アルゴリズム B 演習 No. 11 2014 年 1 月 10 日配布

11. 平方剰余の相互法則

以下，p を 2 でない素数とする．

- p と互いに素な整数 a が，ある整数 x の平方と p を法として合同となる，すなわち，$x^2 \equiv a \pmod{p}$ となるとき，a を法 p に関する**平方剰余** (quadratic residue) という．p と互いに素な整数 a が法 p に関する平方剰余でないとき，a を法 p に関する**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** (Euler's criterion) 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（$p_1, \ldots, p_n$ 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．

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

  n が 2 でない素数ならば，ルジャンドル記号とヤコビ記号は一致する．
- m, n を正の奇数とする．このとき，ヤコビ記号について次が成り立つ．
  (a) $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.
  (b) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.
  (c) $\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4} \left(\frac{n}{m}\right)$.
  (c) において，m, n が異なる素数である場合，ルジャンドル記号に関する等式を得る．これを**平方剰余の相互法則** (quadratic reciprocity law) という．

注意． n が素数でないとき，ヤコビ記号 $\left(\frac{m}{n}\right)$ が 1 に等しくても，合同式

$$X^2 \equiv m \pmod{n}$$

を満たす整数 X が存在するとは限らない．（問題 11-7 参照．）

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 18 までの自然数のうち，法 19 に関する平方剰余であるものをすべて挙げよ.

11-2. n を奇数とする．次の式を示せ.

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

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

11-3. m, n を奇数とする．次の 2 つが同値であることを示せ.

(a) $m \equiv 3 \pmod 4$ かつ $n \equiv 3 \pmod 4$.

(b) $(-1)^{(m-1)(n-1)/4} = -1$.

11-4. ルジャンドル記号 $\left(\dfrac{43}{233}\right)$ の値を求めよ.

11-5. ヤコビ記号 $\left(\dfrac{116}{645}\right)$ の値を求めよ.

11-6. 次の合同式の解の個数を求めよ.（注意：941 は素数である.）

$$X^2 \equiv 568 \pmod{941}.$$

11-7. (a) ヤコビ記号 $\left(\dfrac{8}{15}\right)$ の値を求めよ.

(b) 次の合同式を満たす整数 X は存在しないことを示せ.

$$X^2 \equiv 8 \pmod{15}.$$

11-8. p を $p \equiv 3 \pmod 4$ を満たす素数，a を整数とし，$\left(\dfrac{a}{p}\right) = 1$ とする．このとき，整数 x が $x \equiv a^{(p+1)/4} \pmod p$ を満たすならば，$x^2 \equiv a \pmod p$ となることを示せ.

11-9. 11-8 を用いて，次の合同式を満たす整数 X で，$0 \leq X < 83$ を満たすものをすべて求めよ.

$$X^2 \equiv -2 \pmod{83}.$$