

ペル方程式の解の構造

定理 1

$$x^2 - Dy^2 = 1 \quad (1)$$

を満たす自然数解を $(x, y) = (a, b)$ とすると, 自然数 n について

$$(a + b\sqrt{D})^n = A + B\sqrt{D}$$

で求まる (A, B) も (1) の解である. ここで言う自然数解とは x, y の両方とも自然数 (正整数) であることを示す.

[証明] $n = 1$ では自明. $n = k$ で成り立つと仮定すると,

$$(a + b\sqrt{D})^k = A + B\sqrt{D}$$

で求まる (A, B) が (1) の解である.

$$(a + b\sqrt{D})^{k+1} = (A + B\sqrt{D})(a + b\sqrt{D}) \quad (2)$$

$$= Aa + BbD + (Ab + aB)\sqrt{D} \quad (3)$$

$$\begin{aligned} (Aa + BbD)^2 - D(Ab + aB)^2 &= A^2a^2 + 2AaBbD + B^2b^2D^2 - D(A^2b^2 + 2AaBb + a^2B^2) \\ &= a^2(A^2 - DB^2) - Db^2(A^2 - DB^2) \\ &= a^2 - Db^2 = 1 \end{aligned}$$

よって全ての自然数 n においてこの定理は成り立つ.

[証明おわり]

(2),(3) の計算は行列で表すと,

$$\begin{pmatrix} a & Db \\ b & a \end{pmatrix} \begin{pmatrix} A \\ B \end{pmatrix}$$

とかける. つまり $(a + b\sqrt{D})^n$ の全ては

$$\begin{pmatrix} a & Db \\ b & a \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

と表せる.

定理 2

$$x^2 - Dy^2 = 1 \quad (4)$$

を満たす自然数解のうちで任意に 2 つ選び, それらを $(x, y) = (a, b), (c, d)$ とすると,

$$\frac{c + d\sqrt{D}}{a + b\sqrt{D}} = A + B\sqrt{D}$$

で求まる $(x, y) = (A, B)$ は (4) を満たす.

[証明]

$$\begin{aligned}\frac{c+d\sqrt{D}}{a+b\sqrt{D}} &= \frac{(c+d\sqrt{D})(a-b\sqrt{D})}{a^2-b^2D} \\ &= (ac-bdD) + (ad-bc)\sqrt{D} \\ A^2 - B^2 &= (ac-bdD)^2 - (ad-bc)^2D \\ &= a^2c^2 - 2abcdD + b^2d^2D^2 - a^2d^2D + 2abcdD - b^2c^2D \\ &= a^2c^2 + b^2d^2D^2 - a^2d^2D - b^2c^2D \\ &= a^2(c^2 - d^2D) - b^2(c^2 - d^2D)D = 1\end{aligned}$$

[証明おわり]

(A, B) は (4) を満たすが、必ずしも自然数解というわけではない。 $c+d\sqrt{D} > a+b\sqrt{D}$ のとき自然数解となる。 $c+d\sqrt{D} = a+b\sqrt{D}$ のときは $(1, 0)$ となる。 またこの割り算に相当する計算を行列を用いて表すと、

$$\begin{pmatrix} a & -Db \\ -b & a \end{pmatrix} \begin{pmatrix} c \\ d \end{pmatrix}$$

である。これは定理 1 の行列の逆行列である。

定理 3

$$x^2 - Dy^2 = 1 \tag{5}$$

を満たす自然数解のうちで $x + y\sqrt{D}$ の値を最小とするものを $(x, y) = (p, q)$ とすると、自然数 n について

$$(p + q\sqrt{D})^n = \alpha + \beta\sqrt{D}$$

で求まる (α, β) が (5) の自然数解の全てである。つまり (5) の任意の自然数解は

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} p & Dq \\ q & p \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

で表される。

[証明] (α, β) が (5) の解であることは定理 1 より明らか。その逆を証明する。(4) の任意の解を $(x, y) = (s, t)$ とすると、ある自然数 n について

$$(p + q\sqrt{D})^n \leq s + t\sqrt{D} < (p + q\sqrt{D})^{n+1}$$

全辺を $(p + q\sqrt{D})^n$ で割って、

$$1 \leq \frac{s + t\sqrt{D}}{(p + q\sqrt{D})^n} < p + q\sqrt{D}$$

$p + q\sqrt{D}$ は最小であるので、定理 2 より

$$\frac{s + t\sqrt{D}}{(p + q\sqrt{D})^n} = 1$$

つまり

$$s + t\sqrt{D} = (p + q\sqrt{D})^n$$

である。

[証明おわり]

問題 1 三角数でありかつ平方数であるものは無限に存在することを示せ、またそのような平方数はどのような数か説明せよ。

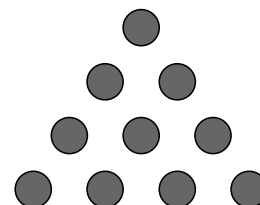
三角数というのは右図のように石をミラミッド状に並べたときの石の総数で、

$$\frac{1}{2}y(y+1) \quad (y \in \mathbf{N})$$

に等しい。

[証明]

$$\frac{1}{2}y(y+1) = x^2$$



を変形して、

$$(2y+1)^2 - 2(2x)^2 = 1 \tag{6}$$

を得る。($(2y+1)^2 - 8x^2 = 1$ でもいいのだが、なんとなくこっちで解こう) ペル方程式

$$X^2 - 2Y^2 = 1$$

の最小解は明らかに $(X, Y) = (3, 2)$ であるので、一般解は $n \geq 1$ に対して

$$\begin{pmatrix} X \\ Y \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{7}$$

奇数 p 、偶数 q に対して

$$\begin{pmatrix} P \\ Q \end{pmatrix} = \begin{pmatrix} p & 2q \\ q & p \end{pmatrix} \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3p+4q & 4p+6q \\ 3q+2p & 4q+3p \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 3p+4q \\ 3q+2p \end{pmatrix}$$

で得られる P は奇数、 Q は偶数であるので、数学的帰納法により、(7) で得られる X, Y は全て (6) の解を与える。つまり無限に存在する。 [証明おわり]

$$\begin{vmatrix} 3-\lambda & 4 \\ 2 & 3-\lambda \end{vmatrix} = 0$$

より、

$$\lambda = 3 \pm 2\sqrt{2}$$

$\lambda = 3 + 2\sqrt{2}$ のとき

$$\begin{pmatrix} -2\sqrt{2} & 4 \\ 2 & -2\sqrt{2} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \mathbf{0}, \left(\begin{pmatrix} a \\ b \end{pmatrix} \neq \mathbf{0} \right)$$

を解くと、

$$\begin{pmatrix} a \\ b \end{pmatrix} = k \begin{pmatrix} \sqrt{2} \\ 1 \end{pmatrix}$$

$\lambda = 3 - 2\sqrt{2}$ のとき

$$\begin{pmatrix} 2\sqrt{2} & 4 \\ 2 & 2\sqrt{2} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \mathbf{0}, \left(\begin{pmatrix} a \\ b \end{pmatrix} \neq \mathbf{0} \right)$$

を解くと、

$$\begin{pmatrix} a \\ b \end{pmatrix} = k \begin{pmatrix} \sqrt{2} \\ -1 \end{pmatrix}$$

$$\begin{pmatrix} \sqrt{2} & \sqrt{2} \\ 1 & -1 \end{pmatrix}^{-1} \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} \sqrt{2} & \sqrt{2} \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 3+2\sqrt{2} & 0 \\ 0 & 3-2\sqrt{2} \end{pmatrix}$$

$$\begin{aligned} \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}^n &= \begin{pmatrix} \sqrt{2} & \sqrt{2} \\ 1 & -1 \end{pmatrix} \begin{pmatrix} (3+2\sqrt{2})^n & 0 \\ 0 & (3-2\sqrt{2})^n \end{pmatrix} \begin{pmatrix} \sqrt{2} & \sqrt{2} \\ 1 & -1 \end{pmatrix}^{-1} \\ &= \frac{1}{2\sqrt{2}} \begin{pmatrix} \sqrt{2}(3+2\sqrt{2})^n & \sqrt{2}(3-2\sqrt{2})^n \\ (3+2\sqrt{2})^n & -(3-2\sqrt{2})^n \end{pmatrix} \begin{pmatrix} 1 & \sqrt{2} \\ 1 & -\sqrt{2} \end{pmatrix} \\ &= \begin{pmatrix} \frac{(3+2\sqrt{2})^n + (3-2\sqrt{2})^n}{2} & \frac{(3+2\sqrt{2})^n - (3-2\sqrt{2})^n}{2} \\ \frac{(3+2\sqrt{2})^n - (3-2\sqrt{2})^n}{2\sqrt{2}} & \frac{\sqrt{2}}{(3+2\sqrt{2})^n + (3-2\sqrt{2})^n} \end{pmatrix} \\ \therefore x &= \frac{(3+2\sqrt{2})^n - (3-2\sqrt{2})^n}{4\sqrt{2}} \end{aligned}$$

求める平方数はこの数の2乗である． x を小さいほうから並べると，

$$x = 1, 6, 35, 204, 1189, 6930, 40391, 235416, 1372105, 7997214, 46611179, \dots$$

である．

問題 2 三辺の長さが連続する整数で，面積も整数である三角形を小さい順に3つ求めよ．

[解] 三辺の長さを $n-1, n, n+1$ ，三辺の長さの和の半分を s ，面積を m とおくと，

$$\begin{aligned} s &= \frac{n-1+n+n+1}{2} = \frac{3n}{2} \\ s - (n-1) &= \frac{n+2}{2}, s - n = \frac{n}{2}, s - (n+1) = \frac{n-2}{2} \\ \therefore m &= \sqrt{\frac{3n^2(n+2)(n-2)}{16}} \\ \therefore 16m^2 &= 3n^2(n+2)(n-2) \end{aligned}$$

左辺は偶数なので n は偶数である（もし n が奇数なら右辺が奇数になってしまう）．また右辺は3の倍数なので m は3の倍数である．よって $n = 2a, m = 3b$ とおくと，

$$16 \times 9b^2 = 12a^2(2a+2)(2a-2)$$

$$\begin{aligned} \therefore 3b^2 &= a^2(a+1)(a-1) \\ &= a^4 - a^2 \end{aligned}$$

$$= \left(a^2 - \frac{1}{2}\right)^2 - \frac{1}{4}$$

$$\therefore 12b^2 = (2a^2 - 1) - 1$$

$$(2a^2 - 1)^2 - 3(2b)^2 = 1 \tag{8}$$

ここでペル方程式

$$x^2 - 3y^2 = 1$$

を解く．最小解は明らかに $(x, y) = (2, 1)$ であるので，一般解は一般解は $k \geq 1$ に対して

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}^k \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (9)$$

$k = 2$ のときは $(x, y) = (7, 4)$ で (8) を満たし，

$$(a, b) = (2, 2)$$

$$\therefore (m, n) = (4, 6)$$

k が 1 増えるごとに， x, y の偶奇が入れ替わるため（数学的帰納法により容易に証明できる），実際は

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}^{2j} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 7 & 12 \\ 4 & 7 \end{pmatrix}^j \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (10)$$

の解の中に求める解はある． $j = 2$ のとき $(x, y) = (97, 56)$, $(a, b) = (7, 28)$, $(m, n) = (14, 84)$ ， $j = 3$ のとき $(x, y) = (1351, 780)$, $(a, b) = (26, 390)$, $(m, n) = (52, 1170)$ でいずれも題意を満たす．

問題 3 (10) で与えられる (x, y) が，問題 2 の解を全て与えることを証明せよ．

[証明]

$$\begin{pmatrix} x_{2j} \\ y_{2j} \end{pmatrix} = \begin{pmatrix} 7 & 12 \\ 4 & 7 \end{pmatrix}^j \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}^{2j} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

とおくと，

$$\begin{aligned} x_{2j} + y_{2j}\sqrt{3} &= \left(2 + \sqrt{3}\right)^{2j} \\ &= \left\{ \left(2 + \sqrt{3}\right)^j \right\}^2 \\ &= \left(x_j + y_j\sqrt{3}\right)^2 \\ &= x_j^2 + 3y_j^2 + 2x_jy_j\sqrt{3} \end{aligned}$$

$x_j^2 - 3y_j^2 = 1$ なので

$$x_{2j} + y_{2j}\sqrt{3} = 2x_j^2 - 1 + 2x_jy_j\sqrt{3}$$

つまり， $a = x_j, b = x_jy_j$ とすれば，(8) を満たし，問題 2 の解の全てを与える．

[証明おわり]

ペル方程式の歴史

ペル方程式の一般的な解法は西洋ではウィリアム・ブランカーが発見した．しかし，オイラーはこの方程式を研究したのはジョン・ペルであると誤解し「ペル方程式」と命名したため，その名前が広く使われるようになった*1．1000 年ほどさかのぼること 628 年にはインドのブラーマグプタが『ブラーマ・スプタ・シッターンタ』において $x^2 - 92y^2 = 1$ の最小自然数解 $(x, y) = (1151, 120)$ を示している．また 12 世紀にはバースカラ II が研究している．西洋で最初にこの問題を提示したのはフェルマーであり，ラーンが出版したときにペルが助けたのでペルの研究だとオイラーが勘違いしたためだといわれている．18 世紀にラグランジュが連分数展開による一般解を求めた．

*1 参考文献 [3]

直接ペル方程式を提示したわけではないが、アルキメデスの考えたと言われている「家畜の問題」はつきつめるとペル方程式に帰着する．それは

$$x^2 - 4729949y^2 = 1$$

で，最小解は 206545 桁であるそうである．

参考文献

- [1] 芹沢正三 『数論入門』(講談社ブルーバックス, 2008 年)
- [2] 加藤和也, 黒川信重, 齋藤毅 『数論 1』(岩波書店, 1996 年)
- [3] 「私的数学塾」http://www004.upp.so-net.ne.jp/s_honma/
- [4] 「ウィキペディア」<<http://ja.wikipedia.org/wiki/>>
- [5] 「Wikipedia」<<http://en.wikipedia.org/wiki/>>
- [6] ガスコン研究所「コマネチ大学数学科 91 講：ペル方程式」
<http://gascon.cocolog-nifty.com/blog/2008/05/91_a088.html>