

ディオファントスの方程式

Diophantine equation

問題 1 一次不定方程式

$$17x + 23y = 1 \quad (x, y \in \mathbb{Z}) \quad (1)$$

を解け.

[解]

$$17(x + y) + 6y = 1$$

より

$$\begin{cases} x_1 = x + y \\ y_1 = y \end{cases}$$

と変数を変換することにより次の方程式になる.

$$17x_1 + 6y_1 = 1 \quad (2)$$

同様に

$$5x_1 + 6(2x_1 + y_1) = 1$$

より

$$\begin{cases} x_2 = x_1 \\ y_2 = 2x_1 + y_1 \end{cases}$$

と変換して,

$$5x_2 + 6y_2 = 1 \quad (3)$$

$$5(x_2 + y_2) + y_2 = 1$$

より

$$\begin{cases} x_3 = x_2 + y_2 \\ y_3 = y_2 \end{cases}$$

と変換して

$$5x_3 + y_3 = 1 \quad (4)$$

ここで

$$(x_3, y_3) = (0, 1)$$

という解を得る. ここで変数変換を遡って,

$$\begin{cases} x_3 = 0 \\ y_3 = 1 \end{cases} \Rightarrow \begin{cases} x_2 = -1 \\ y_2 = 1 \end{cases} \Rightarrow \begin{cases} x_1 = -1 \\ y_1 = 3 \end{cases} \Rightarrow \begin{cases} x = -4 \\ y = 3 \end{cases}$$

つまり

$$(x, y) = (-4, 3)$$

という解を得る．これは確かに (1) を満たしている．もし答が合わないときは途中の (2)(3) で検算を行えばどこで間違えたかわかる．また,

$$17x + 23y = 0$$

の解は

$$(x, y) = (23k, -17k) \quad (k \in \mathbb{Z})$$

が全てであるので, (1) の一般解は

$$(x, y) = (-4 + 23k, 3 - 17k) \quad (k \in \mathbb{Z})$$

である．

このように一次不定方程式を解く方法は確立している．この方法はユークリッドの互除法にほかならない．つまり最大公約数を求める計算に等しい．上の (4) の式が解をもつためには 17 と 23 の公約数が 1 であることが必要である．このことから次のことが言える．

定理 1 一次不定方程式

$$ax + by = 1 \tag{5}$$

が解をもつことは $(a, b) = 1$ であることが必要十分である．

[証明略] 必要条件であることは問題から容易に理解できる．また変数変換は全て可逆なので十分であることもいえる．

また $(a, b) = 1$ のとき

$$ax + by = k \tag{6}$$

の解は (5) の解を全て k 倍すればよいので容易である．さらに次の定理が成り立つ．

定理 2 一次不定方程式

$$ax + by = k \tag{7}$$

が解をもつことは k が (a, b) の倍数であることが必要十分である．

[証明略] (7) の両辺を (a, b) で割ってやれば, a, b が互いに素の場合の (6) になるので当然である．

さて, 問題 1 の解の途中の変数変換は全て一次変換であるので行列で表すこともできる．つまり

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

逆行列をかけることにより

$$\begin{aligned} \begin{pmatrix} x \\ y \end{pmatrix} &= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} -1 \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 \\ 3 \end{pmatrix} \\ &= \begin{pmatrix} -4 \\ 3 \end{pmatrix} \end{aligned} \tag{8}$$

(8) の行列は x の係数で y の係数を割った商が Q_x であるとき

$$\begin{pmatrix} 1 & -Q_x \\ 0 & 1 \end{pmatrix}$$

を, y の係数で x の係数を割った商が Q_y であるとき

$$\begin{pmatrix} 1 & 0 \\ -Q_y & 1 \end{pmatrix}$$

を左から順番にかけてゆけばいいのである. このようにすれば多少機械的に解くことができる.

問題 2 不定方程式を解け

$$113x + 39y = 3$$

[解] 順に

$$113x + 39y = 3$$

$$35x + 39y = 3$$

$$35x + 4y = 3$$

$$3x + 4y = 3$$

$$(x, y) = (1, 0)$$

$$\begin{aligned} \begin{pmatrix} x \\ y \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -8 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ -8 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 9 \\ -8 \end{pmatrix} \\ &= \begin{pmatrix} 9 \\ -26 \end{pmatrix} \end{aligned}$$

一般解は

$$(x, y) = (9 + 39k, -26 - 113k)$$

変数変換は必ずしも最後までやる必要はない. 答が出た時点でやめればよい. また互除法の商や余りは必ずしも正の数にする必要はない. 次のように負になってもかまわない. その方が一般的には早い.

$$113x + 39y = 3$$

$$-4x + 39y = 3$$

$$-4x - y = 3$$

$$(x, y) = (0, -3)$$

$$\begin{aligned} \begin{pmatrix} x \\ y \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 10 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ -3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix} \begin{pmatrix} -30 \\ -3 \end{pmatrix} \\ &= \begin{pmatrix} -30 \\ 87 \end{pmatrix} \end{aligned}$$

あるいは途中でやめないで本当の最後までやっても良い.

$$\begin{aligned}113x + 39y &= 3 \\ -4x + 39y &= 3 \\ -4x - y &= 3 \\ 0x - y &= 3 \\ (x, y) &= (k, -3)\end{aligned}$$

$$\begin{aligned}\begin{pmatrix} x \\ y \end{pmatrix} &= \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 10 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix} \begin{pmatrix} k \\ -3 \end{pmatrix} \\ &= \begin{pmatrix} -39 & 10 \\ 113 & -29 \end{pmatrix} \begin{pmatrix} k \\ -3 \end{pmatrix}\end{aligned}$$

こうすると一般解まで求めることができる. しかしこの方法で得た答が果たして一般解と言えるか. つまり解の全てを本当に網羅しているのかという証明はここでは与えていない.

問題 3 一次不定方程式

$$32x + 57y - 68z = 1 \tag{9}$$

を解け.

[解] 順に

$$\begin{aligned}32x + 57y - 68z &= 1 \\ 32x - 7y - 4z &= 1 \\ y - 4z &= 1 \\ y &= 1 \\ (x, y, z) &= (s, 1, t)\end{aligned}$$

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 1 & -2 & 2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 8 & -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} s \\ 1 \\ t \end{pmatrix} \tag{10}$$

$$= \begin{pmatrix} 17 & -6 & -22 \\ 0 & 1 & 4 \\ 8 & -2 & -7 \end{pmatrix} \begin{pmatrix} s \\ 1 \\ t \end{pmatrix} \tag{11}$$

x の係数で y, z の係数を割ったときの商を Q_y, Q_z とすると, 変数変換を表す行列は

$$\begin{pmatrix} 1 & Q_y & Q_z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

他の場合も同様に,

$$\begin{pmatrix} 1 & 0 & 0 \\ Q_x & 1 & Q_z \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ Q_x & Q_y & 1 \end{pmatrix}$$

で表せる．これらの逆行列は

$$\begin{pmatrix} 1 & -Q_y & -Q_z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ -Q_x & 1 & -Q_z \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -Q_x & -Q_y & 1 \end{pmatrix}$$

なのでこれらをかけていったのが (10) である．

問題 4 連立一次不定方程式

$$\begin{cases} 32x + 57y - 68z = 1 \\ 3x + 2y - 6z = 2 \end{cases} \quad (12)$$

$$(13)$$

を解け．

[解] (13) より,

$$(3 \quad 2 \quad -6) \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 2$$

(11) より

$$(3 \quad 2 \quad -6) \begin{pmatrix} 17 & -6 & -22 \\ 0 & 1 & 4 \\ 8 & -2 & -7 \end{pmatrix} \begin{pmatrix} s \\ 1 \\ t \end{pmatrix} = 2$$

$$(3 \quad -4 \quad -16) \begin{pmatrix} s \\ 1 \\ t \end{pmatrix} = 2$$

つまり

$$3s - 16t = 6$$

という新たな不定方程式を得る．

$$3s - t = 6$$

$$-t = 6$$

より

$$\begin{aligned} \begin{pmatrix} s \\ t \end{pmatrix} &= \begin{pmatrix} 1 & 5 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} u \\ -6 \end{pmatrix} \\ &= \begin{pmatrix} 16 & 5 \\ 3 & 1 \end{pmatrix} \begin{pmatrix} u \\ -6 \end{pmatrix} \end{aligned}$$

これを (11) に代入して

$$\begin{aligned} \begin{pmatrix} x \\ y \\ z \end{pmatrix} &= \begin{pmatrix} 17 & -6 & -22 \\ 0 & 1 & 4 \\ 8 & -2 & -7 \end{pmatrix} \begin{pmatrix} 16 & 0 & 5 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{pmatrix} \begin{pmatrix} u \\ 1 \\ -6 \end{pmatrix} \\ &= \begin{pmatrix} 206 & -6 & 63 \\ 12 & 1 & 4 \\ 107 & -2 & 33 \end{pmatrix} \begin{pmatrix} u \\ 1 \\ -6 \end{pmatrix} \\ &= \begin{pmatrix} 206u - 384 \\ 12u - 23 \\ 107u - 200 \end{pmatrix} \end{aligned}$$

ディオファントス (Diophantus of Alexandria)

3 世紀，古代ギリシアの数学者．生没年はわからないが，ディオファントスの墓碑銘の問題により 84 歳まで生きたと言われる．墓は発見されていない．エジプトのアレクサンドリアに住んでいたこと以外，彼の生涯について全くわかっていない．紀元前 5 世紀～3 世紀はピタゴラス，ユークリッド，アルキメデス，アポロニウスに代表されるギリシャ数学の全盛期であった．しかしその後衰退し，ディオファントス，パップスによって一時復興する．『算術』（あるいは「数論」）13 巻を著した．『算術』はユークリッドの『原論』のような，定義，命題，証明という形式をとらず，問題の形で書かれている．フェルマーが余白にフェルマーの定理を含む書き込みをしたのはこの『算術』である．

参考文献

- [1] 高木貞治『初等整数論講義第 2 版』（共立出版社，1997 年）
- [2] 小林昭七『なっとくするオイラーとフェルマー』（講談社，2003 年）