

数チャレ 第185回 (2016年6月)

p を 2 でない素数とし, 自然数 m, n は

$$(m + n\sqrt{p})(m - n\sqrt{p}) = 1$$

を満たすとする。

(1) 互いに素な自然数の組 (x, y) で

$$m + n\sqrt{p} = \frac{x + y\sqrt{p}}{x - y\sqrt{p}}$$

を満たすものが存在することを示せ。

(2) x は (1) の条件を満たす自然数とする。 x が p で割り切れないことと, m を p で割った余りが 1 であることが, 同値であることを示せ。

出典 : 2016 年 千葉大学

解答

(1) $m + n\sqrt{p} = \frac{x + y\sqrt{p}}{x - y\sqrt{p}}$ を変形して

$$\begin{aligned} x + y\sqrt{p} &= (m + n\sqrt{p})(x - y\sqrt{p}) \\ &= mx - pny + (nx - my)\sqrt{p} \end{aligned}$$

$$\therefore (m - 1)x - pny + \{nx - (m + 1)y\}\sqrt{p} = 0$$

この等式を満たす自然数 x, y があるとすれば, \sqrt{p} は無理数であるから,

$$\begin{cases} (m - 1)x - pny = 0 & \dots\dots \textcircled{1} \\ nx - (m + 1)y = 0 & \dots\dots \textcircled{2} \end{cases}$$

が必要である。①, ② および

$$(m + n\sqrt{p})(m - n\sqrt{p}) - 1 = (m + 1)(m - 1) - pn^2 = 0$$

を考え,

$$x = \frac{pn}{\gcd(pn, m - 1)}, \quad y = \frac{m - 1}{\gcd(pn, m - 1)}$$

とおくと, x と y は互いに素な自然数であり,

$$\begin{aligned} \frac{x + y\sqrt{p}}{x - y\sqrt{p}} &= \frac{pn + (m - 1)\sqrt{p}}{pn - (m - 1)\sqrt{p}} \\ &= \frac{\{pn + (m - 1)\sqrt{p}\}^2}{\{pn - (m - 1)\sqrt{p}\}\{pn + (m - 1)\sqrt{p}\}} \end{aligned}$$

$$\begin{aligned}
&= \frac{p\{pn^2 + (m-1)^2 + 2(m-1)n\sqrt{p}\}}{p\{pn^2 - (m-1)^2\}} \\
&= \frac{pn^2 + (m-1)^2 + 2(m-1)n\sqrt{p}}{pn^2 - (m-1)^2} \\
&= \frac{(m+1)(m-1) + (m-1)^2 + 2(m-1)n\sqrt{p}}{(m+1)(m-1) - (m-1)^2} \\
&= \frac{(m+1) + (m-1) + 2n\sqrt{p}}{(m+1) - (m-1)} \\
&= m + n\sqrt{p}
\end{aligned}$$

(証明おわり)

(2) x, y は ①かつ②を満たす互いに素な自然数であるとする。

x が p で割り切れないとすると, ①より

$$(m-1)x = pny \text{ は素数 } p \text{ で割り切れる}$$

から, $m-1$ は p で割り切れ,

m を p で割った余りは 1 である。

逆に, $m \equiv 1 \pmod{p}$ であるとすれば, p は奇素数であるから,

$m+1$ は p で割り切れない。

y が p で割り切れるなら, x と y は互いに素であるから, x は p で割り切れない。

y が p で割り切れないなら, ②より

$$nx = (m+1)y \text{ は } p \text{ で割り切れない}$$

から, x も p で割り切れない。

以上より, x が p で割り切れないことと, m を p で割った余りが 1 であることは同値である。

(証明おわり)