アルゴリズム B 演習 No. 11　　2015 年 12 月 18 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．

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

- 相異なる奇素数 p, q に対して次の等式が成り立つ．
  (1)（**第一補充法則**）$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.
  (2)（**第二補充法則**）$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.
  (3)（**平方剰余の相互法則**）$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$.
- 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．

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．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．

11-1. 1 から 10 までの自然数のうち，法 11 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） $(-1)^{(n^2-1)/8} = \begin{cases} 1 & (n \equiv 1, 7 \pmod 8), \\ -1 & (n \equiv 3, 5 \pmod 8). \end{cases}$

11-3. m, n を奇数，a, b を整数とする．ヤコビ記号に関する以下の性質を示せ．

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

11-4. m, n を奇数とする．以下の合同式を示せ．

（a） $mn - 1 \equiv (m-1) + (n-1) \pmod 4$.

（b） $m^2n^2 - 1 \equiv (m^2-1) + (n^2-1) \pmod{16}$.

11-5. m, n を互いに素な奇数とする．ヤコビ記号に関する以下の性質を示せ．

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

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

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

11-6. ルジャンドル記号 $\left(\frac{177}{433}\right)$ の値を求めよ．

11-7. ヤコビ記号 $\left(\frac{198}{749}\right)$ の値を求めよ．

11-8. n を正の奇数，a を $0 < a < n$ を満たす整数とする．問題 11-5 の等式を用いてヤコビ記号 $\left(\frac{a}{n}\right)$ を計算するときのビット演算量は $O((\log n)^3)$ であることを示せ．

11-9. 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．

11-10. 以下の問いに答えよ．

（a） ルジャンドル記号 $\left(\frac{3}{47}\right)$ の値を求めよ．

（b） 合同式 $x^2 \equiv 3 \pmod{47}$ を満たす整数 x で，$0 \le x < 47$ を満たすものをすべて求めよ．