

# 数チャレ 第46回 (2004年11月)

$p$  を奇素数 (2 以外の素数) であるとする。

- (1)  $i = 1, 2, \dots, p-1$  に対して,  ${}_p C_i$  は  $p$  で割り切れることを示せ。
- (2)  $p$  で割り切れない整数  $a$  に対して,  $a^{p-1} - 1$  は  $p$  で割り切れることを示せ。
- (3)  $\frac{p-1}{2}$  は奇数であるとする。自然数の平方の和  $m^2 + n^2$  が  $p$  でちょうど  $e (\geq 1)$  回割り切れるとき,  $e$  は偶数であることを示せ。

## 解答

$$(1) \quad {}_p C_i = \frac{p}{i} \cdot {}_{p-1} C_{i-1}$$

および  ${}_{p-1} C_{i-1}$  は整数であり,  $p$  と  $i$  は互いに素であるから

$$\frac{1}{i} \cdot {}_{p-1} C_{i-1} \text{ は整数}$$

である。よって,  ${}_p C_i$  は  $p$  で割り切れる。 (おわり)

- (2) 整数の除法の性質より

$$a = pq + r \quad (q, r \text{ は整数}, 1 \leq r \leq p-1)$$

と表すことができ,

$$a^p = (pq + r)^p \equiv r^p \pmod{p}$$

- (1)の結果より

$$\begin{aligned} r^p &= (r-1+1)^p \equiv (r-1)^p + 1^p \\ &\equiv (r-2)^p + 1^p + 1^p \\ &\vdots \\ &\equiv r \cdot 1^p \pmod{p} \end{aligned}$$

であるから,

$$a^p \equiv r^p \equiv r \equiv a \pmod{p}$$

よって,  $a^p - a = a(a^{p-1} - 1)$  は  $p$  で割り切れるが,  $p$  と  $a$  は互いに素であるから,  $a^{p-1} - 1$  は  $p$  で割り切れる。 (おわり)

- (3)  $\frac{p-1}{2} = s$  とおく。  $s$  が奇数であることに注意すると,

$$\begin{aligned} m^{p-1} + n^{p-1} &= m^{2s} + n^{2s} \\ &= (m^2 + n^2)(m^{2(s-1)} - m^{2(s-2)}n^2 + \dots + n^{2(s-1)}) \end{aligned}$$

と因数分解できて, (2)より

$$m \text{ または } n \text{ が } p \text{ で割り切れないならば, } m^{p-1} + n^{p-1} \equiv 1 \text{ or } 2 \pmod{p}$$

となるから,  $m^2 + n^2$  が  $p$  で割り切れることに反する。

よって、 $m$  も  $n$  も  $p$  で割り切れることになり、

$$m = p^k u, \quad n = p^l v \quad (k, l, u, v \text{ は自然数, } u, v \text{ は } p \text{ と互いに素})$$

と表される。

(i)  $k < l$  のとき

$p^{l-k}$  は  $p$  で割り切れ、 $u$  は  $p$  で割り切れないことより

$$\frac{m^2 + n^2}{p^{2k}} = u^2 + p^{l-k} v^2$$

は  $p$  で割り切れないから、 $m^2 + n^2$  は  $p$  でちょうど  $2k$  回割り切れる。

(ii)  $k > l$  のとき

(i)と同様の考察により、 $m^2 + n^2$  は  $p$  でちょうど  $2l$  回割り切れることがわかる。

(iii)  $k = l$  のとき

$$m^2 + n^2 = p^{2k}(u^2 + v^2)$$

証明の前半で述べたことにより  $u^2 + v^2$  は  $p$  で割り切れないから、 $m^2 + n^2$  は  $p$  でちょうど  $2k$  回割り切れる。

以上より、自然数の平方の和  $m^2 + n^2$  は  $p$  で (割り切れない場合も含めて) ちょうど偶数回割り切れる。 (おわり)

(注) 証明の内容を詳しく見てみると、 $m$  と  $n$  が互いに素であれば  $m^2 + n^2$  は  $p$  で割り切れないことがわかる。

$$\frac{p-1}{2} \text{ が奇数} \iff p \equiv 3 \pmod{4}$$

であるから、次の定理が得られる：

互いに素な平方数の和の素因数  $p$  は  $p = 2$  または  $p \equiv 1 \pmod{4}$  に限られる。

$p \equiv 1 \pmod{4}$  を満たす素数  $p$  は  $p = m^2 + n^2$  ( $m, n$  は自然数) と表されることについては、既に第 11 回(2001 年 12 月)で取り上げた。恒等式

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

により、その積も  $m^2 + n^2$  と表されることはわかるので、上の定理の内容は必要条件だけでなく、十分条件でもある。