割り算を活用して特殊解を求める際の注意

この資料では特殊解を求める際に, 線形代数を活用することで見えてくる事実とそれを踏まえた問題を解く際の検算の視点について述べる. $a, b \in \mathbb{Z}$, $a \neq 0, b \neq 0$, $\gcd(a, b) = 1$ に対し, 不定方程式

$$ax + by = 1$$

を考えてみよう. 例えば $a > 0, b < 0$ のとき,

$$ax + by = ax + (-b)(-y)$$

のように考え, $X = x, Y = -y$ と置き直すことで $aX + (-b)Y = 1$ という自然数係数の方程式に変換できるため, あらかじめ $a, b \in \mathbb{N}$ と仮定しても一般性は失わない[1]. さて $a = bq + r, 0 \leqslant r < b$ と割り算を行うと, 方程式は次のように変形される.

$$ax + by = (bq + r)x + by = b(qx + y) + rx$$

よって, $u = qx + y, v = x$ と置き直すと, $ax + by = bu + rv$ となる. 行列を用いれば

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

となる.

$$P = \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix}$$

とおけば,

$$\begin{pmatrix} u \\ v \end{pmatrix} = P \begin{pmatrix} x \\ y \end{pmatrix}$$

となる. この操作を繰り返す.

$$\begin{aligned}
&b = rq_1 + r_1, \quad 0 \leqslant r_1 < r, \\
&r = r_1 q_2 + r_2, \quad 0 \leqslant r_2 < r_1 \\
&r_1 = r_2 q_3 + r_3, \quad 0 \leqslant r_3 < r_2 \\
&\cdots \\
&r_{n-2} = r_{n-1} q_n + r_n, \quad 0 \leqslant r_n < r_{n-1}
\end{aligned}$$

のように割り算を続けていくことで, 式は $r_{n-1}s + r_n t = ax + by$,

$$\begin{pmatrix} s \\ t \end{pmatrix} = P_n P_{n-1} \cdots P_1 P \begin{pmatrix} x \\ y \end{pmatrix}$$

[1] $\gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b)$ となることにも注意.

となる．ここで

$$P_j = \begin{pmatrix} q_j & 1 \\ 1 & 0 \end{pmatrix}$$

である．ここで $\det P = q \cdot 0 - 1 \cdot 1 = -1$, $\det P_j = q_j \cdot 0 - 1 \cdot 1 = -1$ となることに注目すると[2]，

$$P^{-1} = \frac{1}{\det P}\begin{pmatrix} 0 & -1 \\ -1 & q \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix},\ P_j^{-1} = \frac{1}{\det P_j}\begin{pmatrix} 0 & -1 \\ -1 & q_j \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_j \end{pmatrix}$$

となる．

$$\begin{pmatrix} s \\ t \end{pmatrix} = P_n P_{n-1} \cdots P_1 P \begin{pmatrix} x \\ y \end{pmatrix}$$

から

$$\begin{pmatrix} x \\ y \end{pmatrix} = P^{-1} P_1^{-1} \cdots P_{n-1}^{-1} P_n^{-1} \begin{pmatrix} s \\ t \end{pmatrix}$$

が得られることに注意すると, $s, t \in \mathbb{Z}$ なら P^{-1}, P_j^{-1} $(1 \leqslant j \leqslant n)$ が整数を成分とする行列であることから $x, y \in \mathbb{Z}$ となる．よって不定方程式 $r_{n-1}s + r_n t = 1$ の解 $s, t \in \mathbb{Z}$ を求められれば, 連立方程式を解いて得られる x, y も必ず整数となる．

さらに $\det P_n \det P_{n-1} \cdots \det P_1 \det P = (-1)^{n+1}$ となることから,

$$\begin{pmatrix} s \\ t \end{pmatrix} = P_n P_{n-1} \cdots P_1 P \begin{pmatrix} x \\ y \end{pmatrix} = M \begin{pmatrix} x \\ y \end{pmatrix}$$

$(M = P_n P_{n-1} \cdots P_1 P)$ と行列で変数変換を表した際, $\det M$ は 1 または -1 となる[3]．以上をまとめると, 割り算を活用した不定方程式の解法を考える際, 次の検算の視点が得られる．

- 割り算を繰り返して得られた簡単な不定方程式を解いて得られた整数解から連立方程式を解くと必ず整数解が得られる．よって, 整数解が得られなかった場合は, 割り算を繰り返して方程式を変形していく際どこかで計算ミスをしていることになる．
- 変数変換を表す行列の行列式は必ず 1 か -1 になる．よって行列式を計算してこのような値にならなかった場合もどこかで計算ミスをしていることになる．

▶ **例 1.** 教科書 p.155 例 10 では $177x + 52y = 1$ という方程式は $177x + 52y = 21(7x + 2y) + 10(3x + y) = 21m + 10n$ $(m = 7x + 2y, n = 3x + y)$ となることから $21m + 10n = 1$

[2] 行列 A に対して $\det A$ で A の行列式を表す．

[3] ここで行列式の性質 $\det AB = \det A \det B$ を使っている．

と変形できた．$m=1, n=-2$ という解はすぐ見つかるから連立方程式

$$\begin{pmatrix} 1 \\ -2 \end{pmatrix} = \begin{pmatrix} 7 & 2 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

を解くことで, $x=5, y=-17$ という整数解が得られた．この $x, y \in \mathbb{Z}$ となる性質は上に述べた解説から従う．さらに

$$\begin{pmatrix} 1 \\ -2 \end{pmatrix} = \begin{pmatrix} 7 & 2 \\ 3 & 1 \end{pmatrix}$$

の行列式を計算してみると $7 \cdot 1 - 2 \cdot 3 = 1$ となっている．これも上に述べた解説と整合している．