1　方程式 $x^2+y^2=2^e$ の整数解

r を正の整数とする．方程式

$$x^2+y^2=r$$

の解 (x,y) のうち, $\gcd(x,y)=1$ を満たすものを**原始解**という．

［定理 1.1］ e を正の整数とする．このとき, 方程式

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

が原始解を持つための必要十分条件は $e=1$ となることである．

［証明］ $e=1$ のとき, $(x,y)=(1,1)$ が方程式 (1) の原始解である．

$e\geq 2$ のとき方程式 (1) の原始解が存在しないことを背理法により証明する．もし仮に $e\geq 2$ のとき原始解 (x,y) が存在すれば, x, y はともに奇数でなければならない．なぜなら, (x,y) は原始解だから x, y がともに偶数になることはない．また, もし片方が奇数, もう片方が偶数なら, (x,y) が (1) を満たすことに矛盾する．ともに奇数のとき, $x^2\equiv y^2\equiv 1 \pmod 8$ だから, $x^2+y^2\equiv 2 \pmod 8$. これは $e\geq 2$ に反する． $\square$

［注意 1.2］ 原始解でなければ, $e\geq 2$ のときでも方程式 (1) は整数解を持つ．

e が偶数のとき, $e=2e_1$ $(e_1\geq 1)$ とおくと, $(x,y)=(0,2^{e_1})$ が解になる．

e が奇数のとき, $e=2e_2+1$ $(e_2\geq 1)$ とおくと, $(x,y)=(2^{e_2},2^{e_2})$ が解になる．

［定理 1.3］ e を偶数とする．このとき, 方程式

$$x^2+y^2=2^e$$

が整数解 (x,y) を持つならば, $x=0$ または $y=0$ である．

［証明］ 背理法により証明する．(x,y) を方程式 $x^2+y^2=2^e$ の整数解とし, $x'\neq 0$, $y'\neq 0$ と仮定する．

$\mathrm{ord}_2(x)\leq \mathrm{ord}_2(y)$ としても一般性を失わない．$h=\mathrm{ord}_2(x)$, $x'=x/2^h$, $y'=y/2^h$ とおくと,

$$(x')^2+(y')^2=2^{e-2h}.$$

もし $h=\mathrm{ord}_2(x)=\mathrm{ord}_2(y)$ ならば, x', y' はともに奇数なので, $x'^2\equiv y'^2\equiv 1 \pmod 8$ より, $x'^2+y'^2\equiv 2 \pmod 8$. これは $e-2h$ が偶数であることに矛盾する．したがって, $\mathrm{ord}_2(x)<\mathrm{ord}_2(y)$ でなければならない．よって, x' は奇数, y' は偶数であり, $(x')^2+(y')^2$ は奇数である．ゆえに, $e-2h=0$. すなわち,

$$(x')^2+(y')^2=1.$$

x, y はともに 0 ではないので, 左辺は 1 より大きい．これは不可能である． $\square$

2　有理数の連分数展開

有理数 α の連分数展開

$$\alpha = a_0 + \frac{1}{a_1 +} \frac{1}{a_2 +} \cdots + \frac{1}{a_N}$$

の最初の $n+1$ 項 $(0 \leq n \leq N)$ を既約分数 p_n/q_n で

$$\frac{p_n}{q_n} = a_0 + \frac{1}{a_1 +} \frac{1}{a_2 +} \cdots + \frac{1}{a_n}$$

のように表すとき, p_n/q_n を α の n 番目の**近似分数**という.

$p_{-2} = 0,\ p_{-1} = 1,\ q_{-2} = 1,\ q_{-1} = 0$ と定めると, $n = 0, 1, 2, \ldots$ に対して,

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2}, \\ q_n &= a_n q_{n-1} + q_{n-2}. \end{aligned} \tag{2}$$

また, $n = -2, -1, 0, \ldots$ に対して,

$$p_{n+1} q_n - p_n q_{n+1} = (-1)^n.$$

特に, $\gcd(p_n, q_n) = 1$ が成り立つ. なぜなら, もし仮に $p_n,\ q_n$ の両方を割る素数 p が存在すれば, 上式の左辺は p の倍数であるが, 右辺は $(-1)^n$ のため不可能である.

[補題 2.1] すべての整数 $n \geq 1$ に対して $a_n \geq 1$ であるとする. このとき, すべての整数 $n \geq 1$ に対して

(i) $n \leq q_n$

(ii) $q_n < q_{n+1}$

が成り立つ.

[証明] (i)　n に関する数学的帰納法により証明する. まず, $q_{-2} = 1,\ q_{-1} = 0$ より,

$$q_0 = a_0 q_{-1} + q_{-2} = 1.$$

これと $a_1 \geq 1,\ a_2 \geq 1$ より,

$$\begin{aligned} q_1 &= a_1 q_0 + q_{-1} = a_1 \geq 1, \\ q_2 &= a_2 q_1 + q_0 = a_1 a_2 + 1 \geq 2. \end{aligned}$$

$n \geq 3$ のとき, $1 \leq k < n$ なるすべての番号 k について $k \leq q_k$ であると仮定すると, $a_n \geq 1$ より

$$\begin{aligned} q_n &= a_n q_{n-1} + q_{n-2} \geq q_{n-1} + q_{n-2} \\ &\geq (n-1) + (n-2) = 2n - 3 \\ &\geq n. \end{aligned}$$

以上より, すべての整数 $n \geq 1$ に対して $n \leq q_n$ が成り立つことが示された.

(ii)　まず,

$$q_1 = a_1 q_0 + q_{-1} = a_1,$$
$$q_2 = a_2 q_1 + q_0 = a_1 a_2 + 1.$$

$a_1 \geq 1$, $a_2 \geq 1$ より, $q_1 < q_2$ が成り立つ.

$n \geq 3$ のとき, $a_n \geq 1$ であり, (i) より $n-2 \leq q_{n-2}$ であるから,

$$q_n = a_n q_{n-1} + q_{n-2} \geq q_{n-1} + (n-2) > q_{n-1}.$$

□

[注意 2.2] $q_0 = 1$. よって, $q_0 \leq q_1$ である.

[補題 2.3] α を有理数とし, 連分数展開が

$$\alpha = a_0 + \frac{1}{a_1 +}\frac{1}{a_2 +} \cdots + \frac{1}{a_N}, \quad N > 1$$

によって与えられているものとする. p_n/q_n を α の近似分数とする. このとき, $0 \leq n \leq N-1$ なる任意の番号 n に対して,

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \frac{1}{q_n q_{n+1}}$$

が成り立つ.

[証明] $n \geq 1$ のときは, G. M. ハーディ, E. M. ライト [2], 定理 164 を参照.

$n = 0$ のとき, $a_1, a_2, \ldots, a_N$ はすべて正であり, $p_0 = a_0$, $q_0 = 1$, $q_1 = a_1$ であるから,

$$\alpha - \frac{p_0}{q_0} = \alpha - a_0 = \frac{1}{a_1 +}\frac{1}{a_2 +} \cdots + \frac{1}{a_N} < \frac{1}{a_1} = \frac{1}{q_0 q_1}.$$

また, $0 \leq \alpha - a_0$. ゆえに, 定理の主張が成り立つ. □

[注意 2.4] 有理数 α の連分数展開において, α が整数でない有理数ならば, $N = 1$ の場合でも,

$$a_0 + \frac{1}{a_1} = a_0 + \frac{1}{a_1 - 1 +}\frac{1}{1}$$

のようにして $N > 1$ とすることができる.

逆に, α が整数ならば, 「$N = 0$」または「$N = 1$ かつ $a_1 = 1$」であり, $N > 1$ とすることはできない.

3　方程式 $x^2+y^2=p^e$ の整数解

［補題 3.1］ p を奇素数, a を整数とし, $\gcd(a,p)=1$ とする. また, $e \geq 2$ を整数とする. このとき, 方程式

$$x^2 \equiv a \pmod{p^e}$$

が解を持つための必要十分条件は, 方程式

$$x^2 \equiv a \pmod{p}$$

が解を持つことである. また, 解を持てば, その個数は 2 つである.

［証明］ (必要性)　明らかである.

(十分性)　r を $\bmod p^e$ の原始根とすると, ある整数 $v \geq 0$ が存在して,

$$a \equiv r^v \pmod{p^e}.$$

r は $\bmod p$ の原始根でもあり, $a \equiv r^v \pmod{p}$ である. 方程式 $x^2 \equiv a \pmod{p}$ の解 x' について, ある整数 $u \geq 0$ が存在して,

$$x' \equiv r^u \pmod{p}.$$

よって,

$$r^{2u} \equiv a \pmod{p}.$$

ゆえに,

$$r^{2u} \equiv r^v \pmod{p}.$$

これより, $v \equiv 2u \pmod{p-1}$. 仮定より p は奇素数だから, $p-1$ は偶数であり, $v \equiv 0 \pmod{2}$. したがって, $x \equiv r^{v/2} \pmod{p^e}$ とすれば, $x^2 \equiv a \pmod{p^e}$ が成り立つ.

(解の個数) 方程式 $x^2 \equiv a \pmod{p^e}$ に解 x_0 が少なくとも 1 つ存在すれば, $-x_0$ も解である. もし仮に $x_0 \equiv -x_0 \pmod{p^e}$ ならば, $2x_0 \equiv 0 \pmod{p^e}$ である. 仮定より $\gcd(p,2)=1$ だから, $x_0 \equiv 0 \pmod{p^e}$ でなければならない. よって, $a \equiv x_0^2 \equiv 0 \pmod{p^e}$. ところが, これは $\gcd(a,p)=1$ に反する. したがって, 解があれば少なくとも 2 個ある.

正の整数 e に対して, 合同方程式

$$x^2 \equiv a \pmod{p^e}$$

を E_e で表し, その解の全体を S_e で表すことにする.

方程式 E_1 の解の個数 $|S_1|$ が 2 であること, すなわち方程式 $x^2 \equiv a \pmod{p}$ の解の個数が 2 であることの証明は省略する.

一般の $e \geq 2$ について, E_e の任意の解は E_{e-1} の解であるから, 写像

$$f : S_e \to S_{e-1}, \quad x + p^e\mathbb{Z} \mapsto x + p^{e-1}\mathbb{Z}$$

が定まる.

さて, x, $x' \in \mathbb{Z}$ を E_e の解とし, $f(x+p^e\mathbb{Z}) = f(x'+p^e\mathbb{Z})$ と仮定すると,

$$x \equiv x' \pmod{p^{e-1}}.$$

すなわち, ある $y \in \mathbb{Z}$ が存在して,

$$x = x' + p^{e-1}y. \tag{3}$$

これを E_e に代入すると,

$$\begin{aligned} x^2 - a &= (x' + p^{e-1}y)^2 - a \\ &= (x' - a) + 2p^{e-1}x'y + p^{2(e-1)}y. \end{aligned}$$

ゆえに,

$$2p^{e-1}x'y \equiv 0 \pmod{p^e}.$$

すなわち,

$$2x'y \equiv 0 \pmod{p}.$$

$\gcd(a,p) = 1$ より $\gcd(x',p) = 1$ だから, $y \equiv 0 \pmod{p}$. したがって, (3) より, $x \equiv x' \pmod{p^e}$. よって, f は単射であることが示され, $|S_e| \le |S_{e-1}|$ が得られる. すると,

$$|S_e| \le |S_{e-1}| \le \cdots \le |S_1| = 2.$$

一方, 先に述べたことから $2 \le |S_e|$ なので, $|S_e| = 2$ となる. □

[定理 3.2] p を奇素数とし, $p \equiv 1 \pmod{4}$ を満たすとする. このとき, 任意の整数 $e > 0$ に対して, 方程式

$$x^2 + y^2 = p^e$$

は原始解を持つ.

[証明] $p \equiv 1 \pmod{4}$ であれば, -1 は p を法とする平方剰余である. よって, 補題 3.1 より, ある $l \in \mathbb{Z}$ が存在して,

$$l^2 \equiv -1 \pmod{p^e}.$$

また, $\gcd(l,p) = 1$ である.

有理数 l/p^e を連分数展開したときの近似分数を p_n/q_n $(n = 0, 1, \ldots, N)$ とする. l/p^e は整数ではないので, 必ず $N > 1$ とすることができる. 補題 2.1 より,

$$1 = q_0 \le q_1 < q_2 < \cdots < q_N = p^e.$$

ここで, $q_N = p^e$ は, $l/p^e = p_N/q_N$ と, 両方とも分母が正の既約分数であることから得られる．よって, ある番号 n $(0 \leq n \leq N-1)$ が存在して,

$$q_n \leq p^{e/2} < q_{n+1}. \tag{4}$$

このとき, 補題 2.3 より,

$$\left| \frac{l}{p^e} - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{q_n p^{e/2}}. \tag{5}$$

$a = lq_n - p^e p_n$ とおくと, (5) より,

$$\begin{aligned} |a| = |lq_n - p^e p_n| &= q_n p^e \left| \frac{lq_n - p^e p_n}{p^e q_n} \right| \\ &= q_n p^e \left| \frac{l}{p^e} - \frac{p_n}{q_n} \right| < p^{e/2}. \end{aligned}$$

よって, (4) より,

$$0 < a^2 + q_n^2 < 2p^e. \tag{6}$$

また, $a \equiv lq_n \pmod{p^e}$ であるから,

$$a^2 + q_n^2 \equiv l^2 q_n^2 + q_n^2 = (l^2+1)q_n^2 \equiv 0 \pmod{p^e}.$$

ゆえに, (6) より, $p^e = a^2 + q_n^2$ でなければならない.

最後に, $\gcd(a, q_n) = 1$ を示す.

$$\begin{aligned} p^e = a^2 + q_n^2 &= (lq_n - p^e p_n)^2 + q_n^2 \\ &= (l^2+1)q_n^2 - 2lq_n p^e p_n + p^{2e} p_n^2 \end{aligned}$$

より,

$$\begin{aligned} 1 &= \frac{l^2+1}{p^e} \cdot q_n^2 - 2lq_n p_n + p^e p_n^2 \\ &= a(-p_n) + q_n \left(\frac{l^2+1}{p^e} \cdot q_n - lp_n \right). \end{aligned}$$

したがって, 方程式 $ax + q_n y = 1$ は整数解を持つ. □

[注意 3.3] e が偶数のとき, $e = 2e_1$ とおくと, 方程式 $x^2 + y^2 = p^e$ は常に $(x, y) = (0, p^{e_1})$ を整数解に持つ．これはもちろん原始解ではない.

[定理 3.4] p を奇素数とし, $p \equiv 3 \pmod 4$ を満たすとする．また, $e \geq 0$ を整数とする．このとき, 方程式

$$x^2 + y^2 = p^e$$

が整数解 (x, y) を持てば, $x = 0$ または $y = 0$ である.

[証明] (x, y) を方程式 $x^2+y^2=p^e$ の整数解とする. $x \neq 0$ かつ $y \neq 0$ と仮定して矛盾を導く.

$x \neq 0$ かつ $y \neq 0$ のとき, $x^2+y^2>1$ なので, $e \geq 1$. また, x^2, y^2 は $\bmod 4$ で 0 または 1 に合同なので, x^2+y^2 は $\bmod 4$ で 0, 1, 2 のいずれかに合同である. もし仮に e が奇数ならば $p \equiv 3 \pmod 4$ より矛盾が生じる. よって, e は偶数でなければならない. 特に, $e \geq 2$ である.

$h = \mathrm{ord}_p(x) \leq \mathrm{ord}_p(y)$ と仮定しても一般性を失わない. $x' = x/p^h$, $y' = y/p^h$ と置くと,

$$x'^2 + y'^2 = p^{e-h}, \quad 0 = \mathrm{ord}_p(x') \leq \mathrm{ord}_p(y')$$

を満たす. 先の議論から, $e - h \geq 2$ でなければならない. よって, もし仮に $\mathrm{ord}_p(x) < \mathrm{ord}_p(y)$ ならば, $\mathrm{ord}_p(y') > 0$ であるが, x' が p で割れることになって $\mathrm{ord}_p(x') = 0$ に反する. ゆえに, $\mathrm{ord}_p(x) = \mathrm{ord}_p(y)$ でなければならない. したがって, $\mathrm{ord}_p(x') = \mathrm{ord}_p(y') = 0$. よって,

$$x'^2 \equiv -y'^2 \pmod p, \quad \gcd(x', p) = \gcd(y', p) = 1.$$

このことは -1 が p を法として平方剰余であることを意味し, $p \equiv 3 \pmod 4$ に矛盾する. $\square$

4 一般の場合

[定理 4.1] r を正の整数とし, $r = \prod_{i=1}^{s} p_i^{e_i}$ を素因子分解とする. このとき, 方程式

$$x^2 + y^2 = r$$

が原始解を持つための必要十分条件は, $4 \nmid r$ かつ各 i について $p_i \not\equiv 3 \pmod 4$ が成り立つことである.

[証明] (十分性) まず, 定理 1.1 と定理 3.2 により, $i = 1, 2, \ldots, s$ に対して, 整数の組 (x_i, y_i) が存在して,

$$x_i^2 + y_i^2 = p_i^{e_i}, \quad \gcd(x_i, y_i) = 1$$

を満たす.

次に, $x = x_1x_2 + y_1y_2$, $y = x_1y_2 - x_2y_1$ とおくと, 恒等式

$$(x_1x_2 + y_1y_2)^2 + (x_1y_2 - x_2y_1)^2 = (x_1^2 + y_1^2)(x_2^2 + y_2^2)$$

から,

$$x^2 + y^2 = p_1^{e_1} p_2^{e_2}.$$

もし仮に $q \mid x$ かつ $q \mid y$ なる素数 q が存在すれば, q は $p_1^{e_1}$, $p_2^{e_2}$ のどちらかを割る. $q \mid p_2^{e_2}$ とすると, $\gcd(q, p_1^{e_1}) = 1$. このとき,

$$x_2 p_1^{e_1} = x_2(x_1^2 + y_1^2) = x_1(x_1x_2 + y_1y_2) - y_1(x_1y_2 - x_2y_1),$$
$$y_2 p_1^{e_1} = y_2(x_1^2 + y_1^2) = y_1(x_1x_2 + y_1y_2) + x_1(x_1y_2 - x_2y_1)$$

より, q は x_2, y_2 の公約数となり, $\gcd(x_2, y_2) = 1$ に矛盾する. ゆえに, $\gcd(x, y) = 1$. すなわち, (x, y) は方程式 $x^2 + y^2 = p_1^{e_1} p_2^{e_2}$ の原始解である.

この結果を用いて, $p_1^{e_1} p_2^{e_2}$ と $p_3^{e_3}$ に対して同様の操作を行えば, 方程式 $x^2 + y^2 = p_1^{e_1} p_2^{e_2} p_3^{e_3}$ の原始解が得られる.

これを繰り返せば, ついには $x^2 + y^2 = r$ の原始解が得られる.

(必要性)　方程式 $x^2 + y^2 = r$ が原始解 (x, y) を持つとする. このとき, x, y のどちらか一方は必ず奇数である. よって, $x^2 + y^2 \equiv 1, 2 \pmod 4$ となり, $4 \nmid r$ がいえる.

また, 各 $i = 1, 2, \ldots, s$ に対して, $x^2 \equiv -y^2 \pmod{p_i}$ が成り立つ. p_i が奇素数のとき, -1 は p_i を法とする平方剰余である. ゆえに, $p_i \not\equiv 3 \pmod 4$. $\square$

参考文献

[1] 河田敬義: 数論–古典数論から類体論へ, 岩波書店, 1992.

[2] G. M. ハーディ, E. M. ライト: 数論入門 I, シュプリンガー・フェアラーク東京, 2001.