 より  $\bar{\varepsilon}$  も単数であり)

$$\alpha = \bar{\pi}\bar{\varepsilon} \text{ または } \alpha \text{ は単数}$$

であるから、 $\bar{\pi}$  も素数である。

(おわり)

命題 3 により、有理整数と同様に倍数・約数の議論ができるので、次の 2 つの命題が成り立つのも当然であろう。証明は有理整数の場合と全く同様なので省略する。

**命題 7**  $\mathbb{Z}[i]$ の素数  $\pi$  について

$$\pi \mid \alpha\beta \implies \pi \mid \alpha \text{ または } \pi \mid \beta \quad (\alpha, \beta \in \mathbb{Z}[i])$$

**命題 8**  $\mathbb{Z}[i]$ の整数  $\alpha$  が 0 でも単数でもないとき、積の順序、単数倍、同伴の違いを除いて、有限個の素数の積として一意に表される。

(定理 0 の証明)

(2)を変形すると

$$(y+i)(y-i) = x^3 \tag{3}$$

ここで、 $\mathbb{Z}[i]$ の素数  $\pi$  が  $y+i$  と  $y-i$  の公約数であるとすれば、

$$(y+i) - (y-i) = 2i$$

の約数でもあり、 $i$  は単数であるから

$$\pi \mid 2$$

ノルムを考えると

$$N(\pi) \mid N(2) = 2^2$$

命題 4 より  $N(\pi) > 1$  であるから

$$N(\pi) = 2 \text{ または } N(\pi) = 4$$

の場合に限られ、

$$N(\pi) \mid N(y+i) = y^2 + 1$$

より  $y$  は奇数であり、(2)より  $x$  は偶数である。このとき、

$$y^2 \equiv 1 \pmod{4}, \quad x^3 - 1 \equiv -1 \pmod{4}$$

となって (2) が成り立つことに反するから、

$$y+i \text{ と } y-i \text{ は互いに素 (最大公約数が単数と同伴)}$$

である。

(3)に命題 8 を適用すると、

$$y+i = \varepsilon(a+bi)^3$$

を満たす  $\mathbb{Z}[i]$  の単数  $\varepsilon$ 、および有理整数  $a, b$  が存在する。命題 5 より

$$\varepsilon = \pm 1, \pm i$$

であり、

$$1 = 1^3, \quad -1 = (-1)^3, \quad i = (-i)^3, \quad -i = i^3$$

であるから、

$$y+i = (a+bi)^3 = a^3 - 3ab^2 + (3a^2b - b^3)i$$

と考えてよい。虚部を比べると

$$b(3a^2 - b^2) = 1 \quad \therefore b = 3a^2 - b^2 = \pm 1$$

$b = 1$  のとき  $3a^2 - 1 = 1$  を満たす有理整数  $a$  は存在しないから、

$$b = -1, \quad a = 0$$

に限られ、

$$y = a^3 - 3ab^2 = a(a^2 - 3b^2) = 0$$

$$y^2 = x^3 - 1 = (x-1)(x^2 + x + 1) \text{ および } x^2 + x + 1 = \left(x + \frac{1}{2}\right)^2 + \frac{3}{4} > 0 \text{ より}$$

$$x = 1$$

(証明おわり)

定理 1 の証明

(1) を満たす整数  $x, y$  に対して,

$$X = 3x^2 + 1, \quad Y = 3xy$$

と置くと,

$$\begin{aligned}
Y^2 &= 9x^2y^2 \\
&= 9x^2(3x^4 + 3x^2 + 1) \\
&= (3x^2)^3 + 3(3x^2)^2 + 9x^2 \\
&= (X - 1)^3 + 3(X - 1)^2 + 3(X - 1) \\
&= X^3 - 1
\end{aligned}$$

定理 0 より

$$X = 3x^2 + 1 = 1 \quad \text{かつ} \quad Y = 3xy = 0$$

に限られるから,

$$x = 0$$

よって, (1) の整数解は

$$(x, y) = (0, \pm 1)$$

のみである。

(証明おわり)

定理 2 の証明

[4] によると, 方程式

$$3x^2 + 3x + 1 = y^2 \tag{4}$$

の正の整数解  $(x, y)$  に対して

$$X = 2x + 1, \quad Y = 2y \tag{5}$$

により変換すると,

$$Y^2 - 3X^2 = 1$$

が成り立ち, 正の整数解  $(X, Y) = (x_n, y_n)$  は

$$x_1 = 1, \quad y_1 = 2, \quad \begin{cases} x_{n+1} = 2x_n + y_n \\ y_{n+1} = 3x_n + 2y_n \end{cases} \quad (n = 1, 2, 3, \dots) \tag{6}$$

で尽くされ, (5) で逆変換することにより, 方程式 (4) の非負整数解は

$$(x, y) = \left( \frac{x_{2n-1} - 1}{2}, \frac{y_{2n-1}}{2} \right)$$

で尽くされる。<sup>注4</sup>

$$a_n = \frac{x_{2n-1} - 1}{2}, \quad b_n = \frac{y_{2n-1}}{2} \tag{7}$$

とおくと, (6) より

$$\begin{aligned}
2a_{n+1} + 1 &= x_{2n+1} \\
&= 2x_{2n} + y_{2n} \\
&= 2(2x_{2n-1} + y_{2n-1}) + (3x_{2n-1} + 2y_{2n-1}) \\
&= 7x_{2n-1} + 4y_{2n-1} \\
&= 7(2a_n + 1) + 4 \cdot 2b_n \\
\therefore a_{n+1} &= 7a_n + 4b_n + 3 \tag{8}
\end{aligned}$$

$$\begin{aligned}
2b_{n+1} &= y_{2n+1} \\
&= 3x_{2n} + 2y_{2n} \\
&= 3(2x_{2n-1} + y_{2n-1}) + 2(3x_{2n-1} + 2y_{2n-1}) \\
&= 12x_{2n-1} + 7y_{2n-1} \\
&= 12(2a_n + 1) + 7 \cdot 2b_n \\
\therefore b_{n+1} &= 12a_n + 7b_n + 6 \tag{9}
\end{aligned}$$

(6), (7), (8)より

$$a_2 = 7a_1 + 4b_1 + 3 = 7 \times 0 + 4 \times 1 + 3 = 7$$

(8)を(9)に代入して

$$\frac{a_{n+2} - 7a_{n+1} - 3}{4} = 12a_n + 7 \cdot \frac{a_{n+1} - 7a_n - 3}{4} + 6$$

$$\therefore a_{n+2} = 14a_{n+1} - a_n + 6$$

$a_1 = 0 < a_2 = 7$ であり,  $0 < a_k < a_{k+1}$ であるとすれば,

$$a_{k+2} - a_{k+1} = 12a_{k+1} + (a_{k+1} - a_k) + 6 > 0 + 0 + 6 > 0$$

であるから,

$$a_1 = 0 < a_2 < a_3 < \dots < a_n < \dots$$

方程式(4)の非負整数解は  $(a_n, b_n) (n = 1, 2, 3, \dots)$  で尽くされるから, 定理1より

$$a_n \text{ が平方数ならば } a_n = 0$$

であり,  $\{a_n\}$  は増加数列であるから

$$a_n = 0 \iff n = 1$$

である。

(証明おわり)



注1 誤解がないように述べれば，2次体  $Q(i)$  に属する数の中で  $x$  の2次方程式

$$x^2 + ax + b = 0 \quad (a, b \in \mathbf{Z})$$

の解となるものが2次体  $Q(i)$  の整数であり，その全体が  $\mathbf{Z}[i]$  となる。これはすべての整数環について成り立つわけではない。例えば，2次体  $Q(\sqrt{5})$  の整数全体は  $\mathbf{Z}[\sqrt{5}]$  ではなく，

$$\mathbf{Z}\left[\frac{1+\sqrt{5}}{2}\right] = \left\{a + b\frac{1+\sqrt{5}}{2} \mid a, b \in \mathbf{Z}\right\}$$

となる。ただ，本稿の内容を説明するだけであれば，はじめから  $\mathbf{Z}[i]$  に属する数が整数だと解釈して差し支えない。

注2 有理数上共役は，実部も虚部も有理数に限定すると，高校で習う共役複素数と同じことになり，ノルムは絶対値の平方と同じことになるが，一般の用語で説明しておくことで， $\mathbf{Z}[i]$  以外の2次体についても類推できるように配慮した。

注3 実2次体のノルムはつねに正であるとは限らないので，一般にはノルムの絶対値で考える。

注4 [4] は整数解が無数にあることを示したもので，整数解が一般にどのように表現されるかが未整理であるため，ここで慌ててまとめを行なった次第である。

## 参考文献

- [1] J.H.E.Cohn, *Square Fibonacci Numbers, Etc.*,  
Fibonacci Quarterly 2(1964), 109–113
- [2] D.Duverney (塩川宇賢 訳), 数論, 森北出版(2006)
- [3] 稲葉栄次, 整数論, 共立出版(1956)
- [4] 大塚美紀生, 方程式  $3x^2 + 3x + 1 = y^2$ , 早稲田数学フォーラム(2007)  
<http://wasmath.la.coocan.jp/3x2+3x+1=y2.pdf>