アルゴリズム B 演習 No. 10 2012 年 12 月 21 日配布

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

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

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

  (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．

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．

10-1. 法 17 に関する平方剰余をすべて挙げよ．

10-2. p を 2 でない素数とする．$1 \leq a \leq p-1$ の範囲に平方剰余となる a は $(p-1)/2$ 個あることを示せ．

10-3. 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) $(-1)^{(n^2-1)/8} = \begin{cases} 1 & (n \equiv 1, 7 \pmod 8), \\ -1 & (n \equiv 3, 5 \pmod 8). \end{cases}$

10-4. p を 2 でない素数とする．整数 a について，合同式

$$X^2 \equiv a \pmod p$$

の解の個数を N とする．次の式が成り立つことを示せ．

$$N = 1 + \left(\frac{a}{p}\right).$$

10-5. p を 2 でない素数，a, b を整数とする．ルジャンドル記号について，次が成り立つことを示せ．

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

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

10-6. m, n を奇数，a, b を整数とする．ヤコビ記号について，次が成り立つことを示せ．

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

10-7. ルジャンドル記号 $\left(\frac{91}{313}\right)$ の値を求めよ．

10-8. 次の合同式の解の個数を求めよ．

$$X^2 \equiv 531 \pmod{751}.$$

10-9. p を $p \equiv 3 \pmod 4$ を満たす素数，a を整数とし，$\left(\frac{a}{p}\right) = 1$ 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．

10-10. 10-9 を用いて，次の合同式を満たす整数 X で，$0 \leq X < 103$ を満たすものをすべて求めよ．

$$X^2 \equiv 2 \pmod{103}.$$