# 油分け算と一次不定方程式

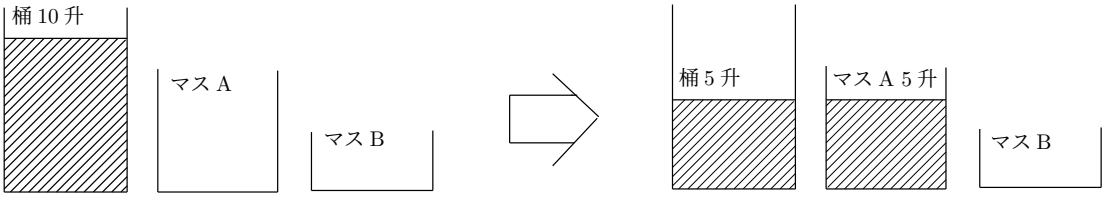
平成 23 年度第 2 回キトキト数学　資料
平成 23 年 12 月 23 日
片山　喜美

## 1　ある油分け算の問題について

平成 23 年 10 月 22 日の富山新聞に、和算に関する記事があることを、杉山先生（富山県教育委員会生涯学習・文化財室）に教えていただいた。その中に、富山中部高等学校探求科学科 1 年生のグループが、強度学習で和算に取り組んでおり、以下の「油分け算」に挑戦したという記述があった。

問題 1

桶に 10 升の油が入っています。7 升マスと 3 升マスの 2 つのマスを使って 5 升ずつに分けなさい。




### 1.1　不定方程式の解とマスの油の移動

この問題は、あれこれ試行錯誤しているうちに解けるに違いない。まあそれでいいのだが、ここでは、一次不定方程式 $7x+3y=5 \quad (x,y\in\mathbb{Z})$ に結びつけて考えてみる。基本となるのは次の命題である。

命題 1
$a,b$ が互いに素な自然数の時、$^{\exists}x,y\in\mathbb{Z} \quad$ s.t. $ax+by=1$

この命題の証明は後回しにする。この命題が成り立つことを認めれば、$a,b$ が互いに素な自然数の時、任意の整数 $n$ について、$^{\exists}x,y\in\mathbb{Z} \quad$ s.t. $ax+by=n \quad$ とできる。

$7x+3y=5$ については、7 と 3 が互いに素であり、例えば $7\times1+3\times(-2)=1$ が簡単に分かるので、

$$7\times5+3\times(-10)=5 \tag{1}$$

とできる。次に、その他の解について考えるのだが

$$7x+3y=5 \tag{2}$$

とおいて、$(2)-(1)$ より、$7(x-5)=-3(y+10)$
この式の両辺の値は 21 で割り切れるから、その値を $=21N \quad (N\in\mathbb{Z})$ とおいて、

$$x=5+3N, \quad y=-10-7N \tag{3}$$

これが不定方程式 $7x+3y=5$ の一般解を与える。
それらの解の中で、小さなものについて考えてみる。

(1) $N=-1$ のとき

$x=2, y=-3$ となるので、$7\times 2-3\times 3=5$ 。これを元に、7 升マスと 3 升マスを用いた油分け算の解法を考える。「7 升マスに 2 回入れ、3 升マスから 3 回取り出す」を実現する方針で考えていくのである。

桶、7 升マス、3 升マスの水の量が $k$ 升、$l$ 升、$m$ 升の状態を $(k,l,m)$ で表す。

ただし、$0\leqq k\leqq 10,\quad 0\leqq l\leqq 7,\quad 0\leqq m\leqq 3$ とする。はじめの状態は、$(10,0,0)$ である。

$(10,0,0)\longrightarrow (3,7,0)_{x=1}\longrightarrow (3,4,3)\longrightarrow (6,4,0)_{y=-1}\longrightarrow (6,1,3)\longrightarrow (9,1,0)_{y=-2}\longrightarrow (9,0,1)\longrightarrow (2,7,1)_{x=2}\longrightarrow (2,5,3)\longrightarrow (5,5,0)_{y=-3}$ これで終了。

(2) $N=-2$ のとき

$x=-1, y=4$ となるので　$7\times(-1)+3\times 4=5$

従って、3 升マスに油を満たし、7 升マスに移すことを 4 回やればよい。

$(10,0,0)\longrightarrow (7,0,3)_{y=1}\longrightarrow (7,3,0)\longrightarrow (4,3,3)_{y=2}\longrightarrow (4,6,0)\longrightarrow (1,6,3)_{y=3}\longrightarrow (1,7,2)\longrightarrow (8,0,2)_{x=-1}\longrightarrow (8,2,0)\longrightarrow (5,2,3)_{y=4}\longrightarrow (5,5,0)$ これで終了。

このように、一次不定方程式 $7x+5y=5$ の 2 つの特殊解から、それぞれに対応する油の移動方法を導くことができる。この不定方程式には無数の整数解が存在し、それに対応する油の移動方法がある。しかし、解 $x, y$ の絶対値が大きければ、対応する油の移動回数は大きくなる。そして、その途中で 5 升ずつの状態が生じてしまっているはずである。従って、手数の短いものは上記の 2 つになるのであろう。

練習問題　次の油分け算を解きなさい.

(1) 桶に 8 升の油があり、それを 5 升マスと 3 升マスを使って、4 升ずつに分ける。

(2) 桶に 18 升の油があり、それを 11 升マスと 7 升マスを使って、9 升ずつに分ける。

# 2　一次不定方程式

命題 1 について、2 通りの証明を与える。

## 2.1　命題 1 の証明　その 1（集合を考える方法）

$M=\{ax+by \quad | \quad x,y\in\mathbb{Z}\}$ とおく。

- $0\in M$

  $\because) 0=a\cdot 0+b\cdot 0$

- $m,n\in M\Longrightarrow m-n\in M$　（減法について閉じている）

  $\because)\quad m=ax_1+by_1,\quad n=ax_2+by_2\quad\Longrightarrow m-n=a(x_1-x_2)+b(y_1-y_2)\in M//$

- $m,n\in M\Longrightarrow m+n\in M$　（加法について閉じている）

  $\because)$ $0, m\in M$ のとき、$-n=0-n\in M$ 。従って、$m+n=m-(-n)\in M//$

- $m\in M\Longrightarrow^{\forall} l\in\mathbb{Z}, lm\in M$

  $\because)$　上に示したことより、$(l-1)m, m\in M$ が言えたら、$lm=(l-1)m+m\in M$ と帰納的に示される。//

- $M$ に含まれる正の整数で最小のものを $d$ とすると、$M=d\mathbb{Z}$ である。($M$ は最小正の数 $d$ の整数倍全体である。)

$\because$) $^{\forall}m \in M.\ \ ^{\exists}q, r \in \mathbb{Z}, 0 \leqq r < d \quad s.t. \quad m = qd + r$ とできる。
$m, qd \in M$ より、$r = m - qd \in M$ である。もし、$r > 0$ ならば、それは $M$ に含まれる正の整数で、$d$ よりも小さくなるので、$d$ を正の整数で最小のものとして取ったことに反する。従って、$r = 0$ で、$m = qd$ となる。//

- $(a, b) = 1$ のとき、 $d = 1$ である。
$\because$) $a = a \cdot 1 + b \cdot 0, \quad b = a \cdot 0 + b \cdot 1$ であるから、$a, b \in M$ である。よって、$a, b$ はいずれも、$d$ の倍数である。言い換えると、$d$ は $a, b$ の公約数である。しかるに、$a, b$ は互いに素であったから、$d = 1$ となる。//

- 以上から、$1 \in M$ 、すなわち、$^{\exists}x, y \in M \quad s.t. \quad ax + by = 1$ （命題１の証明終わり）

## 2.2 命題１の証明　その２（ユークリッドの互除法）

$a, b$ が互いに素である場合に限らず、最大公約数を $(a, b) = d$ として、以下で $d$ を求めていく計算の手順を考える。さらに、その計算の手順を逆にたどることで、$ax + by = d$ をみたす整数 $x, y$ が存在することについて述べる。特に、$d = 1$ の場合が命題１になるのである。

- $^{\exists}q, r \in \mathbb{Z} \quad s.t. \quad a = qb + r \quad (0 \leqq r < b)$ とできるが、このとき、$(a, b) = (b, r)$ である。
$\because$) $(b, r) = d'$ とおく。また、整数 $k$ が整数 $l$ を割り切ることを $k|l$ と表すことにする。
まず、 $d|a$ かつ $d|b$ であるから、$d|(a - qb)$ 。従って、$d|r$ 。$d|b$ かつ $d|r$ が言えたから、$d$ は $b, r$ の公約数であり、最大公約数 $d'$ と比べて、$d \leqq d'$ 。
一方、$d'|b$ かつ $d'|r$ であるから、$d'|(qb + r)$ 。従って、$d|a$ 。これから $d'$ は $a, b$ の公約数であり、$d' \leqq d$ が言える。
以上により、$d = d'$ //

- 数列 $\{q_i\}$, $\{r_i\}$ を以下のように定めていく。
まず、$r_0 = a, r_1 = b$ とおく。次に、$a = qb + r \quad (0 \leqq r < b)$ をみたす整数 $q, r$ を考えて、$q_1 = q, r_2 = r$ とおく。
$r_0, r_1, \cdots, r_i$, 及び $q_1, q_2, \cdots, q_{i-1}$ が定まったとき、$r_{i-1} = q_i r_i + r_{i+1} \quad (0 \leqq r_{i+1} < r_i)$ をみたすように $q_i$ 及び $r_{i+1}$ を定めていく。その作業は有限回で終了する。
例えば、$a = 79, b = 31$ として、具体的に計算してみる。
$r_0 = 79, r_1 = 31$
$79 = 2 \times 31 + 17 \quad \therefore q_1 = 2 \quad r_2 = 17$
$31 = 1 \times 17 + 14 \quad \therefore q_2 = 1 \quad r_3 = 14$
$17 = 1 \times 14 + 3 \quad \therefore q_3 = 1 \quad r_4 = 3$
$14 = 4 \times 3 + 2 \quad \therefore q_4 = 4 \quad r_5 = 2$
$3 = 1 \times 2 + 1 \quad \therefore q_5 = 1 \quad r_6 = 1$
$2 = 2 \times 1 + 0 \quad \therefore q_6 = 2 \quad r_7 = 0$
ここで、$r_1 > r_2 > \cdots > r_6 > r_7 = 0$ と減少し、$r_7 = 0$ になった時点で割り算の商とその余りを求めていく操作が終了する。
一般の場合も、作り方から $r_1 > r_2 > \cdots$ と減少し、あるところで $r_k > r_{k+1} = 0$ となるので、その時点で割り算の商と余りを求める操作が終了する。

- 上記のような操作で、$r_{k+1} = 0$ となるとき、$(a, b) = r_k$ である。
$\because$) 帰納的に $(a, b) = (r_{i-1}, r_i)$ が成り立つ。
従って、$(a, b) = (r_1, r_2) = \cdots\cdots = (r_{k-1}, r_k) = (r_k, r_{k+1}) = (r_k, 0) = r_k$ //
この手順を**「ユークリッドの互除法」**という。

- 上記のユークリッドの互除法を逆にたどってみる。
注意. $r_6 = 1, r_7 = 0$ より、$(79, 31) = 1$ である。この最大公約数 1 を 79 と 31 を用いて表すことを考

える。

$3 = 1 \times 2 + 1 \quad \Longrightarrow \quad 1 = 3 - 1 \times 2$

$2 = 14 - 4 \times 3 \quad \Longrightarrow \quad 1 = 3 - 1 \times (14 - 4 \times 3) = -1 \times 14 + 5 \times 3$

$3 = 17 - 1 \times 14 \quad \Longrightarrow \quad 1 = -1 \times 14 + 5 \times (17 - 1 \times 14) = 5 \times 17 - 6 \times 14$

$14 = 31 - 1 \times 17 \quad \Longrightarrow \quad 1 = 5 \times 17 \times -6 \times (31 - 1 \times 17) = -6 \times 31 + 11 \times 17$

$17 = 79 - 2 \times 31 \quad \Longrightarrow \quad 1 = -6 \times 31 \times +11 \times (79 - 2 \times 31) = 11 \times 79 - 28 \times 31$

$\therefore \ 79 \times 11 + 31 \times (-28) = 1$

一般の場合についても、互除法が $r_{k+1} = 0$ で終了するとき、

$d = r_k = r_{k-2} - q_{k-1} r_{k-1}$

$= r_{k-2} - q_{k-1}(r_{k-3} - q_{k-2} r_{k-2}) = -q_{k-1} r_{k-3} + (1 + q_{k-1} q_{k-2}) r_{k-2} = \cdots\cdots$

と計算を続けていき、$d$ を $r_0, r_1$ で表すことができる。すなわち、 $d = ax + by$ の形で表すことができる。（証明終）

## 2.3 ユークリッドの互除法による一次不定方程式の解の計算について

ユークリッドの互除法による $ax + by = d$ の解 $x, y$ の効率的な計算方法を少し考えておく。

$r_{i-1} = q_i r_i + r_{i+1}$ を行列で表して、

$$\begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix} = \begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} \quad (i = 1, 2, \cdots\cdots, k-1)$$

であるから

$$\begin{pmatrix} r_0 \\ r_1 \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_2 \\ r_3 \end{pmatrix} = \cdots\cdots = \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_2 & 1 \\ 1 & 0 \end{pmatrix} \cdots\cdots \begin{pmatrix} q_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix}$$

ここで、

$$\begin{pmatrix} q_i & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \quad (i = 1, 2, \cdots\cdots, k-1)$$

であるから、上式を逆に解いて、

$$\begin{pmatrix} r_{k-1} \\ r_k \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{k-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{k-2} \end{pmatrix} \cdots\cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} r_0 \\ r_1 \end{pmatrix}$$

$a = 79, b = 31$ のときは、$q_1 = 2$, $q_2 = 1$, $q_3 = 1$. $q_4 = 4$, $q_5 = 1$ で、$d = r_6 = 1$, $r_5 = 2$ であったから、

$$\begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \cdots\cdots \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 79 \\ 31 \end{pmatrix} = \begin{pmatrix} -9 & 23 \\ 11 & -28 \end{pmatrix} \begin{pmatrix} 79 \\ 31 \end{pmatrix}$$

従って、$1 = 79 \cdot 11 + 31 \cdot (-28)$ を得る。

練習問題　次の $a, b$ について、最大公約数 $d$ を求め、 $ax + by = d \quad (x, y \in \mathbb{Z})$ の解を求めよ。

(1) $a = 123, b = 53$　　(2) $a = 476, b = 221$

## 2.4 多項式の最大公約数のユークリッドの互除法による計算について

ユークリッドの互除法は、多項式についても同様に適用できる。

例えば、$f(x) = x^3 - 3x + 1$, $g(x) = x^2 - 2$ のとき、

$r_0(x) = x^3 - 3x + 1, r_1(x) = x^2 - 2$ から始めて、

$x^3 - 3x + 1 = x(x^2 - 2) + (-x + 1) \quad \therefore q_1(x) = x \qquad r_2(x) = -x + 1$

$x^2 - 2 = (-x - 1)(-x + 1) - 1 \qquad \therefore q_2(x) = -x - 1 \quad r_3(x) = -1$

従って、

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

これから、$-1 = (x^3-3x+1)(x+1) + (x^2-2)(-x^2-x+1)$ 、すなわち、$x^3-3x+2$ と $x^2-2$ は互いに素で、$(x^3-3x+1)(-x-1) + (x^2-2)(-x^2-x+1) = 1$ と表すことができる。

さらに、$\alpha$ が方程式 $x^3-3x+1=0$ の解であるとき、上式に $\alpha$ を代入して　$(\alpha^3-3\alpha+1)(-\alpha-1) + (\alpha^2-2)(-\alpha^2-\alpha+1) = 1$

従って、$\dfrac{1}{\alpha^2-2} = -\alpha^2-\alpha+1$ となる。

このように考えると、方程式の解 $\alpha$ の有理関数をすべて $\alpha$ の多項式に直すことができることがわかる。

練習問題１　$f(x) = x^4+4x^3+x^2-13x-14$, $g(x) = x^3+16x^2+12x+8$ の最大公約数 $d(x)$ を求めよ。また、$f(x)k(x)+g(x)l(x) = d(x)$ をみたす多項式 $k(x)$, $l(x)$ を求めよ。

練習問題２　$\alpha$ が方程式 $x^3+3x^2-1=0$ の解であるとき、$\dfrac{1}{\alpha^2+\alpha+2}$ を $\alpha$ の多項式で表せ。

# 3　桶に油を戻さない油分け算と一次不定方程式

## 3.1　桶に油を戻さない油分け算

次のような問題を考えてみる。

問題２

桶には、油がたっぷり入っています。蛇口から７升マスもしくは３升マスに取り出して計り、別の容器に入れます。ただし、取り出した油は元の桶に戻さないものとします。どのような量の油を取り出すことができ、どのような量の油を取り出すことができないか、答えなさい。

この条件では、1 升、2 升の油を計ることができない。3 升は計れるが、4 升、5 升は無理である。そして、ある程度大きな量ならすべて計れそうである。そこで、有限個の計れない量を見つけること、ある量から先は計れること、の 2 つの事実を示せばよい。

この問題は、$7x+3y$　$(x, y \in \mathbb{Z},\quad x, y \geqq 0)$ で表すことができる整数、できない整数を考えることと同じである。

$0 \leqq x \leqq 3$, $0 \leqq y \leqq 7$ について、$7x+3y$ の値を考えてみる。

| $x \setminus y$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 3 | 6 | 9 | 12 | 15 | 18 | 21 |
| 1 | 7 | 10 | 13 | 16 | 19 | 22 | 25 | 28 |
| 2 | 14 | 17 | 20 | 23 | 26 | 29 | 32 | 35 |
| 3 | 21 | 24 | 27 | 30 | 33 | 36 | 39 | 42 |

この表では、32 個の整数が並んでいるが、そのうち重複しているのは 21 のみである。($21 = 7\cdot3+3\cdot0 = 7\cdot0+3\cdot3$)

従って、31 通りの数を表している。上の表の中に出てこない数を以下でアンダーラインを引いてみる。

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 | 42 |

- 1〜42 までの整数のうち $7x+3y$ で表すことができていないのは、まず、1,2,3,5,8,11 で、その後しばらくは、すべて表すことができる。そして、31,34,37,38,40,41 にアンダーラインが引かれている。

- 31,34,37,38,40,41 については、それより 3 だけ少ない数が $7x+3y$ で表すことができていることから、その $y$ の値を 1 だけ加えたものを用いて表すことができる。(表では、$28=7\cdot1+3\cdot7$ として現れているが、その $y$ を 1 だけ増やして、$31=7\cdot1+3\cdot8$ など)
  しかしながら、1,2,3,5,8,11 については、$x,y\geqq0$ の条件では表すことができない。

- 以上により、問題 2 の解答は「計ることができない量は 1,2,3,5,8,11 升で、それ以外はすべて計ることができる」となる
  なお、12 升以上についてすべて計ることができる事については、

  - 12,13,14 が $7x+3y\quad(x,y\in\mathbb{Z},\quad x,y\geqq0)$ で表すことができる。
  - $k,k+1,k+2$ の連続する 3 数を表すことができたとすると、そのときの $y$ の値を 1 ずつ増やして、その次の連続する 3 数 $k+3,k+4,k+5$ も表すことができる。

  ということから、帰納的に示される。

## 3.2 一次不定方程式で表せない自然数の個数について

先に調べたとおり、$7x+3y\quad(x,y\in\mathbb{Z},\quad x,y\geqq0)$ で表すことができない自然数の個数は 6 個であった。一般に、$a,b$ が互いに素であるとき $ax+by\quad(x,y\geqq0)$ で表すことができない自然数の個数について、次の命題が成り立つ。

**命題 2**
$a,b$ が互いに素な自然数の時、$ax+by\quad(x,y\in\mathbb{Z},\quad x,y\geqq0)$ で表すことができない自然数の個数は $\dfrac{1}{2}(a-1)(b-1)$ である。

この命題の証明をいくつかの補題に分けて行う。

補題 1　$a,b$ が互いに素な自然数であるとき、$ax+by\quad(x,y\in\mathbb{Z},\quad 0\leqq x\leqq b,\ 0\leqq y\leqq a)$ で表すことができる相異なる整数は、$(a+1)(b+1)-1$ 通りである。

$\because$) $ax_1+by_1=ax_2+by_2$ が成り立つとすると、$a(x_1-x_2)=b(y_2-y_1)$ 。$(a,b)=1$ であるから、$x_1-x_2$ は $b$ の倍数であり、かつ $y_2-y_1$ は $a$ の倍数である。$x_1\geqq x_2$ とすると、$0\leqq x_1-x_2\leqq b$ であるから、$x_1-x_2=0$ もしくは $x_1-x_2=b$

$x_1-x_2=0\implies y_2-y_1=0\quad\therefore(x_1,y_1)=(x_2,y_2)$

$x_1-x_2=b\implies y_2-y_1=a\quad$ このとき、$(x_1,y_1)=(b,0),\ (x_2,y_2)=(0,a)$

従って、$(x,y)$ の $(a+1)(b+1)$ 通りの取り方の中で、$ax+by$ の値が重複するのは、$a\cdot b+b\cdot0=a\cdot0+b\cdot a=ab$ の時のみである。$\therefore$相異なる $(a+1)(b+1)-1$ 通りの数を表す。//

補題 2　$ax+by\quad(x,y\geqq0)$ により、$ab$ 以上の値をすべて表すことができる。

$\because$) $ab$ 以上の整数は、$ab+k\quad(k\geqq0)$ と表すことができる。

このとき、$^{\exists}l_0,m_0\in\mathbb{Z}\quad s.t.\quad al_0+bm_0=k$

$al+bm=k$ を満たすとき、これらを差し引いて、$a(l-l_0)=-b(m-m_0)$ と変形できるが、$(a,b)=1$ であることから、この両辺の値を $abN$ と置くことができる。従って、一般解 $l=l_0+bN,\ m=m_0-aN$ を得る。

$m$ が負となる解の中で、最も 0 に近いものを考える。$m$ の解は $a$ ずつ増減して得られることから、$^{\exists}N_1\in\mathbb{Z}\quad s.t.\quad -a\leqq m_0-aN_1<0$ 。この $N_1$ を用いて、$l_1=l_0+bN_1,\ m_1=m_0-aN_1$ とおく。$-a\leqq m_1<0$ より、$al_1=k-bm_1>k-0\geqq0$。$\therefore l_1>0$ となる。

$ab+k=ab+(al_0+bm_1)=al_1+b(a+m_1)$ で、$x=l_1>0,\quad y=a+m_1\geqq0$ より、$ab+k$ を表すことができる。//

補題３　$n = ax + by$ について、$n' = 2ab - n$ とおくと、$n' = ax' + by'$　$(0 \leqq x' \leqq b, 0 \leqq y' \leqq a)$ を満たす整数 $x', y'$ が存在する。
$\because$) $n' = (ab - ax) + (ab - by) = a(b - x) + b(a - y)$ 。$x' = b - x$, $y' = a - y$ と置くと条件を満たす。//

さて、補題３より、$n + n' = 2ab$ が成り立つから、$n, n'$ の一方は $ab$ 以上であり、他方は $ab$ 以下である。$n = n'$ とすると、$n = n' = ab$ で、これは補題１で扱った、ただ１つ重複した表現を持つ値である。従って、$ax + by$　$(x, y \in \mathbb{Z},\quad 0 \leqq x \leqq b, 0 \leqq y \leqq a)$ で表すことができる相異なる $(a+1)(b+1) - 1$ 通りの整数のうち、$ab$ を除く $(a+1)(b+1) - 2$ 通りのうち、半分は $ab$ より小さく、半分は $ab$ より大きい。補題２と併せると、表せない整数は、$0, 1, 2, \cdots, ab - 1$ から表せるものを除いたものになるから、その個数は、 $ab - \dfrac{1}{2}\{(a+1)(b+1) - 2\} = ab - \dfrac{1}{2}(ab + a + b - 1) = \dfrac{1}{2}(ab - a - b + 1) = \dfrac{1}{2}(a-1)(b-1)$ //

関連入試問題　H12　大阪大（前期）
どのような負でない２つの整数 $m$, を用いても、 $x = 3m + 5n$ と表すことのできない正の整数 をすべて求めよ
※富山中部高校の中村先生から、「数学入試問題の鉱脈を探る」という難関大学入試対策用の教材を作成しており、「『１次不定方程式』という鉱脈」という節でこの問題を扱っていることを知らせてもらった。また、中村先生からは、映画「ダイハード３」で、主人公のブルース・ウィルスがある油分け算を出され、それを解かないと爆弾が炸裂するシーンがあるということも教えてもらった。

# 4　ブローイングアップによる特異点の解消との関連

この節の内容は、2011 年 8 月 8 日　京都大学で開催された公開講座「現代数学の展望」の講義の１つである「代数幾何と特異点」（並河良典教授）に参加したときのノートに従ったものである。自分なりに解釈した部分で、誤解や理解が不十分なところがあるかもしれない。

## 4.1　ブローイングアップの操作

方程式 $y^2 = x^3$ で表される曲線は、原点で特異点（尖点）を持つ。$f(x, y) = x^3 - y^2$ と置くと、$\dfrac{\partial f}{\partial x}(0,0) = \dfrac{\partial f}{\partial y}(0,0) = 0$ となるのである。

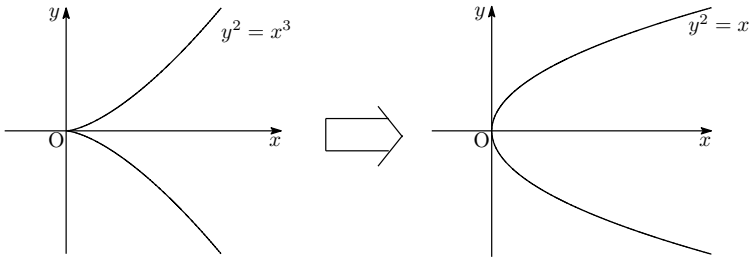



図 1: 特異点の解消

ここで、$x \mapsto x$, $y \mapsto xy$ とすると、これは原点以外では 1 対 1 対応になる。原点では、”blowing up = 爆発” している。

このとき、 $x^3-(xy)^2=x^2(x-y^2)=0$ となり、成分 $x-y^2=0$ は放物線で特異点を持たない。(特異点が解消された。)

$y^3=x^5$ の場合、すなわち $x^5-y^3=0$

- $x\mapsto x,\ y\mapsto xy$ として、$x^5-(xy)^3=x^3(x^2-y^3)=0$
- $x^2-y^3=0$ には、まだ特異点があるので、$x\mapsto xy,\ y\mapsto y$ とすると、$(xy)^2-y^3=y^2(x^2-y)=0$ となり、これで特異点が解消される。

$x^{17}-y^5=0$ の場合

- $x\mapsto x,\ y\mapsto xy$ を繰り返して、$x^{17}-y^5=0 \quad\longrightarrow\quad x^{12}-y^5=0\longrightarrow\quad x^7-y^5=0\longrightarrow\quad x^2-y^5=0$ と変形していく。ここで、 $y$ の次数の方が大きくなる。
- 次に、$x\mapsto xy,\ y\mapsto y$ を繰り返して、$x^2-y^3=0 \quad\longrightarrow\quad x^2-y=0$ となり、特異点が解消される。

この操作は、ユークリッドの互除法 $17=3\cdot5+2,\quad 5=2\cdot2+1$ と対応している。それぞれの段階で、商の値の分だけ、同様の変数変換を繰り返している。この操作を一般的に考えていく。

## 4.2 ブローイングアップとユークリッドの互除法

$p,q$ を互いに素な 2 つの自然数で、$p>q$ とする。また、$r_0=p, r_1=q \quad r_{i-1}=q_ir_i+r_{i+1}\,(i=1,2,\cdots,k) \quad r_k=1, r_{k+1}=0$ をユークリッドの互除法による計算とする。このとき、$x\mapsto x,\ y\mapsto xy$ もしくは $x\mapsto xy,\ y\mapsto y$ によるブローイングアップを繰り返していくと

- $x^p-y^q=0 \quad\longrightarrow\quad \cdots\cdots \quad\longrightarrow\quad x^{r_2}-y^q=0$
- $x^{r_2}-y^q=0 \quad\longrightarrow\quad \cdots\cdots \quad\longrightarrow\quad x^{r_2}-y^{r_3}=0$
- $x^{r_2}-y^{r_3}=0 \quad\longrightarrow\quad \cdots\cdots \quad\longrightarrow\quad x^{r_4}-y^{r_3}=0$
  $\cdots\cdots\cdots$

これを繰り返すと、$x^{r_{k-1}}-y^{r_k}=x^{r_{k-1}}-y=0$ もしくは $x^{r_k}-y^{r_{k-1}}=x-y^{r_{k-1}}=0$ にたどり着き、特異点が解消される。

## 4.3 特異点の悪質度と一次不定方程式

$\mathbb{R}$ を係数とする 2 変数 $x,y$ の多項式環を $\mathbb{R}[x,y]=\left\{\displaystyle\sum_{k,l\geqq0}a_{kl}x^ky^l \quad\middle|\quad a_{kl}\in\mathbb{R}\right\}$ で表す。
さらに、$f(x,y),g(x,y)\in\mathbb{R}[x,y]$ について、$p(x,y)\in\mathbb{R}$ による同値関係を

$$f(x,y)\equiv g(x,y)\ (\mathrm{mod}\ p(x,y)\ ) \quad\Longleftrightarrow\quad {}^{\exists}k(x,y)\in\mathbb{R}[x,y]\ s.t.\ f(x,y)-g(x,y)=p(x,y)k(x,y)$$

とし、同値関係による商環 $\mathbb{R}[x,y]/(p(x,y))$ を考える。そして、曲線 $C:x^3-y^2=0$ 上の関数に、$\mathbb{R}[x,y]/(x^3-y^2)$ を対応させる。

さらに、曲線 $C$ の特異点をブローイングアップで解消した曲線 $C':x'-y'^2=0$ には、$\mathbb{R}[x',y']/(x'-y'^2)$ を対応させるが、これは $g(x',y')$ において、$x'=y'^2$ を代入することになるから、$\mathbb{R}[x',y']/(x'-y'^2)\simeq\mathbb{R}[y']$ といえる。
ここで、$y'=t$ とおくと、$\mathbb{R}[y']=\mathbb{R}[t]$ となり、これを特異点を解消した曲線上の関数と考える。
$x'=t^2,\quad x=x'=t^2,\quad y=x'y'=t^3$ 。これを用いて、

$$\mathbb{R}[x,y] \Longrightarrow \mathbb{R}[t^2,t^3] = \left\{ \sum_{k,l\geqq 0} a_{k\,l}(t^2)^k(t^3)^l \right\} = \left\{ \sum_{k,l\geqq 0} a_{k\,l}t^{2k+3l} \right\}$$

この中に現れる $t$ の単項式は、$1, t^2, t^3, t^4, \cdots$ であり、$t$ の 1 乗の項だけ出てこない。

曲線 $x^5 - y^3 = 0$ の場合は、1 回ブローイングアップして、$x'^2 - y'^3 = 0$ 、さらにブローイングアップして、$x''^2 - y'' = 0$ 。

$x'' = t$ とおいて、特異点を解消した曲線上の関数を $\mathbb{R}[t]$ とする。また、$y'' = x''^2 = t^2, \quad \Longrightarrow \quad x' = x''y'' = t^3,\ y' = y'' = t^2, \quad \Longrightarrow \quad x = x' = t^3,\ y = x'y' = t^5$ 。これを用いて、

$$\mathbb{R}[x,y] \Longrightarrow \mathbb{R}[t^3,t^5] = \left\{ \sum_{k,l\geqq 0} a_{k\,l}(t^3)^k(t^5)^l \right\} = \left\{ \sum_{k,l\geqq 0} a_{k\,l}t^{3k+5l} \right\}$$

この中に現れる $t$ の単項式は、$1, t^3, t^5, t^6, t^8, t^9, t^{10}\cdots$ であり、$t, t^2, t^4, t^7$ が出てこない。

一般に、互いに素な 2 つの自然数 $p, q$ について、曲線 $C_{p,q} : x^p - y^q = 0$ を考える。ブローイングアップを繰り返すと、$x^r - y = 0$ もしくは $x - y^r = 0$ の形になり、特異点が解消され、その曲線上の関数は、$x, y$ いずれかを $t$ とおいて、 $\mathbb{R}[t]$ となる。

これを元の曲線 $C_{p,q}$ に戻すと、$x = t^q, y = t^p$ となり、

$$\mathbb{R}[x,y] \Longrightarrow \mathbb{R}[t^q,t^p] = \left\{ \sum_{k,l\geqq 0} a_{k\,l}(t^q)^k(t^p)^l \right\} = \left\{ \sum_{k,l\geqq 0} a_{k\,l}t^{qk+pl} \right\}$$

となる。

曲線 $C_{p,q}$ 上の関数 $f(x,y) \in \mathbb{R}[x,y]/(x^p - y^q)$ に対して、$f(t^q,t^p) \in \mathbb{R}[t]$ を対応させる写像を $\varphi$ とする。このとき、$Im(\varphi)$ に現れない $t$ のベキは、$pl + qk \quad (k,l \geqq 0)$ によって表せない自然数である。命題 2 により、その個数は $\dfrac{1}{2}(p-1)(q-1)$ である。

曲線 $C_{p,q}$ の特異点の程度（悪質度）

$$\nu(C_{p,q}) = \dim\left(\mathbb{R}[t]/Im(\varphi)\right) = \sharp\{pl + qk \quad (k,l \geqq 0) \text{ によって表せない自然数 }\} = \frac{1}{2}(p-1)(q-1)$$

## 4.4 特異点の悪質度の幾何学的解釈

今度は、複素 2 次元空間で考える。

$C_{p,q} = \{(x,y) \in \mathbb{C}^2 \,|\, x^p - y^q = 0\}$ とする。ただし、 $p, q$ は互いに素な自然数とする。

この曲線は、原点で特異点を持つが、 $0 < t \ll 1$ :十分小さな正の実数をとり、

$C_{p,q,t} = \{(x,y) \in \mathbb{C}^2 \,|\, x^p - y^q + t = 0\}$ 　　（$t$ で $C_{p,q}$ を揺さぶったもの）

とすると、特異点が解消する。そのかわり、$\dfrac{1}{2}(p-1)(q-1)$ 個の穴が開いた浮き輪に位相同型となるそうである。

（簡単に示すことができることなのかどうかわからない）

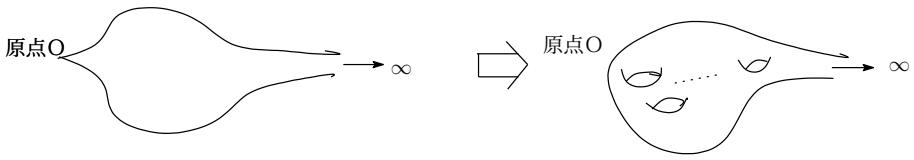



図 2: 揺さぶって特異点解消

特異点の解消について、余り抽象的でない範囲で、勉強できればよいのだが、そんな目的に適した解説書があるのかどうか、よく知らない。そうした中、今回、公開講座に参加し、特異点の解消のあるトピックスが初等的な数論と結びつきがあることを聞き、さらに、そのしばらく後に、油分け算について新聞記事があることを教えてもらったことは偶然かも知れない。おかげで、このような報告をまとめることとなり、日ごろ、数学に全く関係のない仕事に追われている中、ちょっぴり嬉しいことであった。