

11. 平方剰余の相互法則

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 を法 p に関する平方剰余といい, そうでないとき, a を法 p に関する平方非剰余という.
- 整数 a に対して, ルジャンドル記号を次のように定義する.

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

- a を整数とする. 次のオイラーの規準が成り立つ.

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

- n を正の奇数とし, $n = \prod_{i=1}^r p_i^{e_i}$ と素因数分解されているとする (p_1, \dots, p_r は相異なる素数). 整数 a に対して, ヤコビ記号を次のように定義する.

$$\left(\frac{a}{n}\right) = \prod_{i=1}^r \left(\frac{a}{p_i}\right)^{e_i}. \quad (n = 1 \text{ のとき, } \left(\frac{a}{n}\right) = 1 \text{ とする.})$$

n が奇素数ならば, ルジャンドル記号とヤコビ記号は一致する.

- a, b を整数, m, n を正の奇数とするとき, 次の性質が成り立つ.

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

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

(3) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right)$.

(4) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.

(5) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

(6) m と n が互いに素ならば, $\left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = (-1)^{(m-1)(n-1)/4}$.

m, n が異なる奇素数であるとき, (4) を第一補充法則, (5) を第二補充法則, (6) を平方剰余の相互法則という.

問題

解答に際して、その問題より前にある問題の結果を用いてもよい。

11-1. 1 から 16 までの自然数のうち、法 17 に関する平方剰余であるものをすべて挙げよ。

11-2. p を奇素数とする。1 から $p-1$ までの自然数のうち、 p を法とする平方剰余であるものは $\frac{p-1}{2}$ 個であることを示せ。

11-3. m, n を奇数とする。次の等式を示せ。

$$(a) \quad (-1)^{(n-1)/2} = \begin{cases} 1 & (n \equiv 1 \pmod{4}), \\ -1 & (n \equiv 3 \pmod{4}). \end{cases}$$

$$(b) \quad (-1)^{(n^2-1)/8} = \begin{cases} 1 & (n \equiv 1, 7 \pmod{8}), \\ -1 & (n \equiv 3, 5 \pmod{8}). \end{cases}$$

$$(c) \quad (-1)^{(m-1)(n-1)/4} = \begin{cases} 1 & (m \equiv 1 \pmod{4} \text{ または } n \equiv 1 \pmod{4}), \\ -1 & (m \equiv n \equiv 3 \pmod{4}). \end{cases}$$

11-4. ルジャンドル記号 $\left(\frac{277}{419}\right)$ の値を求めよ。

11-5. ヤコビ記号 $\left(\frac{478}{737}\right)$ の値を求めよ。

11-6. 素数 p と整数 a は $p \equiv 3 \pmod{4}$, $\left(\frac{a}{p}\right) = 1$ を満たすとする。このとき、 $x \equiv a^{(p+1)/4} \pmod{p}$ を満たす整数 x に対して、 $x^2 \equiv a \pmod{p}$ が成り立つことを示せ。

11-7. 合同式 $x^2 \equiv 2 \pmod{23}$ を満たす整数 x で、 $0 \leq x < 23$ を満たすものをすべて求めよ。

11-8. $\left(\frac{a}{35}\right) = 1$ であるが $x^2 \equiv a \pmod{35}$ が解を持たない整数 a を一つ求めよ。