

12 平方剰余の相互法則

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

平方剰余の相互法則

定理 12.1. p, q を相異なる素数とする. 次の等式が成り立つ.

- (a) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.
- (b) $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.
- (c) $\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$.

定理 12.1 において, (a) を第 1 補充法則 (first complementary law), (b) を第 2 補充法則 (second complementary law), (c) を平方剰余の相互法則 (quadratic reciprocity law) という.

注意. 平方剰余の相互法則はガウスによって初めて厳密に証明された. 現在では 200 種類以上の証明が知られているが, 本講義では参考書 [1] に従って, Rousseau [2] による中国剰余定理を用いた証明を紹介する. また, 第 2 補充法則は次に述べるヤコビ記号に拡張して, 数学的帰納法により平方剰余の相互法則と第 1 補充法則から証明する.

ヤコビ記号

n を正の奇数とし, $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ と素因数分解されているとする (p_1, p_2, \dots, p_r は相異なる素数). 整数 a に対して, ヤコビ記号 (Jacobi symbol) を次のように定義する.

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

ただし, $n = 1$ のときは $\left(\frac{a}{n}\right) = 1$ 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.

定理 12.2. a, b を整数, m, n を正の奇数とする. 次の性質が成り立つ.

- (a) $a \equiv b \pmod{n}$ ならば, $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.
- (b) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \left(\frac{b}{n}\right)$.
- (c) $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right) \left(\frac{a}{n}\right)$.
- (d) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.
- (e) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.
- (f) m と n が互いに素ならば, $\left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = (-1)^{(m-1)(n-1)/4}$.

定理 12.2 を用いると, ユークリッドの互除法と同様にして, 素因数分解を用いずにヤコビ記号を計算できる. 計算の際, 次の命題が便利である.

命題 12.3. m, n を正の奇数とする. 次の等式が成り立つ.

- (a) $(-1)^{(n-1)/2} = \begin{cases} 1 & (n \equiv 1 \pmod{4}), \\ -1 & (n \equiv 3 \pmod{4}). \end{cases}$
- (b) $(-1)^{(n^2-1)/8} = \begin{cases} 1 & (n \equiv 1, 7 \pmod{8}), \\ -1 & (n \equiv 3, 5 \pmod{8}). \end{cases}$
- (c) $(-1)^{(m-1)(n-1)/4} = \begin{cases} 1 & (m \equiv 1 \pmod{4} \text{ または } n \equiv 1 \pmod{4}), \\ -1 & (m \equiv n \equiv 3 \pmod{4}). \end{cases}$

定理 12.4. a を整数, n を正の奇数として, $0 \leq a < n$ とする. このとき, $\left(\frac{a}{n}\right)$ を求めるのに必要なビット演算量は $O(\log^3 n)$ である.

注意. ユークリッドの互除法と同様に, 計算量を精密に評価することで, ビット演算量が $O((\log a)(\log n)) = O(\log^2 n)$ であることがわかる. また, より高速な乗除算アルゴリズムを用いた場合は, 計算量が減少する.

参考文献

- [1] 中村憲 『数論アルゴリズム』 (朝倉書店, 2009).
- [2] G. Rousseau, On the quadratic reciprocity law, J. Austral. Math. Soc. Ser. A **51** (1991), 423–425.