

## 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.  $a^k \equiv 1 \pmod{m}$  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  $a \pmod{m}$  の位数という. Euler の定理により  $a^{\varphi(m)} \equiv 1 \pmod{m}$  が成り立つから, このような自然数  $k$  は存在する<sup>1</sup>.  $s$  を  $a \pmod{m}$  の位数とする. 位数  $s$  は定義により次の 2 つの条件で特徴付けられる.

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

(既約) 剰余類の積の定義により, 任意の自然数  $k$  に対して

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

が成り立つ. 一方問題 9.4(1) により,  $\bar{a}^k = \bar{1} \iff a^k \equiv 1 \pmod{m}$ . そこで,  $\bar{a}^k = \bar{1}$  をみたす最小の自然数  $k$  を既約剰余類  $\bar{a}$  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,  $p_1, \dots, p_r$  はどの 2 つも相異なる素数である.

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

と定義する.  $\lambda(m) \mid \psi(m) \mid \varphi(m)$  が成り立つ. □

**定義 10.2.** ( $\pmod{m}$  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  $\varphi(m)$  となる時, 整数  $g$  は法  $m$  に関する原始根または  $\pmod{m}$  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. □

---

<sup>1</sup>あるいは  $a$  のべき  $a, a^2, a^3, \dots \pmod{m}$  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  $\pmod{m}$  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  $\pmod{m}$  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.

- (1) 自然数  $3^{45}$  を 7 で割った余りを求めよ.
- (2)  $111^{333} + 333^{111}$  は 7 で割り切れることを示せ.
- (3) 任意の自然数  $n$  について,  $3^{n+2} + 4^{2n+1}$  は 13 で割り切れることを示せ.
- (4) 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  $p \equiv 3 \pmod{4}$  をみたすとき, 2 次合同式  $x^2 \equiv -1 \pmod{p}$  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  $x^2 \equiv 1 \pmod{p}$  の整数解は  $x \equiv \pm 1 \pmod{p}$  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  $x^2 \equiv 1 \pmod{9}$  の整数解は  $x \equiv \pm 1 \pmod{9}$  のみであることを確かめよ.
- (3) 2 次合同式  $x^2 \equiv 1 \pmod{p^2}$  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  $x^2 \equiv 1 \pmod{15}$  の整数解をすべて求めよ.
- (5) (チャレンジ問題) 2 次合同式  $x^2 \equiv 1 \pmod{pq}$  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)  $k \equiv 1 \pmod{p-1}$  かつ  $k \equiv 1 \pmod{q-1}$  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,  $a^k \equiv a \pmod{pq}$  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.

$\bar{a}$	$\bar{1}$	$\bar{5}$	$\bar{7}$	$\bar{11}$	$\bar{13}$	$\bar{17}$	$\bar{19}$	$\bar{23}$
$\bar{a}$ 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:

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

(ヒント: 講義プリントの命題 9.9(1). 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  $\frac{s}{\gcd(k, s)}$  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:

$$(p-1)! \equiv -1 \pmod{p}$$

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)  $p$  を素数,  $n$  を  $p-1$  で割り切れない自然数とする. このとき, 和  $\sum_{k=1}^{p-1} k^n$  は  $p$  で割り切れることを示せ.