数チャレ 第103回(2009年8月)

$a,\ b,\ c,\ d,\ p,\ q,\ r$ は整数であり,

$$ad-bc=1,\ \ p>0,\ \ q^2-pr<0$$

を満たすものとする。

(1) 行列式 $\det\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}p & q\\ q & r\end{pmatrix}\begin{pmatrix}a & c\\ b & d\end{pmatrix}$ を計算せよ。

(2) $\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}p & q\\ q & r\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ および $\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}\begin{pmatrix}p & q\\ q & r\end{pmatrix}\begin{pmatrix}1 & 0\\ k & 1\end{pmatrix}$ を計算せよ。

(3) $\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}p & q\\ q & r\end{pmatrix}\begin{pmatrix}a & c\\ b & d\end{pmatrix}=\begin{pmatrix}s & t\\ t & u\end{pmatrix}$ とするとき,整数 $a,\ b,\ c,\ d\ (ad-bc=1)$ を適当にとれば,$s\geqq u\geqq|t|$ とできることを示せ。

(4) p を $p\equiv 1\pmod 4$ なる素数とするとき,$m^2\equiv -1\pmod p$ を満たす整数 m が($1\leqq m\leqq p-1$ の範囲に)存在することは知られている。この $p,\ m$ に対して,整数 n を $n=\dfrac{m^2+1}{p}$ により定めるとき,

$$\begin{pmatrix}p & m\\ m & n\end{pmatrix}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}a & c\\ b & d\end{pmatrix}$$

を満たすような整数 $a,\ b,\ c,\ d\ (ad-bc=1)$ が存在することを示せ。

解答

(1) 行列式の性質と $ad-bc=1$ より

$$\begin{aligned}\det\begin{pmatrix}a & b\\ c & d\end{pmatrix}\begin{pmatrix}p & q\\ q & r\end{pmatrix}\begin{pmatrix}a & c\\ b & d\end{pmatrix}&=(ad-bc)(pr-q^2)(ad-cb)\\ &=pr-q^2\quad(\text{答})\end{aligned}$$

(2)

$$\begin{aligned}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}p & q\\ q & r\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}&=\begin{pmatrix}q & r\\ -p & -q\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\\ &=\begin{pmatrix}r & -q\\ -q & p\end{pmatrix}\quad(\text{答})\qquad\cdots\cdots\ ①\end{aligned}$$

$$\begin{aligned}\begin{pmatrix}1 & k\\ 0 & 1\end{pmatrix}\begin{pmatrix}p & q\\ q & r\end{pmatrix}\begin{pmatrix}1 & 0\\ k & 1\end{pmatrix}&=\begin{pmatrix}p+kq & q+kr\\ q & r\end{pmatrix}\begin{pmatrix}1 & 0\\ k & 1\end{pmatrix}\\ &=\begin{pmatrix}p+2kq+k^2r & q+kr\\ q+kr & r\end{pmatrix}\quad(\text{答})\qquad\cdots\cdots\ ②\end{aligned}$$

(3) $(0<)\,p<r$ であるとすれば,①により

$$s=r>u=p$$

とできる。

$(0<)\, r<|q|$ であるとすれば，

$$r \geqq |q+kr|$$

を満たす整数 k を用いて $t=q+kr$ とすると，②より

$$u=r \geqq |t|$$

とできる。このとき，$r>0,\ q^2-pr<0$ より

$$p+2kq+k^2r=r\left(k+\frac{q}{r}\right)^2-\frac{q^2-pr}{r}>0$$

であること，(1)より

$$(p+2kq+k^2r)r-(q+kr)^2=pr-q^2>0$$

であることに注意する。

以上の操作により，行列が

$$\begin{pmatrix} p & q \\ q & r \end{pmatrix} \longrightarrow \begin{pmatrix} p_1 & q_1 \\ q_1 & r_1 \end{pmatrix} \longrightarrow \begin{pmatrix} p_2 & q_2 \\ q_2 & r_2 \end{pmatrix} \longrightarrow \cdots\cdots$$

と変形されるとき

$$r \geqq r_1 \geqq r_2 \geqq r_3 \geqq \cdots\cdots \geqq 1$$

であり，ある自然数 n に対して

$$r_n=r_{n+1}=r_{n+2}=\cdots\cdots$$

となる。このとき $s=p_n,\ t=q_n,\ u=r_n$ とすると，

$$s \geqq u \geqq |t|$$

である。各変形に現れる行列 $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ の積を $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ とすると

$$ad-bc=1$$

であり，

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} p & q \\ q & r \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix}=\begin{pmatrix} s & t \\ t & u \end{pmatrix},\quad s \geqq u \geqq |t|$$

となる。　　(証明おわり)

(4)　(3)より，ある整数 $\alpha,\ \beta,\ \gamma,\ \delta$ を用いて

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}\begin{pmatrix} p & m \\ m & n \end{pmatrix}\begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}=\begin{pmatrix} s & t \\ t & u \end{pmatrix} \qquad \cdots\cdots ③$$

$$s \geqq u \geqq |t| \qquad \cdots\cdots ④$$

$$\alpha\delta-\beta\gamma=1 \qquad \cdots\cdots ⑤$$

とすることができる。(1)と $p,\ m,\ n$ の定め方，および⑤より

$$su-t^2=pn-m^2=1 \qquad \cdots\cdots ⑥$$

であるから，④より

$$su=t^2+1 \leqq u^2+1 \qquad \therefore\ 0 \leqq (s-u)u \leqq 1 \qquad \cdots\cdots ⑦$$

(i)　$s=u$ のとき，⑥より

$$1=su-t^2=u^2-t^2=(u+t)(u-t)$$

④より $u+t \geqq 0,\ u-t \geqq 0$ であるから

$$u+t=u-t=1 \qquad \therefore\ u=1,\ \ t=0$$

$$\therefore\ \begin{pmatrix} s & t \\ t & u \end{pmatrix}=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

(ii) $s>u$ のとき

⑥より $u\neq 0$ であるから，④より $u>0$ であり，⑦より

$$s-u=1,\ \ u=1 \qquad \therefore\ s=2,\ \ u=1$$

⑥より

$$t^2=su-1=1 \qquad \therefore\ t=\pm 1$$

よって，

$$\begin{pmatrix} s & t \\ t & u \end{pmatrix}=\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

または

$$\begin{pmatrix} s & t \\ t & u \end{pmatrix}=\begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix}=\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$$

以上により，

(i) の場合は $\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1}=\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$

(ii) の場合は $\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}^{-1}\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}$

（複号同順）

とおくと，③より

$$\begin{pmatrix} p & m \\ m & n \end{pmatrix}=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

が得られる。 （証明おわり）

（注）

1° $p\equiv 1 \pmod 4$ のとき，$p-1=2z$ を満たす（正の）偶数 z が存在するから，

$$\begin{aligned}(p-1)!&=z!\times(p-1)(p-2)\cdots(p-z)\\ &\equiv z!\times(-1)^z z!\equiv(z!)^2 \pmod p\end{aligned}$$

と変形できる。ウィルソンの定理より

$$(p-1)!\equiv -1 \pmod p$$

であるから，$m=z!$ は $m^2\equiv -1 \pmod p$ を満たす。

なお，ウィルソンの定理については第 17 回を参照してもらいたい。

2° 本問により

$p\equiv 1 \pmod 4$ を満たす素数 p は $p=a^2+b^2$ $(a,\ b\in \boldsymbol{N})$ と表される

ことが示されたことになるが，過去にも第 11 回でこのテーマを取り上げている。第 11 回ではトゥエの剰余定理の応用として示されており，単純に考えればそちらの方が証明は簡単であるが，今回用いた整数係数 2 次形式の理論は応用範囲が広いので，数学を学習する上では重要度が高い。