数チャレ 第57回(2005年10月)

整数を成分とする行列 $A=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ について，A^2 のすべての成分が素数 p で割り切れるための必要十分条件は，$a+d$ と $ad-bc$ がともに素数 p で割り切れることである。これを証明せよ。

コメント：行列は表示のためだけのもので，問題の解決にあたって行列は本質ではない。

解答

$$A^2=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} a^2+bc & b(a+d) \\ c(a+d) & bc+d^2 \end{pmatrix}$$

【十分条件であることの証明】

$a+d$ と $ad-bc$ がともに素数 p で割り切れるならば，p の倍数は差および整数倍について閉じているから，

$$a^2+bc=a(a+d)-(ad-bc) \quad \cdots\cdots ①$$
$$b(a+d) \quad \cdots\cdots ②$$
$$c(a+d) \quad \cdots\cdots ③$$
$$bc+d^2=d(a+d)-(ad-bc) \quad \cdots\cdots ④$$

はすべて p で割り切れる。

【必要条件であることの証明】

①, ②, ③, ④がすべて素数 p で割り切れるとする。

(i) b, c がともに素数 p で割り切れるときは，①, ④が p で割り切れることより

a^2, d^2 はともに p で割り切れる。

p は素数であるから，結局

a, b, c, d はすべて p で割り切れる

ことになって，特に

$a+d$, $ad-bc$ はともに p で割り切れる。

(ii) b, c の少なくとも一方が素数 p で割り切れないときは，②, ③より

$a+d$ は p で割り切れる

から，①が p で割り切れることより，

$ad-bc$ も p で割り切れる

ことになる。

(おわり)