ヤコビの記号

文字は全て整数とする．p, q は 奇素数 とする．

定義 1 $n > 1$ が奇数で，$n = pp'p'' \cdots$ と素因数分解できるとき，$(m, n) = 1$ なる整数について（m は負でもかまわない）

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p}\right)\left(\frac{m}{p'}\right)\left(\frac{m}{p''}\right)\cdots$$

左辺の記号を**ヤコビの記号**という．右辺に記したのはルジャンドルの記号である．

ヤコビの記号 $\left(\frac{m}{n}\right)$ が 1 に等しいことは，必ずしも n を法として m が平方剰余であるということではない．m が n を法として平方剰余であるためには，$p, p', p'' \cdots$ 全ての法について平方剰余であることが必要である．しかしながら $\left(\frac{m}{p}\right), \left(\frac{m}{p'}\right), \left(\frac{a}{p''}\right), \cdots$ のうち偶数個が -1 であってもヤコビの記号は 1 となりこの場合は m は平方剰余ではないからである．またヤコビの記号 $\left(\frac{m}{n}\right)$ が -1 に等しいときは m は n を法として平方剰余ではない．なぜならば $\left(\frac{m}{p}\right), \left(\frac{m}{p'}\right), \left(\frac{a}{p''}\right), \cdots$ のうち少なくとも 1 つの -1 が含まれるからである．

定理 1 $m \equiv m' \pmod{n}$ であるとき，（この部分 [1] に誤植あり，$\equiv$ が $=$ になっている）

$$\left(\frac{m}{n}\right) = \left(\frac{m'}{n}\right)$$

［証明］$n = pp'p'' \cdots = \Pi p$ とすると，

$$\begin{aligned} m &\equiv m' \pmod{p} \\ m &\equiv m' \pmod{p'} \\ m &\equiv m' \pmod{p''} \\ &\cdots \end{aligned}$$

つまり

$$\begin{aligned} \left(\frac{m}{p}\right) &= \left(\frac{m'}{p}\right) \\ \left(\frac{m}{p'}\right) &= \left(\frac{m'}{p'}\right) \\ \left(\frac{m}{p''}\right) &= \left(\frac{m'}{p''}\right) \\ &\cdots \end{aligned}$$

よって

$$\begin{aligned} \prod\left(\frac{m}{p}\right) &= \prod\left(\frac{m'}{p}\right) \\ \therefore \left(\frac{m}{n}\right) &= \left(\frac{m'}{n}\right) \end{aligned}$$

［証明おわり］

定理 2

$$\left(\frac{mm'}{n}\right) = \left(\frac{m}{n}\right)\left(\frac{m'}{n}\right)$$

［証明］

$$\begin{aligned}\left(\frac{mm'}{n}\right) &= \prod\left(\frac{mm'}{p}\right)\\ &= \prod\left(\frac{m}{p}\right)\left(\frac{m'}{p}\right)\\ &= \prod\left(\frac{m}{p}\right)\prod\left(\frac{m'}{p}\right)\\ &= \left(\frac{m}{n}\right)\left(\frac{m'}{n}\right)\end{aligned}$$

［証明おわり］

次にルジャンドルの記号の場合の第一補充法則に相当する定理を示す.

定理 3 n が正の奇数であるとき,

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

［証明］a, b を奇数とすると,

$$(a-1)(b-1) \equiv 0 \pmod 4$$

$$ab - 1 \equiv a - 1 + b - 1 \pmod 4$$

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod 2$$

c も奇数ならば

$$\frac{abc-1}{2} \equiv \frac{a-1}{2} + \frac{bc-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} + \frac{c-1}{2} \pmod 2$$

$n = pp'p'' \cdots$ とすると

$$\frac{n-1}{2} \equiv \frac{pp'p'' \cdots - 1}{2} \equiv \frac{p-1}{2} + \frac{p'-1}{2} + \frac{p''-1}{2} \cdots \pmod 2$$

$$\begin{aligned}\left(\frac{-1}{n}\right) &= \prod\left(\frac{-1}{p}\right)\\ &= \prod(-1)^{\frac{p-1}{2}}\\ &= (-1)^{\sum\frac{p-1}{2}}\\ &= (-1)^{\frac{n-1}{2}}\end{aligned}$$

［証明おわり］

次にルジャンドルの記号の場合の平方剰余の相互法則に相当する定理を示す.

定理 4 m, n が正の奇数であるとき,

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$$

［証明］

$$\left(\frac{m}{n}\right)=\prod^{p}\left(\frac{m}{p}\right)=\prod^{p}\prod^{q}\left(\frac{q}{p}\right)$$

同様に

$$\left(\frac{n}{m}\right)=\prod^{q}\prod^{p}\left(\frac{p}{q}\right)$$

$$\begin{aligned}\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)&=\prod^{q}\prod^{p}\left(\frac{p}{q}\right)\left(\frac{p}{q}\right)\\&=\prod^{q}\prod^{p}(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\\&=(-1)^{\sum\frac{p-1}{2}\sum\frac{q-1}{2}}\end{aligned}$$

前定理の証明において示したように

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{m-1}{2}\frac{n-1}{2}}$$

［証明おわり］

次にルジャンドルの記号の場合の第二補充法則に相当する定理を示す.

定理 5 n が正の奇数であるとき,

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

［証明］a,b を奇数とすれば,

$$(a^2-1)(b^2-1)\equiv 0 \pmod{16}$$

左辺を展開して適当に移項すると,

$$a^2b^2-1\equiv a^2-1+b^2-1 \pmod{16}$$

$$\therefore \frac{a^2b^2-1}{8}\equiv\frac{a^2-1}{8}+\frac{b^2-1}{8} \pmod 2$$

$$\therefore \frac{n^2-1}{8}\equiv\sum^{p}\frac{p^2-1}{8} \pmod 2$$

$$\therefore \left(\frac{2}{n}\right)=\prod\left(\frac{2}{p}\right)=(-1)^{\sum\frac{p^2-1}{8}}=(-1)^{\frac{n^2-1}{8}}$$

問題 1 $n\equiv 1,3 \pmod 8$ のとき $\left(\frac{-2}{n}\right)=1$ であることを証明せよ.

［解］$n\equiv 1 \pmod 8$ のとき $\frac{n-1}{2}\equiv 0 \pmod 2$, $\frac{n^2-1}{8}\equiv 0 \pmod 2$

$$\left(\frac{-2}{n}\right)=1$$

$n \equiv 3 \pmod 8$ のとき $\dfrac{n-1}{2} \equiv 1 \pmod 2, \dfrac{n^2-1}{8} \equiv 1 \pmod 2$

$$\left(\frac{-2}{n}\right) = 1$$

［証明おわり］

問題 2 $n \equiv 5, 7 \pmod 8$ のとき $\left(\dfrac{-2}{n}\right) = -1$ であることを証明せよ.

［解］$n \equiv 5 \pmod 8$ のとき $\dfrac{n-1}{2} \equiv 0 \pmod 2, \dfrac{n^2-1}{8} \equiv 1 \pmod 2$

$$\left(\frac{-2}{n}\right) = -1$$

$n \equiv 7 \pmod 8$ のとき $\dfrac{n-1}{2} \equiv 1 \pmod 2, \dfrac{n^2-1}{8} \equiv 0 \pmod 2$

$$\left(\frac{-2}{n}\right) = -1$$

［証明おわり］

問題 3 $\left(\dfrac{365}{1847}\right)$ を求めよ.

［解］$\dfrac{364}{2} = 182$ より

$$\left(\frac{365}{1847}\right) = \left(\frac{1847}{365}\right) = \left(\frac{22}{365}\right) = \left(\frac{2}{365}\right)\left(\frac{11}{365}\right)$$

$\dfrac{365^2-1}{8} = 16653$ より

$$\left(\frac{2}{365}\right)\left(\frac{11}{365}\right) = -\left(\frac{11}{365}\right) = -\left(\frac{365}{11}\right) = -\left(\frac{2}{11}\right)$$

$\dfrac{11^2-1}{8} = 15$ より

$$-\left(\frac{2}{11}\right) = 1$$

定理 6 m が平方数でないならば，m を法とする $\phi(m)$ 個の既約類のうち，半数に属する n に対しては $\left(\dfrac{n}{m}\right) = 1$，他の半数に対しては $\left(\dfrac{n}{m}\right) = -1$ である.

［証明］定理 1 より m を法とする同一既約類に属する n に対して $\left(\dfrac{n}{m}\right)$ の値は一定である.

今，$\phi(m)$ この既約類の代表を $\left(\dfrac{m}{n}\right)$ の値によって $+$ の組と $-$ の組に分け,

$$a_1, a_2, a_3, \cdots, a_u : \quad \left(\frac{a}{n}\right) = +1$$

$$b_1, b_2, b_3, \cdots, b_v : \quad \left(\frac{b}{n}\right) = -1$$

とする．$a \equiv 1 \pmod{m}$ は $+$ の組に属するので $+$ の組は空ではない．また m は平方数ではないので必ず奇数冪の素数を含む．そのような素数を q とすると，

$$m = q^{2k+1}m', (m', q) = 1$$

とおける．q の非平方剰余は必ず存在し，その一つを b_0 とする．$(m', q) = 1$ なので q を法として b_0 と同じ剰余類に属しなおかつ m' を法として 1 と合同な整数 b が存在する．つまり

$$b \equiv b_1 \pmod{q}$$

$$b \equiv 1 \pmod{m'}$$

となる b が存在する．そのような b について

$$\left(\frac{b}{m}\right) = \left(\frac{b}{q}\right)^{2k+1}\left(\frac{b}{m'}\right) = (-1)^{2k+1}\left(\frac{1}{m'}\right) = -1$$

よって $\left(\frac{b}{m}\right) = -1$ となるような b は必ず存在する．つまり m を法とする既約類のうち u 個の $+$ の組と，v 個の $-$ の組が存在し，$u > 0, v > 0$ である．ここで一つの $-$ の組の b を考えると，

$$ba_1, ba_2, ba_3, \cdots, ba_u,$$

$$bb_1, bb_2, bb_3, \cdots, bb_v,$$

は既約代表の一組である．

$$\left(\frac{ba_1}{m}\right) = \left(\frac{b}{m}\right)\left(\frac{a_1}{m}\right) = -1, \cdots$$

$$\left(\frac{bb_1}{m}\right) = \left(\frac{b}{m}\right)\left(\frac{b_1}{m}\right) = +1, \cdots$$

u 個の $-$ の組と，v 個の $+$ の組が存在する ことになる．つまり $u = v = \dfrac{\phi(m)}{2}$ である．　［証明おわり］

参考文献

[1] 高木貞治『初等整数論講義第 2 版」（共立出版社，1997 年）