

方程式 $3x^4 - 3x^2y^2 + y^4 = z^2$ について

大塚美紀生

定理 自然数 x, y, z が

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

を満たすならば, $x^2 = y^2 = z$ である。

[1]において, 方程式 $x^3 + y^3 = 2z^3$ を解くための補題として上の定理を示したが, ピタゴラス方程式でお馴染みの手法だけで示せるものの, 証明の見通しは良いとは言えない。そこで, もう少し見通し良く示せないかと考えたのが本稿の動機である。^{注1}

本稿における証明のポイントは,

$$\frac{a}{b} = \frac{c}{d} \quad (a, b, c, d \text{ は自然数}) \text{ の両辺が既約分数ならば } a = c, b = d$$

が成り立つことへ持ち込むところにある。

定理の証明

(1)を満たす自然数 (x, y, z) の組の中に $x \neq y$ となるものが存在するとき,

x は $x \neq y$ となる最小のもの

であるとする。

$d = \gcd(x, y) > 1$ のときは, (1)より $d^4 | z^2$ であるから

$$x = dx_1, \quad y = dy_1, \quad z = d^2z_1 \quad (x_1, y_1, z_1 \text{ は自然数})$$

と表すことができ,

$$(1) \iff 3x_1^4 - 3x_1^2y_1^2 + y_1^4 = z_1^2$$

$$x^2 = y^2 = z \iff x_1^2 = y_1^2 = z_1$$

であるから, はじめから

x と y は互いに素である

と仮定して証明すれば十分である。

ここで $3|y$ であるとする, (1)より

$$3|y \implies 3|z^2 \implies 3^2|3x^4 \implies 3|x^4 \implies 3|x$$

となって x と y が互いに素であることに反するから,

y は 3 で割り切れない。

$3x^4 - 3x^2y^2 = z^2 - y^4 = (z + y^2)(z - y^2)$ より $z + y^2$ と $z - y^2$ の少なくとも一方は 3 で割り切れるが,

$$(z + y^2) - (z - y^2) = 2y^2$$

は 3 で割り切れないから,

$z + y^2$ と $z - y^2$ の一方は 3 で割り切れ, 他方は 3 で割り切れない。

1° $3 \nmid z + y^2, 3 \mid z - y^2$ のとき

$$\frac{z + y^2}{x^2} = \frac{m}{n} \quad (m \text{ と } n \text{ は互いに素な自然数}) \quad (2)$$

とおくと, $3 \nmid m$ であり,

$$z = \frac{m}{n}x^2 - y^2$$

(1)に代入して

$$\begin{aligned} 3x^4 - 3x^2y^2 &= \frac{m^2}{n^2}x^4 - \frac{2m}{n}x^2y^2 \\ \left(\frac{2m}{n} - 3\right)x^2y^2 &= \left(\frac{m^2}{n^2} - 3\right)x^4 \\ \therefore \frac{y^2}{x^2} &= \frac{m^2 - 3n^2}{n(2m - 3n)} \end{aligned} \quad (3)$$

$$m^2 - 3n^2 - n(2m - 3n) = m(m - 2n) \text{ より}$$

$$\gcd(m^2 - 3n^2, n(2m - 3n)) = \gcd(n(2m - 3n), m(m - 2n))$$

$$\gcd(m, n) = 1 \text{ および } 3 \nmid m \text{ より}$$

$$\gcd(n, m - 2n) = \gcd(n, m) = 1$$

$$\gcd(2m - 3n, m) = \gcd(3n, m) = 1$$

$$\gcd(2m - 3n, m - 2n) = \gcd(2(m - 2n) + n, m - 2n)$$

$$= \gcd(n, m - 2n)$$

$$= \gcd(n, m)$$

$$= 1$$

であるから, (3)より

$$y^2 = \pm(m^2 - 3n^2), x^2 = \pm n(2m - 3n) \quad (\text{複号同順})$$

$3 \nmid m$ より $m^2 - 3n^2 \equiv m^2 \equiv 1 \pmod{3}$ であるから, $y^2 \equiv 0, 1 \pmod{3}$ より

$$y^2 = m^2 - 3n^2 \quad (4)$$

$$x^2 = n(2m - 3n) \quad (5)$$

に定まる。

$$(4) \iff (m + y)(m - y) = 3n^2$$

$$3 \nmid 2m = (m + y) + (m - y)$$

より, $m + y$ と $m - y$ の一方は 3 で割り切れ, 他方は 3 で割り切れないから,

$$\begin{cases} 3 \nmid m + y \text{ のとき } \frac{m + y}{n} = \frac{l}{k} \\ 3 \nmid m - y \text{ のとき } \frac{m - y}{n} = \frac{l}{k} \end{cases} \quad (k \text{ と } l \text{ は互いに素な自然数}) \quad (6)$$

とおくと, いずれの場合も (4)より

$$\frac{l^2}{k^2}n^2 - \frac{2l}{k}mn = -3n^2 \quad \therefore \frac{m}{n} = \frac{k}{2l} \left(\frac{l^2}{k^2} + 3 \right) = \frac{3k^2 + l^2}{2kl}$$

(5)より

$$\frac{x^2}{n^2} = 2 \cdot \frac{m}{n} - 3 = \frac{3k^2 - 3kl + l^2}{kl} \quad (7)$$

k と l は互いに素であるから

$$\gcd(k, 3k^2 - 3kl + l^2) = \gcd(k, l^2) = 1$$

(6)より $3 \nmid l$ であるから

$$\gcd(l, 3k^2 - 3kl + l^2) = \gcd(l, 3k^2) = 1$$

よって, (7)より

$$k = u^2, \quad l = v^2, \quad 3k^2 - 3kl + l^2 = w^2 \quad (8)$$

を満たす自然数 u, v, w が存在^{注2}し, k と l を消去すると

$$3u^4 - 3u^2v^2 + v^4 = w^2$$

(2), (6), (8)より

$$x^2 \geq n \geq k = u^2 \quad (9)$$

であるから, x の最小性より

$$x = u \quad \text{または} \quad x > u = v \quad \text{注3}$$

$x = u$ のとき, (9)より $x^2 = n = k$ であり, (7)より

$$1 = \frac{3k^2 - 3kl + l^2}{l} = \frac{3k^2}{l} - 3k + l$$

であるから $\frac{3k^2}{l}$ は整数であり, $\gcd(k, l) = 1, 3 \nmid l$ より

$$l = 1 \quad \therefore k = l = 1$$

$u = v$ のときも (8) および $\gcd(k, l) = 1$ より $k = l = 1$ となるから,

いずれの場合も $k = l = 1$

(6), (4)より

$$(m + y, m - y) = (n, 3n) \quad \text{または} \quad (3n, n)$$

であるが, $m + y > m - y$ より

$$m + y = 3n, \quad m - y = n \quad \therefore m = 2n, \quad y = n$$

(5)より

$$x = y = n \quad \text{注4}$$

となって $x \neq y$ と仮定したことに反する。

2° $3 \mid z + y^2, 3 \nmid z - y^2$ のとき

$$\frac{z - y^2}{x^2} = \frac{m}{n} \quad (m \text{ と } n \text{ は互いに素な整数, } n > 0)$$

とおくと, $3 \nmid m$ であり,

$$z = \frac{m}{n}x^2 + y^2$$

(1)に代入して

$$3x^4 - 3x^2y^2 = \frac{m^2}{n^2}x^4 + \frac{2m}{n}x^2y^2$$

$$\left(\frac{2m}{n} + 3\right)x^2y^2 = \left(3 - \frac{m^2}{n^2}\right)x^4$$

$$\therefore \frac{y^2}{x^2} = \frac{3n^2 - m^2}{n(2m + 3n)} \quad (10)$$

$$n(2m + 3n) - (3n^2 - m^2) = m(m + 2n) \text{ より}$$

$$\gcd(3n^2 - m^2, n(2m + 3n)) = \gcd(n(2m + 3n), m(m + 2n))$$

$$\gcd(m, n) = 1 \text{ および } 3 \nmid m \text{ より}$$

$$\gcd(n, m + 2n) = \gcd(n, m) = 1$$

$$\gcd(2m + 3n, m) = \gcd(3n, m) = 1$$

$$\begin{aligned} \gcd(2m + 3n, m + 2n) &= \gcd(2(m + 2n) - n, m + 2n) \\ &= \gcd(n, m + 2n) \\ &= \gcd(n, m) \\ &= 1 \end{aligned}$$

$m > 0$ のとき $n(2m + 3n) > 0$ であり, (10)より $x^2 = n(2m + 3n)$, $y^2 = 3n^2 - m^2$ となるが, $3 \nmid m$ より

$$3n^2 - m^2 \equiv -m^2 \equiv -1 \pmod{3}$$

となって $y^2 \equiv 0, 1 \pmod{3}$ と矛盾するから,

$$m < 0, \quad x^2 = n(-2m - 3n), \quad y^2 = m^2 - 3n^2$$

に限られる。以下,

$$m \mapsto -m$$

と置き換えることにより, 1° と全く同様の議論となる。

以上により, 定理は証明された。

注1 単なる別証明のようにもみえるが, 変形の見通しは随分良くなったと思われる。また, [1] のような $2^2 - 1 = 3$ という偶然に依存する方針でもない。証明の長さがほとんど変わらないのは, [1] に比べて詳しく説明をつけたためであると言いつけておく。

注2 x と n は必ずしも互いに素というわけではないが, $\frac{x^2}{n^2}$ を約分すると素数の平方ごとに約されるので, 既約分数表示しても平方数の比となる。

注3 「 $x = u$ または $x > u = v$ 」を導いただけでは何も矛盾しない。というのも, (x, y, z) と x が必ずしも 1 対 1 に対応しているわけではないので, $x = y$ なる自然数解の組の中に x の値だけ一致するものがないとは(その時点では)言えないからである。

注 4 $m = 2n$, $\gcd(m, n) = 1$ より $m = 2$, $n = 1$ まで導かれるが, 結局矛盾しているわけであるから, 詳しく求めても何だか空しい。

参考文献

- [1] 大塚美紀生, ディオファントス方程式 $x^3 + y^3 = 2z^3$ について,
早稲田数学フォーラム (2009)
<http://homepage2.nifty.com/wasmath/x3+y3=2z3.pdf>
- [2] P.Ribenboim, *Catalan's Conjecture*, Academic Press (1994)

2010. 2. 12
修正 2012. 2. 3