アルゴリズム B 演習 No. 11　　2018 年 1 月 5 日配布

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（$p_1, \ldots, p_n$ 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．

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

  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. m, n を奇数とする．次の等式を示せ．

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

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

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

11-2. ルジャンドル記号 $\left(\dfrac{215}{691}\right)$ の値を求めよ．

11-3. ヤコビ記号 $\left(\dfrac{479}{915}\right)$ の値を求めよ．

11-4. p を奇素数，a を $0 < a < p$ を満たす整数とする．ルジャンドル記号 $\left(\dfrac{a}{p}\right)$ を計算するときのビット演算量は $O((\log p)^3)$ であることを示せ．ただし，四則演算のビット演算量として，No. 8 で与えたものを使うものとする．

11-5. 素数 p と整数 a は $p \equiv 3 \pmod 4$, $\left(\dfrac{a}{p}\right) = 1$ 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．

11-6. 合同式 $x^2 \equiv 14 \pmod{31}$ を満たす整数 x で，$0 \leq x < 31$ を満たすものをすべて求めよ．

11-7. p を奇素数，整数 a を法 p に関する平方剰余として，整数 x_1 は $x_1^2 \equiv a \pmod p$ を満たすとする．整数 $x_2, x_3, \ldots, y_1, y_2, \ldots$ がすべての $n = 1, 2, \ldots$ に対して

$$2x_1 y_n \equiv \frac{a - x_n^2}{p^n} \pmod p, \quad x_{n+1} \equiv x_n + p^n y_n \pmod{p^{n+1}}$$

を満たすとする．このとき，すべての $n = 1, 2, \ldots$ に対して $x_n \equiv x_1 \pmod p$, $x_n^2 \equiv a \pmod{p^n}$ が成り立つことを示せ．

11-8. $x^2 \equiv 354 \pmod{625}$ を満たす整数 x を一つ求めよ．