10　Fermat の (小) 定理, Euler の定理, $(\mathbb{Z}/m\mathbb{Z})^\times$ の元の位数, 原始根

10.1　解説編

定義 10.1. ($(\mathbb{Z}/m\mathbb{Z})^\times$ **の元の位数**)　m を 2 以上の自然数, a を m と互いに素な整数とする. $a^k \equiv 1 \mod m$ をみたす最小の自然数 k を, **法 m に関する a の位数** または a **mod** m **の位数**という. Euler の定理により $a^{\varphi(m)} \equiv 1 \mod m$ が成り立つから, このような自然数 k は存在する [1]. s を $a \bmod m$ の位数とする. 位数 s は定義により次の 2 条件で特徴付けられる:

(1) $k \in \mathbb{N}, 1 \leq k < s \Longrightarrow a^k \not\equiv 1 \mod m$.
(2) $a^s \equiv 1 \mod m$.

(既約) 剰余類の積の定義により, 任意の自然数 k に対して

$$\bar{a}^k = \underbrace{\bar{a}\cdots\bar{a}}_{k\text{ 個}} = \overline{\underbrace{a\cdots a}_{k\text{ 個}}} = \overline{a^k}$$

が成り立つ. したがって**問題 9.1(1)** により,

$$\bar{a}^k = \bar{1} \Longleftrightarrow \overline{a^k} = \bar{1} \Longleftrightarrow a^k \equiv 1 \mod m.$$

それで, $\bar{a}^k = \bar{1}$ をみたす最小の自然数 k も既約剰余類 $\bar{a}$ の位数と呼ぶ.

m の素因数分解を $m = p_1^{e_1}\cdots p_r^{e_r}$ と書く. ここで e_j たちは自然数, $p_1, \ldots, p_r$ はどの 2 つも相異なる素数である.

$$\psi(m) := \mathrm{lcm}(\varphi(p_1^{e_1}), \cdots, \varphi(p_r^{e_r})),$$
$$\lambda(m) := \max\{\alpha \text{ の位数} \mid \alpha \in (\mathbb{Z}/m\mathbb{Z})^\times\}$$

と定義する. そのとき, $\lambda(m) \mid \psi(m) \mid \varphi(m)$ が成り立つ (**講義プリント第 9 章**を参照).　□

定義 10.2. (**mod** m **の原始根**)　m を 2 以上の自然数, g を m と互いに素な整数とする. $\bar{g}$ の位数が $\varphi(m)$ となるとき, 整数 g は**法 m に関する原始根**または **mod** m **の原始根**と呼ばれる. 既約剰余類群 $(\mathbb{Z}/m\mathbb{Z})^\times$ が原始根をもつための必要十分条件は m の形が,

$$m = 2,\ 4,\ p^e \text{ または } 2p^e$$

となることである. ここで e は自然数, p は奇素数 ($p \neq 2$). これは Gauss(1801) による結果である.　□

[1] あるいは a のべき $a, a^2, a^3, \cdots \pmod m$ を計算して行くと, $(\mathbb{Z}/m\mathbb{Z})^\times$ は有限集合だからいつかは mod m で同じものが出てきて, これにより位数の存在がわかる. しかし, Euler の定理は $\varphi(m)$ 乗すると必ず mod m で 1 と合同になるという強い主張をしている.

10.2 問題編

問題 10.1. Fermat の小定理を使って次の問いに答えよ.

(1) 自然数 3^{4^5} を 7 で割った余りを求めよ.

(2) 和 $\sum_{k=1}^{100} k^{100}$ を素数 101 で割ったときの余りを求めよ.

問題 10.2. (**チャレンジ問題**)　素数 p が $p \equiv 3 \mod 4$ をみたすとき, 2 次合同式 $x^2 \equiv -1 \mod p$ は整数解をもたないことを示せ.
(ヒント: Fermat の小定理を使う.)

問題 10.3. 奇素数 (odd prime) とは, 「奇数である素数」つまり, 「2 以外の素数」のことである. p, q を相異なる奇素数とする.

(1) 2 次合同式 $x^2 \equiv 1 \mod p$ の整数解は $x \equiv \pm 1 \mod p$ のみであることを証明せよ.
(ヒント: **講義プリントの命題 4.2**.)

(2) 2 次合同式 $x^2 \equiv 1 \mod 9$ の整数解は $x \equiv \pm 1 \mod 9$ のみであることを確かめよ.

(3) 2 次合同式 $x^2 \equiv 1 \mod p^2$ の整数解は $x \equiv \pm 1 \pmod{p^2}$ のみであることを証明せよ.

(4) 2 次合同式 $x^2 \equiv 1 \mod 15$ の整数解をすべて求めよ.

(5) (**チャレンジ問題**)　2 次合同式 $x^2 \equiv 1 \mod pq$ は pq を法として 4 つの整数解をもつことを示せ.

問題 10.4. Euler の定理を使って次の問いに答えよ.

(1) 12^{345} を 121 で割った余りを求めよ.　(2) 7^{2011} の下 2 桁を求めよ.

問題 10.5. p, q を相異なる素数とする. 次の問いに答えよ.

(1) $k \equiv 1 \mod p-1$ かつ $k \equiv 1 \mod q-1$ をみたす自然数 k が無限に多く存在することを示せ.

(2) k を小問 (1) のような自然数とする. このとき, 任意の整数 a に対して, $a^k \equiv a \mod pq$ が成り立つことを示せ.

(3) 197^{157} を 35 で割ったときの余りを求めよ.

問題 10.6. 既約剰余類群 $(\mathbb{Z}/5\mathbb{Z})^\times$ の各元 $\bar{1}, \bar{2}, \bar{3}, \bar{4}$ の位数を求めよ. また原始根をすべて求めよ. その個数はいくつか答えよ.

問題 10.7. 既約剰余類群 $(\mathbb{Z}/10\mathbb{Z})^\times$ の各元の位数を求めよ. また原始根をすべて求めよ.

問題 10.8. 素因数分解 $24 = 2^3 \cdot 3^1$ により, $\varphi(24) = 2^2(2-1)(3-1) = 8$. よって, 既約剰余類群 $(\mathbb{Z}/24\mathbb{Z})^\times$ は 8 個の元をもつ. 各元の位数を求めよ.

$\bar{a}$	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\overline{11}$	$\overline{13}$	$\overline{17}$	$\overline{19}$	$\overline{23}$
$\bar{a}$ の位数								

また $\lambda(24)$ と $\psi(24)$ の値を計算せよ.

問題 10.9. 整数 g が素数 p を法として原始根であるとき, p を法とする剰余類の集合の間の次の等式を示せ:

$$\{\bar{g}, \bar{g}^2, \ldots, \bar{g}^{p-1}\} = \{\bar{1}, \bar{2}, \bar{3}, \ldots, \overline{p-1}\}.$$

(ヒント: 左辺の集合の元の個数を数える.)

問題 10.10. m を 2 以上の自然数, $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$ とする. $\bar{a}$ の位数を s とし, k を自然数とする. このとき, $\bar{a}^k$ の位数は $\dfrac{s}{\gcd(k,s)}$ となることを証明せよ. (**講義プリントの命題 9.9(2)** の一般化.)

問題 10.11. (**チャレンジ問題**)　p を素数, $\bar{a} \in (\mathbb{Z}/p\mathbb{Z})^\times$ とする. $\bar{a}$ の位数が 3 ならば $\overline{1+a}$ の位数は 6 になることを示せ.
(ヒント: $\bar{a}^3 - \bar{1} = \bar{0}$ を因数分解する.)

問題 10.12. p を素数とする. 問題 10.3(1) と問題 10.9 を使って, **Wilson の定理:**

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

を証明せよ.

問題 10.13. a を 2 以上の自然数とする. このとき $a \mid \{(a-1)! + 1\}$ が成り立つならば, a は素数となることを示せ. つまり, Wilson の定理の逆が成り立つ.

問題 10.14. (**チャレンジ問題**)　p を奇素数, n を $p-1$ で割り切れない自然数とする. このとき, 和 $\displaystyle\sum_{k=1}^{p-1} k^n$ は p で割り切れることを示せ.
(ヒント: 問題 10.9.)