

数チャレ 第19回(2002年8月)

p を奇素数, n を p で割り切れない整数とする。 $n \equiv m^2 \pmod{p}$ を満たす整数 m が存在するとき $\left(\frac{n}{p}\right) = 1$, そうでないとき $\left(\frac{n}{p}\right) = -1$ と表す。

必要ならば, フェルマーの小定理 $n^{p-1} \equiv 1 \pmod{p}$ を用いてもよい。

(1) $(1+i)^{p+1} - 2\left(\frac{2}{p}\right)i^{\frac{p+1}{2}}$ の実部, 虚部はともに p の整数倍であることを示せ。

ただし, i は虚数単位である。

(2) p を 8 で割った余りで分類して, $\left(\frac{2}{p}\right)$ を求めよ。

(3) 任意の素数 p に対して,

$$X^4 + 1 \equiv (X^2 + aX + b)(X^2 + cX + d) \pmod{p}$$

を満たす整数 a, b, c, d が存在することを示せ。

コメント: 要するに $X^4 + 1$ は $\text{mod } p$ で可約であると示されるわけですが, 幾何学に応用されるらしいという話を聞いたことがあります。

解答

$$(1) \quad (1+i)^{p+1} = \{(1+i)^2\}^{\frac{p+1}{2}} = (2i)^{\frac{p+1}{2}} = 2 \times 2^{\frac{p-1}{2}} \times i^{\frac{p+1}{2}}$$

であるから, 題意を示すには

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p}$$

であることを示せばよいが, そのためには(あとのことも考えて)

$$1 \leq k \leq p-2 \implies r^k \not\equiv 1 \pmod{p}, \quad r^{p-1} \equiv 1 \pmod{p}$$

となる r が存在することを示すことが本質的である。このような r の類を $\text{mod } p$ における原始根という。

p が素数であることより,

$$ab \equiv 0 \pmod{p} \implies a \equiv 0 \pmod{p} \text{ または } b \equiv 0 \pmod{p}$$

が成り立つから, 高校数学で扱うような方程式の理論が通用する。したがって, $p-1$ 以下の任意の自然数 n に対して

$$x^n \equiv 1 \pmod{p}$$

を満たす整数 x は, $1, 2, 3, \dots, p-1$ の中には n 個以下しかない。累乗して 1 となる(または 1 と合同になる)最小の自然数を位数と呼ぶが, $1, 2, 3, \dots, p-1$ を位数により分類して

$$\left\{ \left(\cos \frac{2\pi}{p-1} + i \sin \frac{2\pi}{p-1} \right)^k \mid k = 1, 2, 3, \dots, p-1 \right\}$$

における位数と比べると, 確かに位数 $p-1$ の剰余類($\text{mod } p$ における原始根)が存在することがわかる。

mod p における原始根の一つを r とし, $2 \equiv r^s \pmod{p}$ とする。

$s = 2k$ (偶数) のとき $\left(\frac{2}{p}\right) = 1$ であり,

$$2^{\frac{p-1}{2}} \equiv (r^{2k})^{\frac{p-1}{2}} \equiv (r^{p-1})^k \equiv 1 \pmod{p}$$

$s = 2k + 1$ (奇数) のとき $\left(\frac{2}{p}\right) = -1$ であり,

$$2^{\frac{p-1}{2}} \equiv (r^{2k+1})^{\frac{p-1}{2}} \equiv (r^{p-1})^k r^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

(おわり)

(2) p は素数であるから, $1 \leq k \leq p-1$ なる任意の整数 k に対して

$${}^p C_k = \frac{p}{k} {}^{p-1} C_{k-1} \text{ は } p \text{ の整数倍}$$

であることに注意すると, 二項定理より

$$(1+i)^{p+1} = (1+i)^p(1+i) \equiv (1+i^p)(1+i) \pmod{p}$$

(a) $p \equiv 1 \pmod{8}$ のとき

$i^p = i$ より $(1+i^p)(1+i) = (1+i)^2 = 2i$, $\frac{p+1}{2} \equiv 1 \pmod{4}$ より $i^{\frac{p+1}{2}} = i$ であるから, (1)より

$$2i \equiv 2\left(\frac{2}{p}\right)i \pmod{p} \quad \therefore \left(\frac{2}{p}\right) = 1$$

(b) $p \equiv 3 \pmod{8}$ のとき

$i^p = -i$ より $(1+i^p)(1+i) = (1-i)(1+i) = 2$, $\frac{p+1}{2} \equiv 2 \pmod{4}$ より $i^{\frac{p+1}{2}} = -1$ であるから, (1)より

$$2 \equiv 2\left(\frac{2}{p}\right)(-1) \pmod{p} \quad \therefore \left(\frac{2}{p}\right) = -1$$

(c) $p \equiv 5 \pmod{8}$ のとき

$i^p = i$ より $(1+i^p)(1+i) = (1+i)^2 = 2i$, $\frac{p+1}{2} \equiv 3 \pmod{4}$ より $i^{\frac{p+1}{2}} = -i$ であるから, (1)より

$$2i \equiv 2\left(\frac{2}{p}\right)(-i) \pmod{p} \quad \therefore \left(\frac{2}{p}\right) = -1$$

(d) $p \equiv 7 \pmod{8}$ のとき

$i^p = -i$ より $(1+i^p)(1+i) = (1-i)(1+i) = 2$, $\frac{p+1}{2} \equiv 0 \pmod{4}$ より $i^{\frac{p+1}{2}} = 1$ であるから, (1)より

$$2 \equiv 2\left(\frac{2}{p}\right) \cdot 1 \pmod{p} \quad \therefore \left(\frac{2}{p}\right) = 1$$

以上をまとめると,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod{p} \\ -1 & \text{if } p \equiv 3, 5 \pmod{p} \end{cases} \quad (\text{答})$$

(3) (1)で示した原始根の存在により

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

(i) $p \equiv 1 \pmod{4}$ のとき, $\frac{p-1}{2}$ は偶数であるから,

$$\left(\frac{-1}{p}\right) = 1$$

よって, $-1 \equiv m^2 \pmod{p}$ となる自然数 m が存在するから,
 $X^4 + 1 \equiv X^4 - m^2 \equiv (X^2 + m)(X^2 - m) \pmod{p}$

(ii) $p \equiv 3 \pmod{8}$ のとき, 上で述べたことと (2) (b)より

$$\left(\frac{-1}{p}\right) = -1, \quad \left(\frac{2}{p}\right) = -1$$

このことは -1 も 2 も \pmod{p} において原始根の奇数乗と合同であるから, -2 は原始根の偶数乗と合同であり, $-2 \equiv m^2 \pmod{p}$ となる自然数 m が存在する。
 よって,

$$\begin{aligned} X^4 + 1 &= (X^2 - 1)^2 + 2X^2 \\ &\equiv (X^2 - 1)^2 - m^2 X^2 \pmod{p} \\ &= (X^2 + mX - 1)(X^2 - mX - 1) \end{aligned}$$

(iii) $p \equiv 7 \pmod{8}$ のとき, (2)より

$$\left(\frac{2}{p}\right) = 2$$

であるから, $2 \equiv m^2 \pmod{p}$ となる自然数 m が存在する。したがって,

$$\begin{aligned} X^4 + 1 &= (X^2 + 1)^2 - 2X^2 \\ &\equiv (X^2 + 1)^2 - m^2 X^2 \pmod{p} \\ &= (X^2 + mX + 1)(X^2 - mX + 1) \end{aligned}$$

(おわり)

(注) 問題では p を奇素数としているが, $p = 2$ のときは

$$X^4 + 1 \equiv X^4 - 1 \equiv (X^2 + 1)(X^2 - 1) \pmod{p}$$

となつて, 同様の結果が成り立つ。