不定方程式 $ax+by=c$ の整数解

河合（かわい） 進輔（しんすけ）

・はじめに

$ax+by=c$（a, b, c は 0 でない整定数）…… ①

を満たす整数の組 x, y を求めなければならない問題が大学入試などでよく出題されるが，この問題の解法について教科書はもちろん参考書類でもきっちりと書かれたものは少ないようだ．

a，b，c が 2 桁以下の小さな数の場合は直感的に解を見つけることは簡単だが(実際そのような場合が多い)，3 桁以上の数になるとそうはいかない．そこでこの問題の解法(計算法)などについて述べてみたい．

・まず問題を整理する

a，b の最大公約数を d とすると明らかに c が d の倍数でなければ解は存在しない．

そこで，$c=kd$（kは整数）とし，$ax+by=d$ …… ⓘ の解の 1 組を $(x_0,\ y_0)$ とすれば，① の解の 1 組は，$(kx_0,\ ky_0)$ でありこれから後述するようにすべての解が求められる．

更に $a=a'd$，$b=b'd$ とすると a'，b' は互いに素な整数で ⓘ の両辺を d で割ると $a'x+b'y=1$ …… ⓘ となるので ⓘ の解を考えるとよい．

符号は解に含ませて考えるとよいので簡単のために，以降，$ax+by=1$（a, bは互いに素な正の整数で $a>b>0$）…… ⓘ の解を考える．

・解の存在証明

ⓘ の整数解が存在することの証明だけなら次のように簡単である．

集合 M を $M=\{ax+by \mid x, y$ は整数$\}$ とし，M に属する最小の正の整数を $ax_0+by_0=d$ とする．M の任意の要素 $ax+by$ を d で割った商を q，余りを r とすると

$ax+by=(ax_0+by_0)q+r$

$r=a(x-x_0q)+b(y-y_0q)\in M$

$0\leqq r<d$ だから，$r\neq 0$ とすると d が M の最小の正の要素であることに反する．よって $r=0$

したがって，M の任意の要素は d の倍数であり，

$a=a\cdot 1+b\cdot 0\in M$，$b=a\cdot 0+b\cdot 1\in M$ だから a，b は d の倍数．

a，b は互いに素であるから $d=1$

よって，$ax_0+by_0=1$ となる x_0，y_0 が存在する．

・具体的な解き方

最も順当な考え方は次のようにユークリッドの互除法を逆に辿る方法だと思うがなかなか面倒である．

a，b に互除法を用いて次のようになったとする．

$a-bq_0=r_0$

$b-r_0q_1=r_1$

$r_0-r_1q_2=r_2$ $\begin{pmatrix} q_0,\ q_1,\ \cdots\cdots,\ q_n\text{は商} \\ r_0,\ r_1,\ \cdots\cdots,\ r_n\text{は余り} \end{pmatrix}$

$r_{n-3}-r_{n-2}q_{n-1}=r_{n-1}$

$r_{n-2}-r_{n-1}q_n=r_n(=1)$

上から順に 1 つ下の式に代入して $r_0, r_1, \cdots\cdots, r_{n-1}$ を消去していくと $ax_0+by_0=1$ の形になり 1 組の解 $(x_0,\ y_0)$ が求められる．実際の数字で計算する場合でも a，b，r_0，r_1，…… ，r_n は文字で表しておかなければ紛らわしい．そこで行列を用いて互除法の式を表すと次のようになる．

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix}=\begin{pmatrix} b \\ r_0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}\begin{pmatrix} b \\ r_0 \end{pmatrix}=\begin{pmatrix} r_0 \\ r_1 \end{pmatrix}$$

$$\vdots$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix}\begin{pmatrix} r_{n-3} \\ r_{n-2} \end{pmatrix}=\begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix}\begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix}=\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix}=\begin{pmatrix} r_{n-1} \\ 1 \end{pmatrix}$$

上から順に 1 つ下の式に代入して $r_0, r_1, \cdots\cdots, r_{n-1}$ を消去すると

$$\begin{pmatrix}0 & 1\\ 1-q_n & \end{pmatrix}\begin{pmatrix}0 & 1\\ 1-q_{n-1} & \end{pmatrix}\cdots\cdots\begin{pmatrix}0 & 1\\ 1-q_0 & \end{pmatrix}\begin{pmatrix}a\\ b\end{pmatrix}=\begin{pmatrix}r_{n-1}\\ 1\end{pmatrix}$$

となる．～～の部分を計算した行列の(2,1)成分がx_0,(2,2)成分がy_0である．いずれにしても，式を代入していかなければならない．そこで次のようにすれば同時進行的にx_0，y_0が求められる．

$A=a$ …… ①，$B=b$ …… ②とおく．

①−②×q_0より　　$A-q_0B=r_0$……③

②−③×q_1より　　$-q_1A+(1+q_1q_0)B=r_1$

と計算を続け右辺が1になったときのA，Bの係数がx_0，y_0である．ただし，実際の計算では次の例に示すようにA，B以外は数字である．

$a=229, b=106$の場合を例に計算すると

$A=229$…… ①

$B=106$…… ②

①−②×2より　$A-2B=17$ …… ③

②−③×6より$-6A+13B=4$ …… ④

③−④×4より $25A-54B=1$

となり，$(25,-54)$が解の1つである．

右辺で互除法を行って余りを求めていき，左辺でA，Bの係数の計算を行うのである．

・一般解(すべての解)

ⓘⓥの1組の解$(x_0,\ y_0)$が求められれば，ⓘⓥの式から$ax_0+by_0=1$を引いて

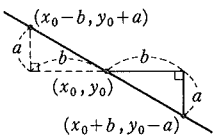
$a(x-x_0)+b(y-y_0)=0$

$a(x-x_0)=-b(y-y_0)$

a，bは互いに素だから，$x-x_0$はbの倍数になるので，$x-x_0=lb$(lは整数)とおくと $y-y_0=-la$

よって,$(x,y)=(x_0+lb,\ y_0-la)$(lは整数)と表される．

これは，ⓘⓥの式を傾き$-\frac{a}{b}$の直線の方程式と見てグラフを考えるとわかりやすい(右図参照)．直線ⓘⓥは格子点$(x_0,\ y_0)$を通り，傾き$-\frac{a}{b}$の直線だから，x座標についてbごとに，y座標についてaごとに格子点を通る．



aとbは互いに素であるからこれらの格子点以外に直線ⓘⓥ上の格子点はない．

ⓘⓥの解が求められれば，ⓘⓘⓘの解が求められ，ⓘⓘと ⓘⓘⓘの解は同じだからその1組を$(x_0,\ y_0)$とすると，

ⓘの解の1組は$(kx_0,\ ky_0)$である．

ⓘの式から$akx_0+bky_0=C$を引いて

$a(x-kx_0)+b(y-ky_0)=0$

$a(x-kx_0)=-b(y-ky_0)$

両辺をa，bの最大公約数dで割って

$a'(x-kx_0)=-b'(y-ky_0)$

a'，b'は互いに素であるからⓘⓥのときと同様に，

$(x,y)=(kx_0+lb',\ ky_0-la')$($l$は整数)となる．

・最後に

実際の入試問題を用いて応用をもう1つ挙げておくことにする．96年の東京理科大の入試に次のような内容の問題が出題された．

nを自然数として集合A，B，Cを次のように定める．

A=$\{8n-5\}$　(8で割って3余る自然数)

B=$\{9n-5\}$　(9で割って4余る自然数)

C=$\{13n-8\}$ (13で割って5余る自然数)

このときA∩B∩Cに属する最小の自然数を求めるのである．

集合A∩Bに属する要素は$72m-5$ (mは自然数)と表されるので，$72m-5=13n-8$…… ①を満たすm，nを求めることによって，A∩B∩Cの要素がわかる．①を変形して$-72m+13n=3$

ここで，$A=72$…… ②　$B=13$…… ③とおいて互除法の計算をするのだが，余りとして絶対値最小の余りをとると計算が早い．すなわち，

②−③×5より　　$A-5B=7$ …… ④

③−④より　　$-A+6B=6$ …… ⑤

④−⑤より　　$2A-11B=1$

としないで

②−③×6より　$A-6B=-6$ …… ④′ ($|-6|<7$)

③+④′×2より　$2A-11B=1$ …… ⑥

とする．

⑥×3より　　$6A-33B=3$

$-72\cdot(-6)+13\cdot(-33)=3$

(①の形に戻すと$72\cdot(-6)-5=13\cdot(-33)-8$)

72と13は互いに素だから，$m=-6+13l$,

$n=-33+72l$(lは整数)となり，$l=1$のときの

$72\cdot7-5=13\cdot39-8=499$が答となる．

以上古い講義ノートより下記の文献を参考にしながらまとめてみました．

(参考文献)一松　信著「代数学入門第一課」(近代科学社)