

方程式 $8x^4 + 6x^2y^2 - 5y^4 = z^2$ の整数解

大塚美紀生

ディオファントス方程式 $x^4 + 12x^2y^2 + y^4 = z^2$ を解く過程において，方程式 $8x^4 + 6x^2y^2 - 5y^4 = z^2$ が現れる^{注1}が，本稿ではこの方程式の解の構造について考察する。

定理 正の整数 x と正の奇数 y ， z ^{注2} が方程式

$$8x^4 + 6x^2y^2 - 5y^4 = z^2$$

を満たすならば， $x = y$ である。

定理の証明

$$8x^4 + 6x^2y^2 - 5y^4 = z^2 \tag{1}$$

かつ

$$x \neq y$$

を満たす自然数の組 (x, y, z) (y, z は奇数) が存在するとすれば，その中で x が最小

となるものが存在するはずである。そう仮定して議論を進めることにする。

$\gcd(x, y) = d$ とすると，(1) より $d^4 \mid z^2$ となるから

$$x = dx_1, y = dy_1, z = d^2z_1$$

を満たす自然数 x_1, y_1, z_1 が存在して

$$8x_1^4 + 6x_1^2y_1^2 - 5y_1^4 = z_1^2$$

が成り立つ。 x の最小性より $d = 1$ となるから，

x と y は互いに素

である。

$$8x^4 + 6x^2y^2 - 5y^4 = (2x^2 - y^2)(4x^2 + 5y^2)$$

と因数分解されることに注目する。 y は奇数であるから

$$\gcd(2x^2 - y^2, y^2) = \gcd(2x^2, y^2) = \gcd(x^2, y^2) = 1$$

であることを用いて，

$$4x^2 + 5y^2 = 2(2x^2 - y^2) + 7y^2$$

より

$$\begin{aligned} \gcd(2x^2 - y^2, 4x^2 + 5y^2) &= \gcd(2x^2 - y^2, 7y^2) \\ &= \gcd(2x^2 - y^2, 7) \\ &= 1 \text{ または } 7 \end{aligned}$$

であるから，(1)より

$$(2x^2 - y^2, 4x^2 + 5y^2, z) = (a^2, b^2, ab) \text{ または } (7a^2, 7b^2, 7ab)$$

を満たす互いに素な正の奇数 a, b が存在する。ここで, x が偶数ならば

$$4x^2 + 5y^2 \equiv 5 \pmod{8},$$

x が奇数ならば

$$2x^2 - y^2 \equiv 2 - 1 \equiv 1 \pmod{8}, \quad 4x^2 + 5y^2 \equiv 4 + 5 \equiv 1 \pmod{8}$$

であるから, x と y はともに奇数であり,

$$2x^2 - y^2 = a^2 \tag{2}$$

$$4x^2 + 5y^2 = b^2 \tag{3}$$

である場合に限られる。

(2)を変形すると

$$x^2 = \frac{y^2 + a^2}{2} = \left(\frac{y+a}{2}\right)^2 + \left(\frac{y-a}{2}\right)^2 \tag{4}$$

$\frac{y+a}{2}$ と $\frac{y-a}{2}$ が共通の素因数 p をもつとすれば,

$$p|y \text{ かつ } p^2|x^2$$

より $p|x$ かつ $p|y$ が成り立って互いに素であることに反するから,

$$\frac{y+a}{2} \text{ と } \frac{y-a}{2} \text{ は互いに素}$$

である。 $x \neq y$ の仮定のもとでは, (2)より

$$y \neq a$$

であるから, (4)にピタゴラス方程式の定理^{注3}を適用すると

$$x = m^2 + n^2, \quad \frac{y+a}{2} = m^2 - n^2, \quad \frac{|y-a|}{2} = 2mn$$

または

$$x = m^2 + n^2, \quad \frac{y+a}{2} = 2mn, \quad \frac{|y-a|}{2} = m^2 - n^2$$

を満たすような偶奇の異なる互いに素な自然数 m, n が存在する。必要ならば, m と n を入れかえることにより

$$x = m^2 + n^2 \tag{5}$$

$$y = m^2 - n^2 \pm 2mn \tag{6}$$

と表されるとしてよい。

(3)を変形すると

$$b^2 - 4x^2 = (b+2x)(b-2x) = 5y^2 \tag{7}$$

$b+2x$ と $b-2x$ が共通の素因数 p をもつとすれば,

$$p|4x \text{ かつ } p^2|5y^2$$

が成り立つが, $p^2|5y^2$ より $p|y$ となって p は奇素数であり, $p|x$ かつ $p|y$ が成り立って互いに素であることに反するから,

$$b+2x \text{ と } b-2x \text{ は互いに素}$$

である。よって, (7)より

$$(b+2x, b-2x, y) = (5k^2, \ell^2, k\ell) \text{ または } (\ell^2, 5k^2, k\ell)$$

を満たす互いに素な正の奇数 k, ℓ が存在し,

$$4x = |5k^2 - \ell^2| \quad (8)$$

$$y = k\ell \quad (9)$$

(5), (6), (8), (9)をもとに,

$4x$ が $5k^2 - \ell^2$ であるか $\ell^2 - 5k^2$ であるか,

y が $m^2 - n^2 + 2mn$ であるか $m^2 - n^2 - 2mn$ であるか

によって 4 つに場合分け^{注4}して考えていくことにする。

Case 1

$$4x = 4(m^2 + n^2) = 5k^2 - \ell^2 \quad (10)$$

$$y = m^2 - n^2 + 2mn = k\ell \quad (11)$$

IA m が奇数のとき

(10) + (11) × 4 より

$$8m^2 + 8mn = 5k^2 + 4k\ell - \ell^2$$

$$2m(m+n) = \frac{k+\ell}{2} \cdot \frac{5k-\ell}{2}$$

$\gcd\left(m, \frac{k+\ell}{2}\right) = s$ とおくと, s は正の奇数であり,

$$m = st, \quad \frac{k+\ell}{2} = su \quad (12)$$

を満たす互いに素な自然数 t, u (t は奇数) が存在する。

$$2t(m+n) = u \cdot \frac{5k-\ell}{2}$$

より

$$2(m+n) = uv, \quad \frac{5k-\ell}{2} = tv \quad (13)$$

を満たす自然数 v が存在する。

$$su + tv = 3k$$

は奇数であるから, (s, t が奇数であることより)

$$u \not\equiv v \pmod{2} \quad (14)$$

(12), (13) より

$$m = st, \quad n = \frac{uv}{2} - st, \quad k = \frac{su+tv}{3}, \quad \ell = \frac{5su-tv}{3}$$

(10)に代入して

$$\begin{aligned} 4s^2t^2 + (uv - 2st)^2 &= \frac{5(su+tv)^2 - (5su-tv)^2}{9} \\ &= \frac{-20s^2u^2 + 20stuv + 4t^2v^2}{9} \end{aligned}$$

$$9\left(2s^2t^2 - stuv + \frac{u^2v^2}{4}\right) = -5s^2u^2 + 5stuv + t^2v^2$$

$$(18t^2 + 5u^2)s^2 - 14stuv + \frac{9u^2 - 4t^2}{4}v^2 = 0 \quad (15)$$

$$(18t^2 + 5u^2)\left(\frac{s}{v}\right)^2 - 14tu \cdot \frac{s}{v} + \frac{9u^2 - 4t^2}{4} = 0$$

2次方程式が有理数解 $\frac{s}{v}$ をもつから

$$\begin{aligned} \frac{1}{4}(\text{判別式}) &= 49t^2u^2 - (18t^2 + 5u^2)\frac{9u^2 - 4t^2}{4} \\ &= \frac{1}{4}\{(18t^2 + 5u^2)(4t^2 - 9u^2) + 196t^2u^2\} \\ &= \frac{1}{4}(72t^4 + 54t^2u^2 - 45u^2) \\ &= \frac{9}{4}(8t^4 + 6t^2u^2 - 5u^4) \end{aligned}$$

は有理数の平方であり、

$$8t^4 + 6t^2u^2 - 5u^4 = w^2$$

を満たす自然数 w が存在する。ここで、 u が奇数であるとすれば、(12)、(5) より

$$t \leq st = m \leq m^2 < m^2 + n^2 = x$$

となって、(1) が成り立つときの x の最小性に反するから、

u は偶数

である。すると、(14) より

v は奇数

である。このとき、(15) を書き直すと

$$\begin{aligned} \frac{20s^2 + 9v^2}{4}u^2 - 14stuv + (18s^2 - v^2)t^2 &= 0 \\ \frac{20s^2 + 9v^2}{4}\left(\frac{u}{t}\right)^2 - 14sv \cdot \frac{u}{t} + 18s^2 - v^2 &= 0 \end{aligned}$$

2次方程式が有理数解 $\frac{u}{t}$ をもつから

$$\begin{aligned} \frac{1}{4}(\text{判別式}) &= 49s^2v^2 - \frac{20s^2 + 9v^2}{4}(18s^2 - v^2) \\ &= \frac{1}{4}\{(20s^2 + 9v^2)(v^2 - 18s^2) + 196s^2v^2\} \\ &= \frac{1}{4}(9v^4 + 54s^2v^2 - 360s^4) \\ &= \frac{9}{4}(v^4 + 6s^2v^2 - 40s^4) \end{aligned}$$

は有理数の平方であり、

$$v^4 + 6s^2v^2 - 40s^4 = w^2$$

を満たす自然数 w が存在する。ところが、 s 、 v はともに奇数であるから

$$v^4 + 6s^2v^2 - 40s^4 \equiv 1 + 6 - 0 \equiv 7 \pmod{8}$$

となって $w^2 \equiv 0, 1, 4 \pmod{8}$ であることと矛盾する。

IB n が奇数のとき

(10) - (11) $\times 4$ より

$$\begin{aligned} 8n^2 - 8mn &= 5k^2 - 4kl - \ell^2 \\ 2n(n - m) &= \frac{5k + \ell}{2} \cdot \frac{k - \ell}{2} \end{aligned}$$

$\gcd\left(n, \frac{5k + \ell}{2}\right) = s$ とおくと, s は正の奇数であり,

$$n = st, \quad \frac{5k + \ell}{2} = su \tag{16}$$

を満たす互いに素な自然数 t, u (t は奇数) が存在する。

$$2t(n - m) = u \cdot \frac{k - \ell}{2}$$

より

$$2(n - m) = uv, \quad \frac{k - \ell}{2} = tv \tag{17}$$

を満たす 0 でない整数 v が存在する。

$$su + tv = 3k$$

は奇数であるから, (s, t が奇数であることより)

$$u \not\equiv v \pmod{2} \tag{18}$$

(16), (17) より

$$n = st, \quad m = st - \frac{uv}{2}, \quad k = \frac{su + tv}{3}, \quad \ell = \frac{su - 5tv}{3}$$

(10) に代入して

$$\begin{aligned} 4s^2t^2 + (2st - uv)^2 &= \frac{5(su + tv)^2 - (su - 5tv)^2}{9} \\ &= \frac{4s^2u^2 + 20stuv - 20t^2v^2}{9} \\ 9\left(2s^2t^2 - stuv + \frac{u^2v^2}{4}\right) &= s^2u^2 + 5stuv - 5t^2v^2 \\ \frac{20t^2 + 9u^2}{4}v^2 - 14stuv + (18t^2 - u^2)s^2 &= 0 \\ \frac{20t^2 + 9u^2}{4}\left(\frac{v}{s}\right)^2 - 14tu \cdot \frac{v}{s} + 18t^2 - u^2 &= 0 \end{aligned} \tag{19}$$

2 次方程式が有理数解 $\frac{v}{s}$ をもつから

$$\begin{aligned} \frac{1}{4}(\text{判別式}) &= 49t^2u^2 - \frac{20t^2 + 9u^2}{4}(18t^2 - u^2) \\ &= \frac{1}{4}\{(20t^2 + 9u^2)(u^2 - 18t^2) + 196t^2u^2\} \\ &= \frac{1}{4}(9u^4 + 54t^2u^2 - 360t^4) \end{aligned}$$

$$= \frac{9}{4}(u^4 + 6t^2u^2 - 40t^4)$$

は有理数の平方であり,

$$u^4 + 6t^2u^2 - 40t^4 = w^2$$

を満たす自然数 w が存在する。ここで, u が奇数であるとすれば

$$u^4 + 6t^2u^2 - 40t^4 \equiv 1 + 6 - 0 \equiv 7 \pmod{8}$$

となって $w^2 \equiv 0, 1, 4 \pmod{8}$ であることと矛盾するから,

u は偶数

である。すると, (18) より

v は奇数

である。このとき, (19) を書き直すと

$$(18s^2 + 5v^2)t^2 - 14stuv + \frac{9v^2 - 4s^2}{4}u^2 = 0$$

$$(18s^2 + 5v^2)\left(\frac{t}{u}\right)^2 - 14sv \cdot \frac{t}{u} + \frac{9v^2 - 4s^2}{4} = 0$$

2 次方程式が有理数解 $\frac{t}{u}$ をもつから

$$\begin{aligned} \frac{1}{4}(\text{判別式}) &= 49s^2v^2 - (18s^2 + 5v^2)\frac{9v^2 - 4s^2}{4} \\ &= \frac{1}{4}\{(18s^2 + 5v^2)(4s^2 - 9v^2) + 196s^2v^2\} \\ &= \frac{1}{4}(72s^4 + 54s^2v^2 - 45v^4) \\ &= \frac{9}{4}(8s^4 + 6s^2v^2 - 5v^4) \end{aligned}$$

は有理数の平方であり,

$$8s^4 + 6s^2v^2 - 5v^4 = w^2$$

を満たす自然数 w が存在する。いま v は奇数であるから, (16), (5) より

$$s \leq st = n \leq n^2 < m^2 + n^2 = x$$

となって, (1) が成り立つときの x の最小性に反する。

Case 2

$$4x = 4(m^2 + n^2) = \ell^2 - 5k^2 \tag{20}$$

$$y = m^2 - n^2 + 2mn = k\ell \tag{21}$$

II A m が奇数のとき

(20) + (21) $\times 4$ より

$$8m^2 + 8mn = \ell^2 + 4k\ell - 5k^2$$

$$2m(m+n) = \frac{\ell + 5k}{2} \cdot \frac{\ell - k}{2}$$

$\gcd\left(m, \frac{\ell+5k}{2}\right) = s$ とおくと, s は正の奇数であり,

$$m = st, \quad \frac{\ell+5k}{2} = su \quad (22)$$

を満たす互いに素な自然数 t, u (t は奇数) が存在する。

$$2t(m+n) = u \cdot \frac{\ell-k}{2}$$

より

$$2(m+n) = uv, \quad \frac{\ell-k}{2} = tv \quad (23)$$

を満たす自然数 v が存在する。

$$su - tv = 3k$$

は奇数であるから, (s, t が奇数であることより)

$$u \not\equiv v \pmod{2} \quad (24)$$

(22), (23) より

$$m = st, \quad n = \frac{uv}{2} - st, \quad k = \frac{su-tv}{3}, \quad \ell = \frac{su+5tv}{3}$$

(20) に代入して

$$\begin{aligned} 4s^2t^2 + (uv - 2st)^2 &= \frac{(su+5tv)^2 - 5(su-tv)^2}{9} \\ &= \frac{-4s^2u^2 + 20stuv + 20t^2v^2}{9} \\ 9\left(2s^2t^2 - stuv + \frac{u^2v^2}{4}\right) &= -s^2u^2 + 5stuv + 5t^2v^2 \\ (18t^2 + u^2)s^2 - 14stuv + \frac{9u^2 - 20t^2}{4}v^2 &= 0 \\ (18t^2 + u^2)\left(\frac{s}{v}\right)^2 - 14tu \cdot \frac{s}{v} + \frac{9u^2 - 20t^2}{4} &= 0 \end{aligned} \quad (25)$$

2次方程式が有理数解 $\frac{s}{v}$ をもつから

$$\begin{aligned} \frac{1}{4}(\text{判別式}) &= 49t^2u^2 - (18t^2 + u^2)\frac{9u^2 - 20t^2}{4} \\ &= \frac{1}{4}\{(18t^2 + u^2)(20t^2 - 9u^2) + 196t^2u^2\} \\ &= \frac{1}{4}(360t^4 + 54t^2u^2 - 9u^4) \\ &= \frac{9}{4}(40t^4 + 6t^2u^2 - u^4) \end{aligned}$$

は有理数の平方であり,

$$40t^4 + 6t^2u^2 - u^4 = w^2$$

を満たす自然数 w が存在する。ここで, u が奇数であるとすれば,

$$40t^4 + 6t^2u^2 - u^4 \equiv 0 + 6 - 1 \equiv 5 \pmod{8}$$

となつて $w^2 \equiv 0, 1, 4 \pmod{8}$ であることと矛盾するから,

u は偶数

である。すると, (24) より

v は奇数

である。このとき, (25) を書き直すと

$$\begin{aligned} \frac{4s^2 + 9v^2}{4}u^2 - 14stuv + (18s^2 - 5v^2)t^2 &= 0 \\ \frac{4s^2 + 9v^2}{4}\left(\frac{u}{t}\right)^2 - 14sv \cdot \frac{u}{t} + 18s^2 - 5v^2 &= 0 \end{aligned}$$

2 次方程式が有理数解 $\frac{u}{t}$ をもつから

$$\begin{aligned} \frac{1}{4}(\text{判別式}) &= 49s^2v^2 - \frac{4s^2 + 9v^2}{4}(18s^2 - 5v^2) \\ &= \frac{1}{4}\{(4s^2 + 9v^2)(5v^2 - 18s^2) + 196s^2v^2\} \\ &= \frac{1}{4}(45v^4 + 54s^2v^2 - 72s^4) \\ &= \frac{9}{4}(5v^4 + 6s^2v^2 - 8s^4) \end{aligned}$$

は有理数の平方であり,

$$5v^4 + 6s^2v^2 - 8s^4 = w^2$$

を満たす自然数 w が存在する。ところが, s, v はともに奇数であるから,

$$5v^4 + 6s^2v^2 - 8s^4 \equiv 5 + 6 - 0 \equiv 3 \pmod{8}$$

となつて $w^2 \equiv 0, 1, 4 \pmod{8}$ であることと矛盾する。

II B n が奇数のとき

(20) - (21) $\times 4$ より

$$\begin{aligned} 8n^2 - 8mn &= \ell^2 - 4k\ell - 5k^2 \\ 2n(n - m) &= \frac{\ell + k}{2} \cdot \frac{\ell - 5k}{2} \end{aligned}$$

$\gcd\left(n, \frac{\ell + k}{2}\right) = s$ とおくと, s は正の奇数であり,

$$n = st, \quad \frac{\ell + k}{2} = su \tag{26}$$

を満たす互いに素な自然数 t, u (t は奇数) が存在する。

$$2t(n - m) = u \cdot \frac{\ell - 5k}{2}$$

より

$$2(n - m) = uv, \quad \frac{\ell - 5k}{2} = tv \tag{27}$$

を満たす 0 でない整数 v が存在する。

$$su - tv = 3k$$

は奇数であるから , $(s, t$ が奇数であることより)

$$u \not\equiv v \pmod{2} \tag{28}$$

(26), (27) より

$$n = st, \quad m = st - \frac{uv}{2}, \quad k = \frac{su - tv}{3}, \quad \ell = \frac{5su + tv}{3}$$

(20)に代入して

$$\begin{aligned} 4s^2t^2 + (2st - uv)^2 &= \frac{(5su + tv)^2 - 5(su - tv)^2}{9} \\ &= \frac{20s^2u^2 + 20stuv - 4t^2v^2}{9} \\ 9\left(2s^2t^2 - stuv + \frac{u^2v^2}{4}\right) &= 5s^2u^2 + 5stuv - t^2v^2 \\ \frac{9u^2 + 4t^2}{4}v^2 - 14stuv + (18t^2 - 5u^2)s^2 &= 0 \\ \frac{9u^2 + 4t^2}{4}\left(\frac{v}{s}\right)^2 + 14tu \cdot \frac{v}{s} + 18t^2 - 5u^2 &= 0 \end{aligned} \tag{29}$$

2次方程式が有理数解 $\frac{v}{s}$ をもつから

$$\begin{aligned} \frac{1}{4}(\text{判別式}) &= 49t^2u^2 - \frac{9u^2 + 4t^2}{4}(18t^2 - 5u^2) \\ &= \frac{1}{4}\{(9u^2 + 4t^2)(5u^2 - 18t^2) + 196t^2u^2\} \\ &= \frac{1}{4}(45u^4 + 54t^2u^2 - 72t^4) \\ &= \frac{9}{4}(5u^4 + 6t^2u^2 - 8t^4) \end{aligned}$$

は有理数の平方であり ,

$$5u^4 + 6t^2u^2 - 8t^4 = w^2$$

を満たす自然数 w が存在する。ここで , u が奇数であるとすれば ,

$$5u^4 + 6t^2u^2 - 8t^4 \equiv 5 + 6 - 0 \equiv 3 \pmod{8}$$

となって $w^2 \equiv 0, 1, 4 \pmod{8}$ であることと矛盾するから ,

u は偶数

である。すると , (28) より

v は奇数

である。このとき , (29)を書き直すと

$$\begin{aligned} (18s^2 + v^2)t^2 - 14stuv + \frac{9v^2 - 20s^2}{4}u^2 &= 0 \\ (18s^2 + v^2)\left(\frac{t}{u}\right)^2 - 14sv \cdot \frac{t}{u} + \frac{9v^2 - 20s^2}{4} &= 0 \end{aligned}$$

2次方程式が有理数解 $\frac{t}{u}$ をもつから

$$\begin{aligned}
\frac{1}{4}(\text{判別式}) &= 49s^2v^2 - (18s^2 + v^2)\frac{9v^2 - 20s^2}{4} \\
&= \frac{1}{4}\{(18s^2 + v^2)(20s^2 - 9v^2) + 196s^2v^2\} \\
&= \frac{1}{4}(360s^4 + 54s^2v^2 - 9v^4) \\
&= \frac{9}{4}(40s^4 + 6s^2v^2 - v^4)
\end{aligned}$$

は有理数の平方であり,

$$40s^4 + 6s^2v^2 - v^4 = w^2$$

を満たす自然数 w が存在する。ところが, s, v はともに奇数であるから,

$$40s^4 + 6s^2v^2 - v^4 \equiv 0 + 6 - 1 \equiv 5 \pmod{8}$$

となって $w^2 \equiv 0, 1, 4 \pmod{8}$ であることと矛盾する。

Case 3

$$4x = 4(m^2 + n^2) = 5k^2 - \ell^2 \quad (30)$$

$$y = m^2 - n^2 - 2mn = k\ell \quad (31)$$

III A m が奇数のとき

(30) + (31) $\times 4$ より

$$8m^2 - 8mn = 5k^2 + 4k\ell - \ell^2$$

$$2m(m - n) = \frac{k + \ell}{2} \cdot \frac{5k - \ell}{2}$$

$\gcd\left(m, \frac{k + \ell}{2}\right) = s$ とおくと, s は正の奇数であり,

$$m = st, \quad \frac{k + \ell}{2} = su \quad (32)$$

を満たす互いに素な自然数 t, u (t は奇数) が存在する。

$$2t(m - n) = u \cdot \frac{5k - \ell}{2}$$

より

$$2(m - n) = uv, \quad \frac{5k - \ell}{2} = tv \quad (33)$$

を満たす 0 でない整数 v が存在する。

$$su + tv = 3k$$

は奇数であるから, (s, t が奇数であることより)

$$u \not\equiv v \pmod{2}$$

(32), (33) より

$$m = st, \quad n = st - \frac{uv}{2}, \quad k = \frac{su + tv}{3}, \quad \ell = \frac{5su - tv}{3}$$

(30) に代入して

$$4s^2t^2 + (2st - uv)^2 = \frac{5(su + tv)^2 - (5su - tv)^2}{9}$$

ここから先は，IAと全く同じ議論で矛盾が導かれる。

III B n が奇数のとき

(30) - (31) $\times 4$ より

$$\begin{aligned} 8n^2 + 8mn &= 5k^2 - 4kl - \ell^2 \\ 8n(n + m) &= \frac{5k + \ell}{2} \cdot \frac{k - \ell}{2} \end{aligned}$$

$\gcd\left(n, \frac{5k + \ell}{2}\right) = s$ とおくと， s は正の奇数であり，

$$n = st, \quad \frac{5k + \ell}{2} = su \tag{34}$$

を満たす互いに素な自然数 t, u (t は奇数) が存在する。

$$8t(n + m) = u \cdot \frac{k - \ell}{2}$$

より

$$2(n + m) = uv, \quad \frac{k - \ell}{2} = tv \tag{35}$$

を満たす自然数 v が存在する。

$$su + tv = 3k$$

は奇数であるから，(s, t が奇数であることより)

$$u \not\equiv v \pmod{2}$$

(34), (35) より

$$n = st, \quad m = \frac{uv}{2} - st, \quad k = \frac{su + tv}{3}, \quad \ell = \frac{su - 5tv}{3}$$

(30)に代入して

$$4s^2t^2 + (uv - 2st)^2 = \frac{5(su + tv)^2 - (su - 5tv)^2}{9}$$

ここから先は，IBと全く同じ議論で矛盾が導かれる。

Case 4

$$4x = 4(m^2 + n^2) = \ell^2 - 5k^2 \tag{36}$$

$$y = m^2 - n^2 - 2mn = k\ell \tag{37}$$

IV A m が奇数のとき

(36) + (37) $\times 4$ より

$$\begin{aligned} 8m^2 - 8mn &= \ell^2 + 4k\ell - 5k^2 \\ 2m(m - n) &= \frac{\ell + 5k}{2} \cdot \frac{\ell - k}{2} \end{aligned}$$

$$\gcd\left(m, \frac{\ell + 5k}{2}\right) = s \text{ とおくと, } s \text{ は正の奇数であり,}$$

$$m = st, \quad \frac{\ell + 5k}{2} = su \tag{38}$$

を満たす互いに素な自然数 t, u (t は奇数) が存在する。

$$2t(m - n) = u \cdot \frac{\ell - k}{2}$$

より

$$2(m - n) = uv, \quad \frac{\ell - k}{2} = tv \tag{39}$$

を満たす 0 でない整数 v が存在する。

$$su - tv = 3k$$

は奇数であるから, (s, t が奇数であることより)

$$u \not\equiv v \pmod{2}$$

(38), (39) より

$$m = st, \quad n = st - \frac{uv}{2}, \quad k = \frac{su - tv}{3}, \quad \ell = \frac{su + 5tv}{3}$$

(36) に代入して

$$4s^2t^2 + (2st - uv)^2 = \frac{(su + 5tv)^2 - 5(su - tv)^2}{9}$$

ここから先は, ΠA と全く同じ議論で矛盾が導かれる。

IV B n が奇数のとき

(36) - (37) $\times 4$ より

$$8n^2 + 8mn = \ell^2 - 4k\ell - 5k^2$$

$$2n(n + m) = \frac{\ell + k}{2} \cdot \frac{\ell - 5k}{2}$$

$$\gcd\left(n, \frac{\ell + k}{2}\right) = s \text{ とおくと, } s \text{ は正の奇数であり,}$$

$$n = st, \quad \frac{\ell + k}{2} = su \tag{40}$$

を満たす互いに素な自然数 t, u (t は奇数) が存在する。

$$2t(n + m) = u \cdot \frac{\ell - 5k}{2}$$

より

$$2(n + m) = uv, \quad \frac{\ell - 5k}{2} = tv \tag{41}$$

を満たす自然数 v が存在する。

$$su - tv = 3k$$

は奇数であるから, (s, t が奇数であることより)

$$u \not\equiv v \pmod{2}$$

(40), (41) より

$$n = st, \quad m = \frac{uv}{2} - st, \quad k = \frac{su - tv}{3}, \quad \ell = \frac{5su + tv}{3}$$

(36)に代入して

$$4s^2t^2 + (uv - 2st)^2 = \frac{(5su + tv)^2 - 5(su - tv)^2}{9}$$

ここから先は，II Bと全く同じ議論で矛盾が導かれる。

以上によりすべての場合が尽くされ，定理が証明された。 ■

注1 もちろん，解き方によっては現れない可能性もある。しかし，ディオファントス方程式 $x^4 + 12x^2y^2 + y^4 = z^2$ に関連することだけに意味があるのではなく，この定理自体の意味合いや証明の手法の中にも独自の興味深さが感じられる。

注2 y が偶数のときは， $2^3 \mid z^2$ より z は 4 で割れ，

$$y = 2u, \quad z = 4v \quad (u, v \text{ は自然数})$$

と表すことができるから，本稿の方程式は

$$x^4 + 3x^2u^2 - 10u^4 = 2v^2$$

と姿を変えてしまう。 y が奇数ならば，必然的に z も奇数となる。

注3 互いに素な自然数 x, y, z がピタゴラス方程式

$$x^2 + y^2 = z^2$$

を満たすとき，

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2$$

または

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2$$

であるような偶奇が異なる互いに素な自然数 m, n が存在する。

証明は読者に委ねるが，必要ならば [1] pp.20 - 22 などを参照されるとよい。

注4 4つの場合というには，あくまでも (8)における絶対値のはずれ方と (6)における複号の選び方によるものである。既に m と n の対称性は盛り込まれているので，各場合において m が奇数か n が奇数かで場合を分ける必要があり，さらに途中で出てくる偶奇の異なる u, v についての場合分けも行なうので，実際には 16 通りに場合分けして考察する。ただし， u, v の場合分けについては，[4]と同様のアイデアによりひとまとめに考えることができ，また，後半は前半と同じ議論の繰り返しとなるので，実質的にはかなり少ない労力で済むことになる。

参考文献

- [1] 足立恒雄, フェルマーの大定理, 筑摩書房 (2006).
- [2] 大塚美紀生, 方程式 $(5x^2 - 4y^2)(5y^2 - 4x^2) = z^2$ の整数解,
早稲田数学フォーラム (2020),
[http://wasmath.la.coocan.jp/\(5x2-4y2\)\(5y2-4x2\)=z2.pdf](http://wasmath.la.coocan.jp/(5x2-4y2)(5y2-4x2)=z2.pdf)
- [3] 大塚美紀生, ディオファントス方程式 $x^4 + 8x^2y^2 + y^4 = z^2$ の原始解,
早稲田数学フォーラム (2021),
<http://wasmath.la.coocan.jp/x4+8x2y2+y4=z2-prim.pdf>
- [4] 大塚美紀生, 方程式 $x^4 + 7x^2y^2 + y^4 = z^2$ 再論,
早稲田数学フォーラム (2022),
<http://wasmath.la.coocan.jp/9x4-2x2y2+9y4=z2.pdf>