合同数

MATHEMATICS.PDF

平成 18 年 11 月 14 日

目 次

1 $x^2+y^2=z^2$ の整数解

この節では, 方程式

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

の正の整数解 (x,y,z) であって, 条件

$$x>0,\ y>0,\ z>0 \tag{2}$$

を満たすものを, 2 つの変数 r, s によってパラメータ表示することを目標とする.

ちなみに, $z=0$ であるとき, (x,y,z) が (1) を満たすならば $x=y=0$ である. $x=0$ または $y=0$ のとき, 任意の $t\in\mathbb{Z}$ に対して $(0,\pm t,\pm t)$, $(\pm t,0,\pm t)$ が (1) の解である. これらは (1) の自明な解と呼ばれる. さらに, (x,y,z) が (1) の解ならば, $(\pm x,\pm y,\pm z)$ もまた (1) の解である. したがって, 条件 (2) を満たすような整数解 (x,y,z) について考えることが本質的である.

もし $d=\gcd(x,y,z)>0$ ならば,

$$\left(\frac{x}{d},\frac{y}{d},\frac{z}{d}\right),\quad \gcd\left(\frac{x}{d},\frac{y}{d},\frac{z}{d}\right)=1$$

もまた (1) の整数解である. よって

$$\gcd(x,y,z)=1 \tag{3}$$

と仮定してもよい.

補題 1.1. (x, y, z) が (1) の整数解であるとき, (3) が成り立つことと,

$$\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1 \tag{4}$$

が成り立つこととは同値である.

証明. $d = \gcd(x, y, z) > 1$ と仮定すると, $\gcd(x, y) \geq d > 1$ である. $\gcd(x, z)$ や $\gcd(y, z)$ についても同様である. したがって (4) が成り立てば, (3) が成り立つ.

$d_1 = \gcd(x, y) > 1$ と仮定すると,

$$z^2 = d_1^2 \left(\left(\frac{x}{d_1} \right)^2 + \left(\frac{y}{d_1} \right)^2 \right)$$

なので, $d_1^2 \mid z^2$, したがって $d_1 \mid z$ である. よって $\gcd(x, y, z) \geq d_1 > 1$ である.

また, $d_2 = \gcd(x, z) > 1$ と仮定すると,

$$y^2 = d_2^2 \left(\left(\frac{z}{d_2} \right)^2 - \left(\frac{x}{d_2} \right)^2 \right)$$

なので, $d_2^2 \mid y^2$, したがって $d_2 \mid y$ である. よって $\gcd(x, y, z) \geq d_2 > 1$ である. $\gcd(y, z) > 1$ を仮定したときにも同様にして $\gcd(x, y, z) > 1$ がいえる. したがって (3) が成り立てば, (4) が成り立つ. □

注意 1.2. 整数 x, y, z について, $\gcd(x, y) = 1$, $\gcd(x, z) = 1$, $\gcd(y, z) = 1$ のいずれか一つでも成り立てば, (3) が成り立つ.

しかしながら, (3) が成り立っても一般には (4) は成立しない. $x = 2$, $y = 3$, $z = 6$ が反例の一つである.

補題 1.3. (x, y, z) が (3) を満たすような (1) の整数解であるとする. このとき, $x \not\equiv y \pmod 2$, すなわち, x と y が共に偶数あるいは共に奇数になることはない.

証明. $\gcd(x, y, z) = 1$ ならば, $\gcd(x, y) = 1$ なので, x と y が共に偶数になることはない. また, もし仮に x と y が共に奇数ならば, $x^2 \equiv y^2 \equiv 1 \pmod 4$ なので,

$$z^2 = x^2 + y^2 \equiv 2 \pmod 4.$$

一方, z は偶数なので,

$$z^2 \equiv 0 \pmod 4.$$

これは矛盾である. よって x と y が共に奇数になることはない. □

x と y のどちらが偶数であっても本質的な違いはない. ただ, いずれにせよ z は奇数である. そこで

$$x \equiv z \equiv 1 \pmod 2, \quad y \equiv 0 \pmod 2 \tag{5}$$

と仮定する.

(4), (5) より,

$$\frac{z+x}{2}, \frac{z-x}{2} \in \mathbb{Z}, \quad \gcd\left(\frac{z+x}{2}, \frac{z-x}{2} \right)$$

が成り立つ. (1) より

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

で, 2 つの因子は互いに素だから, 2 つとも平方数でなければならない. よって, ある r, $s \in \mathbb{Z}$ が存在して

$$r^2 = \frac{z+x}{2}, \quad s^2 = \frac{z-x}{2}, \tag{6}$$

$$r > s > 0, \quad \gcd(r, s) = 1 \tag{7}$$

が成り立つ. (6) より,

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

再び (6) より,

$$4r^2s^2 = (z+x)(z-x) = z^2 - x^2 = y^2.$$

$r > s > 0$, $y > 0$ より

$$y = 2rs.$$

よって

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

$z > 0$ だから,

$$z = r^2 + s^2.$$

次に, $r \equiv r^2$, $s \equiv s^2 \pmod 2$ だから,

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

よって

$$r \not\equiv s \pmod 2.$$

すなわち, r と s の偶奇は異なる.

最後に,

$$x = r_1^2 - s_1^2 = r_2^2 - s_2^2, \tag{8}$$

$$y = 2r_1s_1 = 2r_2s_2, \tag{9}$$

$$z = r_1^2 + s_1^2 = r_2^2 + s_2^2 \tag{10}$$

とすると, (8), (10) より $r_1^2 = r_2^2$, $s_1^2 = s_2^2$ が得られる. r_1, r_2, s_1, s_2 がすべて正ならば, $r_1 = r_2$, $s_1 = s_2$ となる.

以上より, (1) の正の整数解 (x, y, z) のパラメータ表示が得られた.

定理 1.4. 方程式 (1) の整数解 (x, y, z) が. 条件

$$x > 0, \quad y > 0, \quad z > 0, \tag{11}$$

$$\gcd(x, y, z) = 1, \tag{12}$$

$$x \equiv z \equiv 1, \quad y \equiv 0 \pmod 2 \tag{13}$$

を満たすとき, ある r, $s \in \mathbb{Z}$ が存在して

$$x = r^2 - s^2, \quad y = 2rs, \quad z = r^2 + s^2, \tag{14}$$

$$r > s > 0, \tag{15}$$

$$\gcd(r, s) = 1, \tag{16}$$

$$r \not\equiv s \pmod 2 \tag{17}$$

が成り立つ. さらに, (11), (12), (13) を満たす整数解 (x, y, z) に対して, (14), (15), (16), (17) を満たす整数 r, s の組が一意的に定まる.

定理 1.4 の逆も成り立つ.

定理 1.5. 定理 1.4 の条件 (15), (16), (17) を満たす任意の整数 r, s に対して,

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

とおく. このとき, (x, y, z) は方程式 (1) の整数解であって, 定理 1.4 の条件 (11), (12), (13) を満たす.

証明. $r > s > 0$ なので, $x > 0$, $y > 0$, $z > 0$ である. また,

$$x^2 + y^2 = (r^2 - s^2)^2 - 4r^2s^2 = (r^2 + s^2)^2 = z^2. \tag{18}$$

$r \not\equiv s \pmod 2$ なので, x は奇数. 一方, y の定め方から y は偶数. よって $x \not\equiv y \pmod 2$.

$d = \gcd(x, y, z)$ とおくと,

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

$\gcd(r, s) = 1$ より, $d \mid 2$. よって $d = 1$ または $d = 2$. x は奇数なので, $d = 1$ でなければならない. □

2　3 辺が整数である直角三角形の面積は平方数にならない

定理 2.1. 直角三角形の 3 辺が整数のとき, その面積は平方数にならない.

証明. 面積が平方数であるような直角三角形が存在するならば, そのうちで面積において最小のものが存在する. そのような直角三角形の 3 辺を a, b, c とし, 面積を $S = k^2$ とする. このとき

$$k^2 = \frac{ab}{2}$$

が成り立つ.

a, b, c は 2 つずつ互いに素である. なぜなら, a, b が公約数 $d > 1$ をもつとすると, a/d, b/d, c/d を 3 辺とする直角三角形は $(k/d)^2$ の面積をもち, k^2 の最小性に反する. それ以外の場合についても同様である.

そこで a を奇数, b を偶数とすると, ある正の整数 r, s によって

$$a = r^2 - s^2, \quad b = 2rs$$

と書ける．したがって

$$k^2 = rs(r-s)(r+s)$$

となる．r, s, $r+s$, $r-s$ は 2 つずつ互いに素であるから, それぞれ平方数になる．よって, ある正の整数 r_1, s_1, t, u によって

$$r = r_1^2, \quad s = s_1^2, \quad r+s = t^2, \quad r-s = u^2$$

と書ける．

$$(t-u)(t+u) = t^2 - u^2 = 2s = 2s_1^2$$

であるから, $t-u$, $t+u$ の少なくとも一方は偶数である．$(t-u)+2u = t+u$ だから, 一方が偶数ならもう一方も偶数である．よって両方とも偶数である．

$t-u$, $t+u$ の最大公約数 g は, $t-u$, $t+u$ の和 $2t$ と差 $2u$ の両方を割る．t, u は互いに素だから, g の素因子は 2 を割らなければならない．よって, $t-u$, $t+u$ の最大公約数は 2 のベキである．

したがって, $t-u$, $t+u$ のうち, 一方が平方数かつ偶数で, もう一方が平方数の 2 倍である．すなわち, ある正の整数 v, w が存在して

$$\begin{cases} t+u = 2v^2 \\ t-u = 4w^2 \end{cases} \quad \text{または} \quad \begin{cases} t+u = 4w^2 \\ t-u = 2v^2 \end{cases}$$

と書ける．これより

$$\begin{cases} t = v^2 + 2w^2 \\ u = v^2 - 2w^2 \end{cases} \quad \text{または} \quad \begin{cases} t = v^2 + 2w^2 \\ u = -(v^2 - 2w^2) \end{cases}$$

となる．このとき

$$r_1^2 = r = \frac{t^2+u^2}{2} = (v^2)^2 + (2w^2)^2.$$

したがって, v^2, $2w^2$, r_1 がある直角三角形の 3 辺の長さとなり, その面積 S' は

$$S' = \frac{v^2 \cdot 2w^2}{2} = (vw)^2$$

で与えられる．しかも,

$$s = \frac{(t-u)(t+u)}{2} = 4v^2w^2$$

であるから,

$$S' < s < S$$

である．これは S の最小性に反する． □

定理 2.1 の証明を少し修正すると, 平方数の 2 倍についても証明できる．

定理 2.2. 直角三角形の 3 辺が整数のとき, その面積は平方数の 2 倍にならない．

証明. 面積が平方数の 2 倍であるような直角三角形が存在するならば, そのうちで面積において最小のものが存在する．そのような直角三角形の 3 辺を a, b, c とし, 面積を $S = 2k^2$ とする．このとき

$$2k^2 = \frac{ab}{2}$$

が成り立つ．

a, b, c は 2 つずつ互いに素である．なぜなら, a, b が公約数 $d > 1$ をもつとすると, a/d, b/d, c/d を 3 辺とする直角三角形は $(k/d)^2$ の面積をもち, k^2 の最小性に反する．それ以外の場合についても同様である．

そこで a を奇数, b を偶数とすると, ある正の整数 r, s によって

$$a = r^2 - s^2, \quad b = 2rs$$

と書ける．したがって

$$2k^2 = rs(r-s)(r+s)$$

となる．

(i)　r が奇数, s が偶数のとき, r, $s/2$, $r+s$, $r-s$ は 2 つずつ互いに素であるから, それぞれ平方数になる．よって, ある正の整数 r_1, s_1, t, u によって

$$r = r_1^2, \quad s = 2s_1^2, \quad r+s = t^2, \quad r-s = u^2$$

と書ける．

$$(t-u)(t+u) = t^2 - u^2 = 2s = 4s_1^2$$

であるから, $t-u$, $t+u$ の少なくとも一方は偶数である．$(t-u)+2u = t+u$ だから, 一方が偶数ならもう一方も偶数である．よって両方とも偶数である．

$t-u$, $t+u$ の最大公約数 g は, $t-u$, $t+u$ の和 $2t$ と差 $2u$ の両方を割る．t, u は互いに素だから, g の素因子は 2 を割らなければならない．よって, $t-u$, $t+u$ の最大公約数は 2 のベキである．

したがって, $t-u$, $t+u$ は, 両方とも平方数かつ偶数か, 両方とも平方数の 2 倍である．すなわち, ある正の整数 v, w が存在して

$$\begin{cases} t+u = 4v^2 \\ t-u = 4w^2 \end{cases} \quad \text{または} \quad \begin{cases} t+u = 2v^2 \\ t-u = 2w^2 \end{cases}$$

と書ける．これより

$$\begin{cases} t = 2(v^2+w^2) \\ u = 2(v^2-w^2) \end{cases} \quad \text{または} \quad \begin{cases} t = v^2+w^2 \\ u = v^2-w^2 \end{cases}$$

となる．ところが前者の場合, $t = 2(v^2+w^2)$ であることが, t が奇数であることに反する．後者の場合,

$$r_1^2 = r = \frac{t^2+u^2}{2} = (v^2)^2 + (w^2)^2.$$

したがって, v^2, w^2, r_1 がある直角三角形の 3 辺の長さとなり, その面積 S' は

$$S' = \frac{v^2w^2}{2} = \frac{(vw)^2}{2}$$

で与えられる．$t = v^2+w^2$ は奇数なので, v, w の一方は偶数である．よって vw は偶数であり, S' は平方数の 2 倍になっている．しかも,

$$s = \frac{(t-u)(t+u)}{2} = v^2w^2$$

であるから,

$$S' < s < S$$

である．これは S の最小性に反する．

(ii)　r が偶数, s が奇数のとき, $r/2$, s, $r+s$, $r-s$ は 2 つずつ互いに素であるから, それぞれ平方数になる．よって, ある正の整数 r_1, s_1, t, u によって

$$r = 2r_1^2, \quad s = s_1^2, \quad r+s = t^2, \quad r-s = u^2$$

と書ける．

$$(t-u)(t+u) = t^2 - u^2 = 2s = 2s_1^2$$

であるから, $t-u$, $t+u$ の少なくとも一方は偶数である．$(t-u)+2u = t+u$ だから, 一方が偶数ならもう一方も偶数である．よって両方とも偶数である．

$t-u$, $t+u$ の最大公約数 g は, $t-u$, $t+u$ の和 $2t$ と差 $2u$ の両方を割る．t, u は互いに素だから, g の素因子は 2 を割らなければならない．よって, $t-u$, $t+u$ の最大公約数は 2 のベキである．

したがって, $t-u$, $t+u$ のうち, 一方が平方数かつ偶数で, もう一方が平方数の 2 倍である．すなわち, ある正の整数 v, w が存在して

$$\begin{cases} t+u = 2v^2 \\ t-u = 4w^2 \end{cases} \quad \text{または} \quad \begin{cases} t+u = 4w^2 \\ t-u = 2v^2 \end{cases}$$

と書ける．これより

$$\begin{cases} t = v^2 + 2w^2 \\ u = v^2 - 2w^2 \end{cases} \quad \text{または} \quad \begin{cases} t = v^2 + 2w^2 \\ u = -(v^2 - 2w^2) \end{cases}$$

となる．このとき

$$r_1^2 = \frac{r}{2} = t^2 + u^2 = 2\big((v^2)^2 + (2w^2)^2\big).$$

t は奇数なので, v も奇数である．よって, 上式の右辺は 4 を法として 2 と合同である．これは矛盾である．　□

3　合同数

合同数とは, 3 辺の長さが全て有理数であるような直角三角形の面積となるような正の整数のことである．すなわち, 正の整数 n が合同数であるとは, ある a, b, $c \in \mathbb{Q}$ が存在して

$$a^2 + b^2 = c^2, \quad n = \frac{ab}{2} \tag{19}$$

であることをいう．

例 1. 5 は合同数である．実際, $a = 9$, $b = 40$, $c = 41$ とすると, $a^2 + b^2 = c^2$, $ab/2 = 5$ である．

例 2. 6 は合同数である．実際, $a = 3$, $b = 4$, $c = 5$ とすると, $a^2 + b^2 = c^2$, $ab/2 = 6$ である．

例 3. 7 は合同数である．実際, $a = 35/12$, $b = 24/5$, $c = 337/60$ とすると, $a^2 + b^2 = c^2$, $ab/2 = 7$ である．

例 4. 100 以下の合同数は 36 個ある．それらは 5, 6, 7, 13, 14, 15, 21, 22, 23, 29, 30, 31, 34, 37, 38, 39, 41, 46, 47, 53, 55, 61, 62, 65, 69, 70, 71, 77, 78, 79, 85, 86, 87, 93, 94, 95 である．

定理 3.1. 任意の正の整数 n と整数 k に対して, n が合同数であることと nk^2 が合同数であることは同値である．

証明. n が合同数ならば, ある a, b, $c \in \mathbb{Q}$ が存在して

$$a^2 + b^2 = c^2, \quad n = \frac{ab}{2}$$

が成り立つ. このとき,

$$(ak)^2 + (bk)^2 = (ck)^2, \quad nk^2 = \frac{(ak)(bk)}{2}$$

が成り立つ. したがって nk^2 は合同数である.

逆に, nk^2 が合同数ならば, ある a, b, $c \in \mathbb{Q}$ が存在して

$$a^2 + b^2 = c^2, \quad nk^2 = \frac{ab}{2}$$

が成り立つ. このとき,

$$\left(\frac{a}{k}\right)^2 + \left(\frac{b}{k}\right)^2 = \left(\frac{c}{k}\right)^2, \quad n = \frac{1}{2}\left(\frac{a}{k}\right)\left(\frac{b}{k}\right)$$

が成り立つ. したがって nk^2 は合同数である.

□

定理 3.2. 正の整数 n が合同数であるための必要十分条件は, ある k, a, b, $c \in \mathbb{Z}$ が存在して

$$a^2 + b^2 = c^2, \quad nk^2 = \frac{ab}{2} \tag{20}$$

となることである.

証明. 正の整数 n が合同数のとき, ある k, a, b, $c \in \mathbb{Z}$ が存在して (20) が成り立つことをいえば十分である.

a, b, c を (19) を満たすような有理数とする. k として, a, b, c の分母の最小公倍数をとり, $a_1 = ak$, $b_1 = bk$, $c_1 = ck$ とすれば, a_1, b_1, $c_1 \in \mathbb{Z}$ であり,

$$\begin{aligned} a^2 + b^2 = c^2 &\Longleftrightarrow a^2k^2 + b^2k^2 = c^2k^2 \\ &\Longleftrightarrow a_1^2 + b_1^2 = c_1^2. \end{aligned}$$

さらに,

$$nk^2 = \frac{abk^2}{2} = \frac{a_1 b_1}{2}$$

が成り立つ. □

例 5. 1 は合同数ではない. なぜなら, 3 辺が整数で面積が平方数であるような直角三角形は存在しない（定理 2.1）からである.

例 6. 2 は合同数ではない. なぜなら, 3 辺が整数で面積が平方数の 2 倍であるような直角三角形は存在しない（定理 2.2）からである.

§1 で述べたように, 整数 a, b, c が

$$a^2 + b^2 = c^2 \tag{21}$$

$$a > 0, \quad b > 0, \quad c > 0, \tag{22}$$

$$\gcd(a, b, c) = 1, \tag{23}$$

$$a \equiv c \equiv 1, \quad b \equiv 0 \pmod 2 \tag{24}$$

を満たすとき, ある r, $s \in \mathbb{Z}$ が存在して

$$a = r^2 - s^2, \quad b = 2rs, \quad c = r^2 + s^2, \tag{25}$$

$$r > s > 0, \tag{26}$$

$$\gcd(r, s) = 1, \tag{27}$$

$$r \not\equiv s \pmod 2 \tag{28}$$

が成り立つ.

逆に, 条件 (26), (27), (28) を満たす任意の整数 r, s に対して,

$$a = r^2 - s^2, \quad b = 2rs, \quad c = r^2 + s^2$$

とおくとき, (a, b, c) は (21), (22), (23), (24) を満たす.

よって, 定理 3.2 から次の定理が得られる.

定理 3.3. 正の整数 n が合同数であるための必要十分条件は, ある整数 k, r, s が存在して

$$nk^2 = rs(r^2 - s^2)$$

となり, 条件 (26), (27), (28) を満たすことである.

証明. n が合同数なら, ある整数 a, b, c, k が存在して (20) を満たす. このとき, (22), (23), (24) が成り立つと仮定してもよい. よって

$$n = \frac{ab}{2} = rs(r^2 - s^2)$$

となり, r, s は (26), (27), (28) を満たす.

逆に, $nk^2 = rs(r^2 - s^2)$ と表せるなら, (25) のようにして a, b, c を定めれば (20) を満たす. □

定理 3.4. a, b, $c \in \mathbb{Z}$ とする. $a^2 + b^2 = c^2$ ならば, ac, bc は合同数である.

証明. $a^2 + b^2 = c^2$ ならば,

$$(ac)b^2 = ca(c^2 - a^2),$$
$$(bc)a^2 = cb(c^2 - b^2).$$

ゆえに定理 3.3 より, ac, bc は合同数である. □

定理 3.5. 正の整数 n が合同数であるための必要十分条件は, ある正の有理数 x が存在して

$$x - n, \quad x, \quad x + n$$

がすべて有理数の平方となることである.

証明. n が合同数のとき, ある a, b, $c \in \mathbb{Q}$ が存在して

$$a^2 + b^2 = c^2, \quad n = \frac{ab}{2}$$

を満たす. このとき

$$\left(\frac{a \pm b}{2}\right)^2 = \frac{a^2 \pm 2ab + b^2}{4} = \frac{a^2 + b^2}{4} \pm \frac{2ab}{4} = \left(\frac{c}{2}\right)^2 \pm n.$$

よって $x=(c/2)^2$ とおけば, $x-n$, x, $x+n$ はすべて有理数の平方となる.

逆に, 正の有理数 x が存在して $x-n$, x, $x+n$ がすべて有理数の平方になるとする.

$$a=\sqrt{x+n}-\sqrt{x-n},\quad b=\sqrt{x+n}+\sqrt{x-n},\quad c=2\sqrt{x}$$

とおくと, a, b, c はすべて正の整数であり,

$$\begin{aligned}a^2+b^2&=(\sqrt{x+n}-\sqrt{x-n})^2+(\sqrt{x+n}+\sqrt{x-n})^2\\&=2(x+n)+2(x-n)=4x=c^2\end{aligned}$$

となり, さらに

$$\begin{aligned}\frac{ab}{2}&=\frac{(\sqrt{x+n}-\sqrt{x-n})(\sqrt{x+n}+\sqrt{x-n})}{2}\\&=\frac{(x+n)-(x-n)}{2}=n\end{aligned}$$

となる. よって n は合同数である. □

4 合同数と Diophantus 方程式

1 つまたは複数の $\mathbb{Z}$ 係数の多項式

$$f_i(x_1,x_2,\ldots,x_n),\quad 1\le i\le m$$

から作られる方程式（$m=1$ のとき）もしくは連立方程式（$m\ge 2$ のとき）

$$f_i(x_1,x_2,\ldots,x_n)=0,\quad 1\le i\le m$$

は, 一般に Diophantus 方程式と呼ばれている. Diophantus 方程式の整数解に関する問題は昔から研究されている.

例 7. Diophantus 方程式は, その整数解を決定することが見た目よりずっと困難である場合が多い. その最たる例は,

$$x^n+y^n=z^n$$

という形の方程式である. $n\ge 3$ のとき, この方程式に $xyz\neq 0$ なる整数解 (x,y,z) が存在しないことを示す問題, いわゆる Fermat 予想は, 1995 年に A. Wiles が現代的な手法を駆使してようやく解決した.

この節では, 合同数と関係の深い 2 つの Diophantus 方程式

$$\begin{cases}x^2+ny^2=z^2,\\ x^2-ny^2=w^2\end{cases}$$

と

$$x^4-ny^4=u^2$$

について考察する.

n を合同数とすると, 定理 3.3 より, ある整数 k, r, s が存在して

$$nk^2 = rs(r^2 - s^2)$$

となる.

$$\begin{aligned} x &= r^2 + s^2, \\ y &= 2k, \\ z &= r^2 - s^2 + 2rs, \\ w &= r^2 - s^2 - 2rs \end{aligned}$$

とおくと,

$$\begin{cases} x^2 + ny^2 = z^2, \\ x^2 - ny^2 = w^2 \end{cases} \tag{29}$$

が成り立つ.

今度は, n を正の整数とし, (x, y, z, w) を (29) が成り立つような任意の整数の組とするとき, $u = zw$ とおけば,

$$x^4 - n^2y^4 = u^2 \tag{30}$$

が成り立つ.

さらに, n を正の整数とし, (x, y, u) を (30) が成り立つような任意の整数の組とするとき,

$$u^2 + (ny^2)^2 = (x^2)^2$$

となる. 定理 3.4 より, ny^2x^2 は合同数である. したがって定理 3.1 より, n は合同数である.

以上より, 次の定理が得られる.

定理 4.1. 正の整数 n が合同数であるための必要十分条件は, 連立方程式

$$\begin{cases} x^2 + ny^2 = z^2 \\ x^2 - ny^2 = w^2 \end{cases} \tag{31}$$

が $xyzw \neq 0$ なる整数解 (x, y, z, w) を持つことである.

定理 4.2. 正の整数 n が合同数であるための必要十分条件は, 方程式

$$x^4 - n^2y^4 = u^2 \tag{32}$$

が $xyu \neq 0$ なる整数解 (x, y, u) を持つことである.

注意 4.3. 方程式 (32) の整数解 (x, y, u) に対して, 必ずしも (x, y, z, w) が連立方程式 (31) の解であるような整数 z, w が取れるとは限らない.

例えば, $n = 23$, $x = 205$, $y = 17$, $u = 41496$ とするとき, (x, y, u) は方程式 (32) の整数解であるが,

$$x^2 - ny^2 = 2 \cdot 7^2 \cdot 19^2, \quad x^2 + ny^2 = 2^5 \cdot 3^2 \cdot 13^2$$

となる.

例 8. 1 が合同数でないということは, 連立方程式

$$x^2+y^2=z^2,\quad x^2-y^2=w^2$$

が $xyzw\neq 0$ なる整数解 (x,y,z,w) を持たないことと同値である.

また, 1 が合同数でないということは, 方程式

$$x^4-y^4=u^2$$

が $xyu\neq 0$ なる整数解 (x,y,u) を持たないこととも同値である. なお, $x^4-y^4=u^2$ が自明でない整数解を持たないことから, $x=X$, $u=Y^2$, $y=Z$ とおくことにより, Fermat の定理の $n=4$ の場合, すなわち, 方程式 $X^4+Y^4=Z^4$ に自明でない整数解が存在しないことが導かれる.

例 9. $n=101$ のとき, 連立方程式 (31) の最小解は

$$\begin{aligned}x&=2015242462949760001961,\\ y&=118171431852779451900,\\ z&=2339148435306225006961,\\ w&=1628124370727269996961\end{aligned}$$

である.

n を正の整数とし, (x,y,u) を方程式

$$x^4-n^2y^4=-u^2 \tag{33}$$

の整数解とする.

$$\begin{aligned}x^4-n^2y^4=-u^2 &\Longleftrightarrow n^2x^4-n^4y^4=-n^2u^2\\ &\Longleftrightarrow (ny)^4-n^2x^4=(nu)^2.\end{aligned}$$

よって, (nx,y,nu) は方程式 (32) の整数解である.

逆に, (x,y,u) を方程式 (32) の整数解とすると,

$$\begin{aligned}x^4-n^2y^4=u^2 &\Longleftrightarrow n^2x^4-n^4y^4=n^2u^2\\ &\Longleftrightarrow (ny)^4-n^2x^4=-(nu)^2.\end{aligned}$$

よって, (nx,y,nu) は方程式 (32) の整数解である.

したがって, 次の定理が得られる.

定理 4.4. 正の整数 n が合同数であるための必要十分条件は, 方程式

$$x^4-n^2y^4=-u^2 \tag{34}$$

が $xyu\neq 0$ なる整数解 (x,y,u) を持つことである.

(x,y,u) が連立方程式

$$x^2+ny^2=z^2,\quad x^2-ny^2=-w^2$$

の整数解ならば,

$$x^4-n^2y^4=-(zw)^2$$

が成り立つので, (x,y,zw) は方程式 (34) の整数解である. したがって, 次の定理が得られる.

定理 4.5. n を正の整数とする. 連立方程式

$$\begin{cases} x^2 + ny^2 = z^2 \\ x^2 - ny^2 = -w^2 \end{cases} \tag{35}$$

が $xyzw \neq 0$ なる整数解 (x, y, z, w) を持てば, n は合同数である.

注意 4.6. n を正の整数とし, (x, y, z, w) を (35) の整数解とすると,

$$2x^2 = z^2 - w^2, \quad 2ny^2 = z^2 + w^2 \tag{36}$$

である.

$$\begin{aligned} x_1 &= z^4 + w^4, \\ y_1 &= 4xyzw, \\ z_1 &= z^4 + 2z^2w^2 - w^4, \\ w_1 &= z^4 - 2z^2w^2 - w^4 \end{aligned}$$

とおき, (36) を用いて計算すると

$$\begin{aligned} x_1^2 + ny_1^2 &= z^8 + 2w^4z^4 + w^8 + 16nx^2y^2z^2w^2 \\ &= z^8 + 2w^4z^4 + w^8 + 4(z^2 - w^2)(z^2 + w^2)z^2w^2 \\ &= z^8 + 4w^2z^6 + 2w^4z^4 - 4w^6z^2 + w^8 \\ &= (z^4 + 2z^2w^2 - w^4)^2 = z_1^2. \end{aligned}$$

同様に計算すると

$$\begin{aligned} x_1^2 - ny_1^2 &= z^8 + 2w^4z^4 + w^8 - 16nx^2y^2z^2w^2 \\ &= z^8 + 2w^4z^4 + w^8 - 4(z^2 - w^2)(z^2 + w^2)z^2w^2 \\ &= z^8 - 4w^2z^6 + 2w^4z^4 + 4w^6z^2 + w^8 \\ &= (z^4 - 2z^2w^2 - w^4)^2 = w_1^2. \end{aligned}$$

よって, (x_1, y_1, z_1, w_1) は連立方程式 (31) の解である.

1 が合同数でないことと, 連立方程式

$$\begin{cases} x^2 + y^2 = z^2, \\ x^2 - y^2 = w^2 \end{cases} \tag{37}$$

が $xyzw \neq 0$ なる整数解 (x, y, z, w) を持たないことが同値であることはすでに述べた.

そもそもは, Fermat によって, 上の連立方程式に $xyzw \neq 0$ なる整数解 (x, y, z, w) を持たないことが示され, それによって 3 辺が有理数で面積が 1 の直角三角形が存在しないことが示された, と歴史では伝えられている.

ここでは, §2 の結果を使わずに, 上の連立方程式が解を持たないことを示す.

定理 4.7. 連立方程式 (37) は $xyzw \neq 0$ なる整数解 (x, y, z, w) を持たない.

証明. 正の整数解について考えれば十分である. 連立方程式 (37) が正の整数解を持つと仮定し, その中で x について最小のものを (x_0, y_0, z_0, w_0) とする:

$$\begin{cases} x_0^2 + y_0^2 = z_0^2, \\ x_0^2 - y_0^2 = w_0^2. \end{cases}$$

まず,

$$\gcd(x_0, y_0, z_0, w_0) = 1$$

が成り立つ. なぜなら, もし x_0, y_0, z_0, w_0 を割る素数 p が存在すれば, $(x_0/p, y_0/p, z_0/p, w_0/p)$ も連立方程式の整数解であるが, $x_0/p < x_0$ となるので x_0 の最小性に反する.

次に,

$$\gcd(x_0, y_0) = 1$$

が成り立つ. なぜなら, もし仮に x_0, y_0 を両方とも割る素数 p が存在すれば, p は z_0, w_0 も割るので, $\gcd(x_0, y_0, z_0, w_0) = 1$ に反する.

x_0, y_0 がともに偶数ではないことは $\gcd(x_0, y_0) = 1$ より明らかであるが, さらに,

$$x_0 \equiv z_0 \equiv w_0 \equiv 1, \quad y_0 \equiv 0 \pmod 2$$

がいえる. なぜなら, もし仮に x_0, y_0 がともに奇数であるとすると, $x_0^2 + y_0^2$ は 4 を法として 2 と合同になり, z_0^2 が 4 を法として 0 か 1 と合同であることに反する. また, もし仮に y_0 が偶数であるとすると, x_0 は奇数でなければならないうえに, $x_0^2 - y_0^2$ は 4 を法として 3 と合同になり, w_0^2 が 4 を法として 0 か 1 と合同であることに反する. よって x_0 は奇数, y_0 は偶数である. これにより, z_0, w_0 が奇数であることもわかる.

$w_0^2 = x_0^2 - y_0^2 < x_0^2 + y_0^2 = z_0^2$ より, $w_0 < z_0$ である. よって $(z_0 \pm w_0)/2$ は正の整数である. ここで

$$\gcd\left(\frac{z_0 + w_0}{2}, \frac{z_0 - w_0}{2}\right) = 1$$

が成り立つ. なぜなら, もし仮に素数 p が $(z_0 \pm w_0)/2$ を両方とも割れば, その和と差である z_0, w_0 も割る. これらは奇数だから $p \neq 2$. さらに p は $x_0^2 \pm y_0^2$ を割り, その和と差である $2x_0^2$, $2y_0^2$ を割る. これは $\gcd(x_0, y_0) = 1$, $p \neq 2$ に反する.

また,

$$\left(\frac{z_0 + w_0}{2}\right)^2 + \left(\frac{z_0 - w_0}{2}\right)^2 = \frac{z_0^2 + w_0^2}{2} = x_0^2$$

が成り立つ. x_0 は奇数だから, $(z_0 \pm w_0)/2$ の一方は奇数で, もう一方は偶数である. したがって, ある整数 r, s によって

$$\begin{cases} \dfrac{z_0 + w_0}{2} = r^2 - s^2, \\ \dfrac{z_0 - w_0}{2} = 2rs, \\ x_0 = r^2 + s^2 \end{cases} \quad \text{または} \quad \begin{cases} \dfrac{z_0 + w_0}{2} = 2rs, \\ \dfrac{z_0 - w_0}{2} = r^2 - s^2, \\ x_0 = r^2 + s^2 \end{cases}$$

と表示できて,

$$r > s > 0, \quad \gcd(r, s) = 1, \quad r \not\equiv s \pmod 2$$

が成り立つ. いずれにせよ, $2y_0^2 = z_0^2 - w_0^2$ より

$$\left(\frac{y_0}{2}\right)^2 = \frac{1}{2} \cdot \frac{z_0 + w_0}{2} \cdot \frac{z_0 - w_0}{2} = rs(r + s)(r - s)$$

となる．y_0 は偶数だから，$y_0/2$ は整数である．また，$\gcd(r,s)=1$，$r \not\equiv s \pmod 2$ だから，r，s，$r+s$，$r-s$ のどの 2 つも互いに素である．よって，どれも平方数になる．

$$r = x_1^2, \quad s = y_1^2, \quad r+s = z_1^2, \quad r-s = w_1^2$$

とおけば，

$$\begin{cases} x_1^2 + y_1^2 = z_1^2, \\ x_1^2 - y_1^2 = w_1^2 \end{cases}$$

となり，さらに

$$x_1 \leq r \leq r^2 < r^2 + s^2 = x_0$$

が成り立つ．これは x_0 の最小性に反する． □

5　合同数と楕円曲線

正の整数 n に対して

$$E_n : y^2 = x^3 - n^2 x$$

を $\mathbb{Q}$ 上定義された楕円曲線とする．

$P = (x, y)$ を E_n 上の点とする．x，y がともに有理数であるとき，P は有理点であるという．$E_n(\mathbb{Q})$ を E_n 上の有理点の全体とする．$E_n(\mathbb{Q})$ は，幾何的に定義された演算を導入することにより，無限遠点と呼ばれる点 $\mathcal{O}$ を零元とする加法群をなす．しかも，有限生成であることが知られている．$E_n(\mathbb{Q})$ の有限位数の点の全体を $E_n(\mathbb{Q})_{\mathrm{tors}}$ とおくと，ある負でない整数 r が存在して

$$E_n(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E_n(\mathbb{Q})_{\mathrm{tors}}$$

が成り立つ．r は E_n に対して一定の値である．r を楕円曲線 E_n の階数といい，$\operatorname{rank} E_n(\mathbb{Q})$ で表す．

E_n 上の点 P について，ある正の整数 m が存在して $mP = \mathcal{O}$ が成り立つとき，そのような m のうちで最小のものを P の位数という．そのような m が存在しないとき，P の位数は無限であるという．

E_n 上の無限遠点以外の点が位数 2 であることの必要十分条件は，その点の y 座標が 0 となることである．よって，E_n 上の有理点 $(0,0)$，$(\pm n, 0)$ はいずれも位数 2 である．さらに，

$$E_n(\mathbb{Q})_{\mathrm{tors}} = \{\mathcal{O},\, (0,0),\, (n,0),\, (-n,0)\} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

が成り立つ．これにより，$(0,0)$，$(\pm n, 0)$ 以外の有理点 P が存在すれば，P の位数は無限であること，すなわち，$\operatorname{rank} E_n(\mathbb{Q}) > 0$ がいえる．

楕円曲線について，次のことが成り立つ．

定理 5.1 (2 倍公式). 楕円曲線

$$y^2 = x^3 + ax^2 + bx + c, \quad a,\, b,\, c \in \mathbb{Q}$$

上の点 $P = (x, y)$ に対して，$2P \neq \mathcal{O}$ ならば，$2P$ の x 座標 $x(2P)$ は

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx - 4ac + b^2}{4y^2}$$

で与えられる. 特に, $a = c = 0$ のとき

$$x(2P) = \left(\frac{x^2 - b}{2y}\right)^2$$

となる.

定理 5.1 を用いると, $P = (x, y)$ を E_n 上の無限位数の点とすれば, $2P \neq \mathcal{O}$ だから,

$$x(2P) = \left(\frac{x^2 + n^2}{2y}\right)^2 \in \mathbb{Q}^{\times 2}$$

が成り立つ. さらに,

$$\begin{aligned} x(2P) \pm n &= \left(\frac{x^2 + n^2}{2y}\right)^2 \pm n = \frac{(x^2 + n^2)^2 \pm 4y^2 n}{(2y)^2} \\ &= \frac{(x^2 + n^2)^2 \pm 4(x^3 - n^2 x)n}{(2y)^2} \\ &= \left(\frac{x^2 - n^2 \pm 2nx}{2y}\right)^2 \in \mathbb{Q}^{\times 2} \end{aligned}$$

が成り立つ. 定理 3.5 より, n は合同数である.

逆に, n を合同数とすると, ある正の有理数 a, b, c が存在して

$$a^2 + b^2 = c^2, \quad n = \frac{ab}{2}$$

となる. このとき

$$(a \pm b)^2 = a^2 + b^2 \pm 2ab = c^2 \pm 4n.$$

よって,

$$\left(\frac{a \pm b}{2}\right)^2 = \left(\frac{c}{2}\right)^2 \pm n.$$

2 つを掛け合わせると

$$\left(\frac{a^2 - b^2}{4}\right)^2 = \left(\frac{c}{2}\right)^4 - n^2.$$

両辺に $(c/2)^2$ を乗じると

$$\left(\frac{(a^2 - b^2)c}{8}\right)^2 = \left(\frac{c}{2}\right)^6 - n^2\left(\frac{c}{2}\right)^2.$$

よって,

$$(x_1, y_1) = \left(\frac{c^2}{4}, \frac{(a^2 - b^2)c}{8}\right)$$

は楕円曲線 E_n 上の有理点である. また, $y_1 \neq 0$ である. なぜなら, もし仮に $y_1 = 0$ ならば, $c \neq 0$ より $a = b$ である. $a^2 + b^2 = c^2$ より $2a^2 = c^2$ となるが, これは起こりえない. ゆえに (x_1, y_1) は無限位数の点である.

以上より, 次の定理が得られる.

定理 5.2. 正の整数 n について, n が合同数であることの必要十分条件は, 楕円曲線 E_n が無限位数の点を持つこと, すなわち, $\operatorname{rank} E_n(\mathbb{Q}) > 0$ となることである.

与えられた正の整数が合同数であるかどうかを判定することについて, J. Tunnell は決定的な定理を発見した.

定理 5.3 (Tunnell). n を square-free な正の整数とする.

n が奇数の合同数ならば,

$$\#\{x,y,z\in\mathbb{Z}\mid n=2x^2+y^2+32z^2\}=\frac{1}{2}\cdot\#\{x,y,z\in\mathbb{Z}\mid n=2x^2+y^2+8z^2\}$$

が成り立つ. さらに, もし楕円曲線 E_n に関して Birch and Swinnerton-Dyer 予想が正しければ, 逆も成り立つ.

また, n が偶数の合同数ならば,

$$\#\left\{x,y,z\in\mathbb{Z}\;\middle|\;\frac{n}{2}=4x^2+y^2+32z^2\right\}=\frac{1}{2}\cdot\#\left\{x,y,z\in\mathbb{Z}\;\middle|\;\frac{n}{2}=4x^2+y^2+8z^2\right\}$$

が成り立つ. さらに, もし楕円曲線 E_n に関して Birch and Swinnerton-Dyer 予想が正しければ, 逆も成り立つ.

なお, Birch and Swinnerton-Dyer 予想とは, $\mathbb{Q}$ 上定義された楕円曲線に関する次のような主張である.

予想 5.4 (Birch and Swinnerton-Dyer). E を $\mathbb{Q}$ 上定義された楕円曲線とし, $L(E,s)$ を E の Hasse-Weil L 関数とする. このとき,

$$L(E,1)=0\Longleftrightarrow\operatorname{rank}E(\mathbb{Q})>0$$

が成り立つ.

正確には, これは Birch and Swinnerton-Dyer 予想の weak version と呼ばれるものである. E が虚数乗法を持つ場合には, $\operatorname{rank}E(\mathbb{Q})>0$ ならば $L(E,1)=0$ であることが J. Coates と A. Wiles によって示されている. 特に, 楕円曲線 E_n は虚数乗法を持つので, Coates と Wiles の結果が適用できる.

Tunnell の結果は, 見た目はシンプルだが, 楕円曲線の Hasse-Weil L 関数や半整数 weight の保型形式などを研究することで得られたものである.