

## 11 二次合同式と平方剰余記号

### オイラーの $\varphi$ 関数

自然数  $n$  に対して,  $n$  未満の非負整数のうち  $n$  と互いに素なものの個数を  $\varphi(n)$  で表す. すなわち,

$$\varphi(n) = \#\{a \in \mathbb{Z} \mid 0 \leq a < n, \gcd(a, n) = 1\}$$

である. これにより定まる関数  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  をオイラーの  $\varphi$  関数 (Euler  $\varphi$ -function, Euler totient function) という.  $p$  が素数ならば,  $\varphi(p) = p - 1$  である. また,  $\varphi(1) = 1$  であることに注意する.

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a + n\mathbb{Z} \mid \gcd(a, n) = 1\}$$

と定義する. このとき,  $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$  である.

**注意.** 定理 10.4 より,  $(\mathbb{Z}/n\mathbb{Z})^\times$  は可換環  $\mathbb{Z}/n\mathbb{Z}$  の単元全体がなすアーベル群である.

**補題 11.1.**  $m, n$  を互いに素な自然数とする. 写像  $f: (\mathbb{Z}/mn\mathbb{Z})^\times \rightarrow (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$  を  $f(a + mn\mathbb{Z}) = (a + m\mathbb{Z}, a + n\mathbb{Z})$  で定義すると,  $f$  は well-defined であり, 全単射である.

**注意.** 補題 11.1 の  $f$  は群同型である.

**命題 11.2.**  $m, n$  を互いに素な自然数とする. このとき,  $\varphi(mn) = \varphi(m)\varphi(n)$  が成り立つ.

**系 11.3.**  $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$  と素因数分解されるとき,

$$\varphi(n) = \prod_{i=1}^r (p_i^{e_i} - p_i^{e_i-1}) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right).$$

**定理 11.4 (オイラー).**  $n$  を自然数,  $a$  を  $n$  と互いに素な整数とする. このとき, 次の式が成り立つ.

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

**系 11.5 (フェルマーの小定理 (Fermat's little theorem)).**  $p$  を素数,  $a$  を  $p$  で割り切れない整数とする. このとき, 次の式が成り立つ.

$$a^{p-1} \equiv 1 \pmod{p}.$$

### 原始根

$n$  を自然数とする.  $n$  と互いに素な整数  $a$  に対して,  $a^r \equiv 1 \pmod{n}$  となる最小の自然数  $r$  を,  $a$  の位数 (order) という.  $a$  の位数が  $\varphi(n)$  に等しいとき,  $a$  を  $n$  を法とする原始根 (primitive root) という.

**注意.**  $a$  の位数  $r$  は  $a + n\mathbb{Z}$  の群  $(\mathbb{Z}/n\mathbb{Z})^\times$  における位数である.  $a$  が  $n$  を法とする原始根であることは,  $a + n\mathbb{Z}$  が群  $(\mathbb{Z}/n\mathbb{Z})^\times$  の生成元であることに他ならない. このとき,  $(\mathbb{Z}/n\mathbb{Z})^\times \cong \mathbb{Z}/\varphi(n)\mathbb{Z}$  である.

**定理 11.6.** 任意の素数  $p$  に対して,  $p$  を法とする原始根が存在する.

## 平方剰余記号

以下,  $p$  を奇素数とする.

$a$  を  $p$  と互いに素な整数とする. 合同式  $x^2 \equiv a \pmod{p}$  を満たす整数  $x$  が存在するとき,  $a$  を  $p$  を法とする平方剰余 (quadratic residue) といい, そうでないとき,  $a$  を  $p$  を法とする平方非剰余 (quadratic non-residue) という.

整数  $a$  に対して, ルジャンドル記号 (Legendre symbol) を次のように定義する.

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & (a \text{ が } p \text{ で割り切れるとき}), \\ 1 & (a \text{ が } p \text{ を法とする平方剰余のとき}), \\ -1 & (a \text{ が } p \text{ を法とする平方非剰余のとき}). \end{cases}$$

定理 11.7 (オイラーの規準 (Euler's criterion)).  $a$  を整数とする. このとき, 次の式が成り立つ.

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

命題 11.8.  $a, b$  を整数とする.

(a)  $a \equiv b \pmod{p}$  ならば,  $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ .

(b)  $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$ .