P-6

ディオファントス方程式の整数解について
Integer solutions of Diophantine equations

○善養寺 未来
Miku Zenyouji [1]

Abstract: We discuss integer solutions of Diophantine equations. We prove that the equation $x^2+y^2=z^2$ has infinitely many solutions of specific form in integers. We also show how to use infinite descent method to deal with equations of higher degree.

定義
3 つの正の整数の組 $(x,\ y,\ z)$ が $x^2+y^2=z^2$ を満たすとき $(x,\ y,\ z)$ をピタゴラス数という. 特に $(x,\ y)=1$ のときこれを原始ピタゴラス数という.

Lemma 1
$u,\ v$ を互いに素である正の整数とする. このとき uv が平方数ならば, u と v もまた平方数である.

Lemma 1 の証明
p を u のある素因数とし, α をその最大指数とする. 今 u と v は互いに素であるから $p\nmid v$ である. また $p^\alpha|u$ であるから, $p^\alpha|uv$ である. 今 uv は平方数であるから α は偶数である. これが u のすべての素因数について成り立つから u は平方数である. u が平方数であり, かつ uv が平方数であるから v も平方数である. □

Lemma 2
$x,\ y,\ z$ は正の整数で

$$x^2+y^2=z^2,\quad (x,\ y)=1$$

を満たすとする. このとき x と y の偶奇は異なり z は奇数である.

Lemma 2 の証明
$(x,\ y)=1$ より x と y が共に偶数であることはない. x と y を共に奇数であると仮定すると

$$x^2\equiv 1\ (\mathrm{mod}\ 4),\quad y^2\equiv 1\ (\mathrm{mod}\ 4)$$

であるから

$$z^2=x^2+y^2\equiv 2\ (\mathrm{mod}\ 4)$$

であるがこれは起こりえない. よって x と y の偶奇は異なる. これより

$$z^2=x^2+y^2\equiv 1\ (\mathrm{mod}\ 2)$$

である. 以上より z は奇数である. □

Theorem 1
ディオファントス方程式

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

を満たす

$$x,\ y,\ z\ \text{正の整数},\ 2\mid y,\ (x,\ y)=1$$

の一般解は,

$$x=r^2-s^2,\ y=2rs,\ z=r^2+s^2$$

である. ここで $r,\ s$ は偶奇が異なる整数で

$$(r,\ s)=1,\ r>s>0$$

を満たすものを動く. $r,\ s$ の異なる値と $x,\ y,\ z$ の異なる値の間には一対一対応がある.

Theorem 1 の証明
$2\mid y$ かつ $(x,\ y)=1$ であるから x は奇数である. よって $z^2=x^2+y^2$ は奇数であるから z も奇数である. したがって $z-x$ と $z+x$ は偶数である. 故に

$$\frac{z+x}{2}\frac{z-x}{2}=\left(\frac{y}{2}\right)^2\qquad \left(\frac{z+x}{2},\ \frac{z-x}{2}\in\mathbb{Z}_{>0}\right)$$

ここで $\left(\dfrac{z+x}{2},\ \dfrac{z-x}{2}\right)=d\ (d>1)$ とすると, $d\mid z$ かつ $d\mid x$ となるから x と y は公約数 $d>1$ をもつ. これより $d^2\mid z^2-x^2=y^2$ であるから $d\mid y$ である. これは $(x,\ y)=1$ であることに矛盾する. したがって $\left(\dfrac{z+x}{2},\ \dfrac{z-x}{2}\right)=1$ である. よって Lemma 1 より $\dfrac{z+x}{2}$ と $\dfrac{z-x}{2}$ は平方数である. よって

$$\frac{z+x}{2}=r^2,\ \frac{z-x}{2}=s^2$$

と表せる. ただし $r>s>0,\ (r,\ s)=1$ である.

1: 日大理工・院 (前)・数学

また

$$r+s \equiv r^2+s^2 = z \equiv 1 \pmod 2$$

であるから r と s の偶奇は異なる.
故に, $x>0,\ y>0,\ z>0,\ (x,\ y)=1,\ 2 \mid y$ を満たす $x^2+y^2=z^2$ の任意の解は

$$x=r^2-s^2,\ y=2rs,\ z=r^2+s^2$$

の形をしており, r と s は偶奇が異なり, $(r,\ s)=1,\ r>s>0$ を満たす.
次に r と s は偶奇が異なり, $(r,\ s)=1,\ r>s>0$ を満たすとする. このとき

$$x^2+y^2=(r^2-s^2)^2+(2rs)^2=(r^2+s^2)^2=z^2$$

$$x=r^2-s^2>0,\ 2 \mid y,\ y=2rs>0,\ z=r^2+s^2>0$$

である. $(x,\ y)=d\quad (d \geq 1)$ とすると, $d \mid z$ であり,

$$d \mid x=r^2-s^2,\ d \mid z=r^2+s^2$$

したがって $d \mid 2r^2,\ d \mid 2s^2$ となる. 今 $(r,\ s)=1$ であるから $d=1$ または $d=2$ である. しかし x は奇数であるから $d=2$ は起こりえない. したがって $(x,\ y)=1$ である.
ここで $(r,\ s)$ の異なる値の組に対して, (x,y,z) の異なる値の組が対応することがわかる. また x と z が与えられれば r と s は $r=\dfrac{x+y}{2},\ s=\dfrac{-x+y}{2}$ より一意的に定まる. したがって $r,\ s$ の異なる値と $x,\ y,\ z$ の異なる値の間には一対一対応がある. □

Theorem 2
ディオファントス方程式

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

を満たす正の整数 $x,\ y,\ z$ は存在しない.

Theorem 2 の証明
$x,\ y,\ z$ を $x^4+y^4=z^2$ を満たす任意の正の整数とする. $g=\gcd(x,\ y)$ とすると g^4 は (1) の左辺を割り切る. よって $g^4 \mid z^2$ であるから $g^2 \mid z$ である.

$$x_1=\frac{x}{g},\quad y_1=\frac{y}{g},\quad z_1=\frac{z}{g^2}$$

とすると, $x_1,\ y_1,\ z_1$ は (1) を満たす正の整数であり $(x_1,\ y_1)=1$ であるから Lemma 2 より x_1^2 と y_1^2 の偶奇は異なり, z_1 は奇数である. よって x_1^2 を奇数とすると Theorem 1 より

$$x_1^2 = r^2-s^2 \tag{2}$$
$$y_1^2 = 2rs \tag{3}$$
$$z_1 = r^2+s^2 \tag{4}$$

$$r>0,\ s>0,\ (r,\ s)=1$$

を満たす $r,\ s \in \mathbb{Z}$ が存在する. r と s は偶奇が異なるが, r を偶数とすると

$$x^2=r^2-s^2 \equiv -1 \pmod 4$$

となるがこれは起こりえない. したがって r は奇数, s は偶数である. $(r,\ 2s)=1$ であるから Lemma 1 と (3) より r と $2s$ は平方数である. したがって正の整数 b, c が存在して $r=c^2,\ s=2b^2$ と表せる. ここで $a=x_1$ とすると (2) より

$$a^2+4b^4=c^4 \tag{5}$$

を満たす正の整数である. さらに (4) より

$$c \leq c^4=r^2<r^2+s^2=z_1 \leq z \tag{6}$$

である. $h=\gcd(b,\ c)$ とすると $h^4 \mid a^2$ であるから $h^2 \mid a$ である. ここで $a_1=\dfrac{a}{h^2},\ b_1=\dfrac{b}{h},\ c_1=\dfrac{c}{h}$ とおくと $a_1,\ b_1,\ c_1$ は $a_1^2+4b_1^4=c_1^4$ を満たす正の整数であり, $(b_1,\ c_1)=1$ である. したがって Theorem 1 より

$$a_1^2 = r'^2-s'^2 \tag{7}$$
$$b_1^2 = r's' \tag{8}$$
$$c_1^2 = r'^2+s'^2 \tag{9}$$

$$r'>0,\ s'>0,\ (r',\ s')=1$$

を満たす $r',\ s' \in \mathbb{Z}$ が存在する. Lemma 1 より r' と s' は平方数であるので正の整数 x', y' が存在して $r'=x'^2,\ s'=y'^2$ と表せる. $z'=c_1$ とすると (9) より $x',\ y',\ z'$ は (1) を満たす正の整数である. $z' \leq c$ と (6) から $z'<z$ である. よって (1) を満たす正の整数 z が存在したとすると (1) を満たすより小さな解 z' が存在した. これは任意の空でない正の整数の集合が最小元をもつことに矛盾する. 以上より (1) を満たす正の整数解は存在しない. □

1. 参考文献

[1] I. Niven, H. S. Zuckerman and H. L. Montgomery *An Introduction to the Theory of Numbers*, Wiley, First edition 1960, Fifth edition, 1991.

[2] T. Nagell, *Introduction to number theory*, AMS Chelsea, First edition, 1964, Second Edition, 2001.

[3] G. H. ハーディ, E. M. ライト, 数論入門 I, 丸善出版, 2012.

[4] H. Cohen, *Number Theory Volume I:Tools and Diophantine Equations*, GTM 297, Springer, 2007.