平方剰余の相互法則
―ガウスによる第III証明―

明治大学理工学部数学科
竹田 慎吾

2010年2月23日

1　はじめに

ガウスは生涯に7通りのまったく趣の異なる平方剰余相互法則の証明を与えた。そのうちの6つは生前公表されたが、1つ（第VII証明）は死後公表された。私は初等整数論を学ぶ上で、ガウスがこの平方剰余の相互法則に非常に高い関心を持っていたことに興味を持ち、これを卒業論文のテーマにした。

1.1　平方剰余の相互法則

定義 1.1　a は整数で、p を2以外の素数とする。a と p が互いに素であるとする。$x^2 \equiv a \pmod{p}$ が整数解を持てば、a を p の平方剰余、そうでないときに平方非剰余という。$a \not\equiv 0 \pmod{p}$ であるとき、a が平方剰余であるか、または非剰余であるかに従って、それぞれ

$$\left(\frac{a}{p}\right) = +1 \text{ または } -1$$

とかく。これをルジャンドルの記号という。

平方剰余の相互法則は整数 a が奇素数 p を法として平方剰余であるか否かを見いだすための一つの法則である。

定理 1.2 (平方剰余の相互法則)　p、q を相異なる奇素数とするときに、

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

が成り立つ。

また、このほかに以下の第 1 補充法則、第 2 補充法則が知られている。

定理 1.3 (第 1 補充法則) p は奇素数とする、このとき次が成立する。

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

定理 1.4 (第 2 補充法則) p は奇素数とする、このとき次が成立する。

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

p と a、p と b が素であれば、

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

が成立することに注意する。一般に $\mathbb{Z}_p^\times = \{1, 2, \cdots, p-1\}$ は p を法として乗法に関して群になることが知られているが、この式は $\left(\frac{-}{p}\right)$ が $\mathbb{Z}_p^\times$ より $\{-1, 1\}$ への準同型写像であることを示している。故にその写像の核は位数 $(p-1)/2$ の部分群となり、$\mathbb{Z}_p^\times$ の要素の半分は平方剰余であり半分は平方非剰余であることが分かる。また、$\mathbb{Z}_p^\times$ は乗法に関して巡回群であることに注意すれば、p と k が互いに素であれば

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

であることがわかる。この式はオイラーの基準と呼ばれている。第 1 補充法則はこの式から直ちに従う。

平方剰余の相互法則は、レオンハルト・オイラーによって予想され、カール・フリードリッヒ・ガウスによって証明された（ガウスの日誌によれば、1796 年 4 月 8 日に証明され。発表されたのはおそらく 1801 年に出版された著書「整数論」において）。ガウスはこの法則に対して生涯で 7 つの異なる証明を与えた。その一つの動機は、三次や四次の相互法則を証明することにあった。現在では 200 近くもの証明が知られている。しかし、どれもそれほど簡単ではない。

1.2 平方剰余の相互法則の応用

1.2.1 $4k+1$ 型の素数は二個の平方数の和で表すことができる

$4k+1$ 型の素数は二個の平方数の和で表すことができる。また逆にある奇素数が二つの平方数の和で表すことができるならば、$4k+1$ 型の素数である。

$$
\begin{aligned}
5 &= 1^2 + 2^2 \\
13 &= 2^2 + 3^2 \\
17 &= 1^2 + 4^2 \\
29 &= 2^2 + 5^2 \\
37 &= 1^2 + 6^2 \\
41 &= 4^2 + 5^2 \\
53 &= 2^2 + 7^2 \\
61 &= 5^2 + 6^2
\end{aligned}
$$

逆は明らかである。$4k+1$ 型の素数は第 1 補充法則より $x^2 + 1^2 = kp$ と表すことができる。よって $x^2 + y^2 = kp \ \ (k > 1)$ と表せたとすれば、より小さい $k'(k > r' \geq 1)$ を選び $x'^2 + y'^2 = k'p$ とすることができるアルゴリズムが存在することを示せばよい。

証明 $p \equiv 1 \ (mod\ 4)$ より $\frac{p-1}{2}$ は偶数。オイラーの定理より p に関して $x^2 \equiv -1 \ (mod\ p)$ が解を持つことと、$p \equiv 1 \ (mod\ 4)$ は同値なので、

$$x^2 + 1 = kp \ \ (k = 1, 2, 3, \cdots)$$

とおくことができる。ここで $\frac{p}{2} < x < p$ とすると $x' = p - x$ とおけば $o < x' < \frac{p}{2}$ となり

$$x'^2 = p^2 - 2px + x^2 \equiv x^2 \equiv -1 \ (mod\ p)$$

である。つまり $0 < x < \frac{p}{2}$ のときを考えれば十分。では、あらためて

$$x^2 + 1 = kp \ (k = 1, 2, 3, \cdots)$$

$$0 < x < \frac{p}{2}$$

とできる。これは、$y = 1$ とおけば、

$$x^2 + y^2 = kp \quad \cdots (*)$$

が整数解 $(x, y) \ (0 < x, y < \frac{p}{2})$ を持つことを意味している。また $0 < x, y < \frac{p}{2}$ より

$$
\begin{aligned}
k &= \frac{x^2 + y^2}{p} \\
&< \frac{\left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2}{p} \\
&= \frac{p}{2}
\end{aligned}
$$

よって $k < p$ となる。$k = 1$ なら証明終わりなので $k > 1$ のときを考える。$k > 1$ のとき、$(*)$ の解 (x, y) で、x と y の k を法として合同な数で絶対値が最小のものをそれぞれ x_1、y_1 とおくと、

$$x_1^2 + y_1^2 \equiv 0 \ \ (mod\ k) \qquad (0 < x_1, y_1 \leq \frac{k}{2})$$

なので

$$x_1^2 + y_1^2 = k'k \quad \cdots (**)$$

とおくことができる。ここで、x、y の両方が k の倍数であるということはないので、$k' > 0$ である。このときもまた同様に、

$$\begin{aligned} k' &= \frac{x_1^2 + y_1^2}{k} \\ &\leq \frac{\frac{k}{2}^2 + \frac{k}{2}^2}{k} \\ &= \frac{k}{2} \\ &< k \end{aligned}$$

となる。$(*)$ と $(**)$ の積を考えると、

$$k'k^2 p = (x^2 + y^2)(x_1^2 + y_1^2) = (xx_1 + yy_1)^2 + (xy_1 - yx_1)^2$$

と変形できる。ここで右辺の各項は、

$$\begin{aligned} xx_1 + yy_1 &\equiv x^2 + y^2 \equiv 0\ (mod\ k) \\ xy_1 - yx_1 &\equiv xy - xy = 0\ (mod\ k) \end{aligned}$$

となる。よって、$x' = \frac{xx_1 + yy_1}{k}$、$y' = \frac{xy_1 - yx_1}{k}$ とおくことにより、

$$x'^2 + y'^2 = k'p$$

が得られる。 **証明終**

1.2.2 整数は四つの平方数の和に分解することができる

定理 1.5 全ての正の整数は、四つの平方数の和として表わすことができる :

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

上の定理において $0^2 = 0$ も平方数と考えている。よって、0 を除くならば四つ以下の平方数の和というべきである .

証明 恒等式

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2) &= (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2\\ &\quad +(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2\\ &\quad +(x_1y_3+x_2y_4-x_3y_1-x_4y_2)^2\\ &\quad +(x_1y_4-x_2y_3+x_3y_2-x_4y_1)^2\cdots(\sharp)\end{aligned}$$

によって、四つの平方数の和の積もまた、四つの平方数の和として表わされるから、定理を n が素数である場合に証明すればよい。$n=2$ のときは $2=1^2+1^2$ により明らか。p を奇素数とする。まず、p^2 より小さな p の倍数で、四つの平方数の和になっている数が存在することを示す。そのために $\frac{p+1}{2}$ 個の平方数

$$0^2, 1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2 \tag{1}$$

を考える。これらのどの 2 つも p を法として合同ではない。よって

$$-1, -1-1^2, -1-2^2, \cdots, -1-\left(\frac{p-1}{2}\right)^2 \tag{2}$$

も p を法として合同ではない。(1),(2) を合わせると全部で $p+1$ 個の数がある。よって部屋割り論法から p を法として同じ剰余類に入る数がある。すなわち

$$x_1^2 \equiv -1-x_2^2 \ (mod\ p),\ \ 0 \le x_i \le \frac{p-1}{2},\ \ i=1,2$$

となる整数 x_1, x_2 がある。これより、ある正の整数 h によって

$$x_1^2+x_2^2+1 = ph,\ \ 0 \le x_i \le \frac{p-1}{2},\ \ i=1,2 \tag{3}$$

と書ける。しかも

$$\begin{aligned}ph &= x_1^2+x_2^2+1\\ &\le \frac{(p-1)^2}{4}+\frac{(p-1)^2}{4}+1\\ &= \frac{(p-1)^2}{2}+1\\ &< \frac{(p-1)^2}{2}+\frac{(p-1)^2}{2}\\ &< p^2\end{aligned}$$

であるから $1 \le h < p$ である。今、

$$x_1^2+x_2^2+x_3^2+x_4^2 = ph,\ \ 1<h<p \tag{4}$$

とするとき、$0 < h' < h$ であるような整数 h' を適当にとって ph' が四つの平方数の和に分解できることを示す。これが示せれば (3) の形から、h が 1 になるまで上の操作を続けることにより、最後には p 自身の分解が得られる。(4) における x_1, x_2, x_3, x_4 を h で割り、絶対値において最小の剰余を y_1, y_2, y_3, y_4 とおいて

$$x_1 \equiv y_1, \quad x_2 \equiv y_2, \quad x_3 \equiv y_3, \quad x_4 \equiv y_4 \pmod{h} \tag{5}$$

$$|\, y_i \,| \leq \frac{h}{2}, \quad i = 1, 2, 3, 4 \tag{6}$$

とする。このとき

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{h}$$

である。よって、ある整数 $h' \geq 0$ によって

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = hh' \tag{7}$$

と書ける。これを冒頭に述べた恒等式 (♯) に代入すると

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 = ph^2h'$$

となる。ただし (5) によって

$$\begin{aligned}
z_1 &= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv \sum_{i=1}^{4} x_i^2 \equiv 0 \pmod{h} \\
z_2 &= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \equiv x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3 \equiv 0 \pmod{h} \\
z_3 &= x_1y_3 + x_2y_4 - x_3y_1 - x_4y_2 \equiv 0 \pmod{h} \\
z_4 &= x_1y_4 - x_2y_3 + x_3y_2 - x_4y_1 \equiv 0 \pmod{h}
\end{aligned}$$

となる。よって

$$z_1 = ht_1, z_2 = ht_2, z_3 = ht_3, z_4 = ht_4$$

とおけば

$$t_1^2 + t_2^2 + t_3^2 + t_4^2 = ph'$$

となる。さて、(6)、(7) によって

$$hh' = \sum_{i=1}^{4} y_i^2 \leq 4\left(\frac{h}{2}\right)^2 = h^2$$

故に $h' \leq h$ である。もし仮に等号が成り立つならば

$$y_i = \frac{h}{2}, \quad i = 1, 2, 3, 4$$

である。したがって $\frac{h}{2}$ は整数であり、h は偶数である。また $h > 1$ より各 i について $y_i \neq 0$。よって x_i は h の倍数にはなりえない。故に x_i は $\frac{h}{2}$ の奇数倍でなければならない。今

$$x_i = (2m_i + 1)\frac{h}{2}$$

とおき、(4) に代入すれば

$$\frac{h}{4}\sum_{i=1}^{4}(2m_i + 1)^2 = p$$

を得る。左辺は偶数だからこれは矛盾。したがって $h' < h$ である。最後に $h' \neq 0$ を示す。もし $h' = 0$ とすると (7) から $y_1 = y_2 = y_3 = y_4 = 0$ となる。よって (5) から

$$x_1 = hu_1, x_2 = hu_2, x_3 = hu_3, x_4 = hu_4$$

となる整数 u_1, u_2, u_3, u_4 が定まる。このとき (4) の両辺を h で割ると

$$h(u_1^2 + u_2^2 + u_3^2 + u_4^2) = p, \ \ 1 < h < p$$

となる。p は素数なのでこれは矛盾である。したがって $h' \neq 0$ となる。　**証明終**

2　相互法則の第 III 証明

定義 2.1 (最小剰余) $a \in \mathbb{Z}$ に対して、$a \equiv r \pmod m$, $0 \leq r < m$ となる $r \in \mathbb{Z}$ が唯一つ存在する。この r を a の m を法とする最小剰余と言う。

定義 2.2 (絶対値最小剰余) (1)　m を正の奇数とする。このとき、$a \in \mathbb{Z}$ に対して、$a \equiv r \pmod m$, $|r| \leq \frac{m-1}{2}$ となる $r \in \mathbb{Z}$ が丁度 1 つ存在する。この r を m を法とする絶対値最小剰余と言う。
(2)　m を正の偶数とする。このとき $a \in \mathbb{Z}$ に対して、$a \equiv r \pmod m$, $-\frac{m}{2} \leq r < \frac{m}{2}$ となる $r \in \mathbb{Z}$ が丁度 1 つ存在する。この r を m を法とする絶対値最小剰余と言う。

まず次を証明する。

補題 2.3 (ガウスの補題) p を奇素数、k を p で割り切れない整数とする。集合 A、B を次のように定める。

$$A = \left\{1, 2, 3, \cdots, \frac{1}{2}(p-1)\right\}$$

$$B = \left\{\frac{1}{2}(p+1), \frac{1}{2}(p+3), \cdots, p-1\right\}$$

k と A に含まれる数の積の最小正剰余 $(mod\ p)$ のうち B に属するものの個数を μ とする。このとき

$$\left(\frac{k}{p}\right) = (-1)^{\mu}$$

が成立する。

証明 k と A の元との積の最小正剰余を $r_1, r_2, \cdots, r_{\frac{1}{2}(p-1)}$ とする。($i, j \in A$ が $i \neq j$ なら $ki \not\equiv kj (mod\ p)$ であるので、$r_1, \cdots, r_{\frac{1}{2}(p-1)}$ は、互いに異なることに注意する。) $r_1, \cdots, r_{\frac{1}{2}(p-1)}$ のうち A に属するものを

$$a_1, a_2, \cdots, a_{\nu}$$

とし、B に入るものを

$$b_1, b_2, \cdots, b_{\mu}$$

としよう。すると $\nu + \mu = \frac{1}{2}(p-1)$ となる。このとき

$$p - b_1, p - b_2, \cdots, p - b_{\mu}$$

は全て異なり、$\frac{1}{2}(p-1)$ を越えず、かつ $a_1, a_2, \cdots, a_{\nu}$ とも異なる。なぜならもし $p - b_j = a_i$ となったとすれば

$$p - kj \equiv ki\ (mod\ p), 1 \leq i, j \leq \frac{1}{2}(p-1)$$

の形の式が成り立つから

$$k(i + j) \equiv 0\ (mod\ p)$$

となるが $p \nmid k$ だから $i + j \equiv 0\ \ (mod\ p)$ となる。ところが $i + j \leq p - 1$ だからこれは不可能である。

以上のことから $a_1, a_2, \cdots, a_{\nu}, p - b_1, p - b_2, \cdots, p - b_{\mu}$ は全体として A に一致する。ゆえに

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdots \frac{1}{2}(p-1) &= a_1 a_2 \cdots a_{\nu}(p - b_1)(p - b_2) \cdots (p - b_{\mu}) \\ &\equiv (-1)^{\mu} a_1 a_2 \cdots a_{\nu} b_1 b_2 \cdots b_{\mu} \\ &\equiv (-1)^{\mu} k^{\frac{1}{2}(p-1)} 1 \cdot 2 \cdot 3 \cdots \frac{1}{2}(p-1) \end{aligned}$$

となる。両辺を p と互いに素な $1 \cdot 2 \cdot 3 \cdots \frac{1}{2}(p-1)$ で割ると

$$1 \equiv (-1)^{\mu} k^{\frac{1}{2}(p-1)}$$

を得る。オイラーの基準により

$$k^{\frac{1}{2}(p-1)} \equiv \left(\frac{k}{p}\right)$$

が成立する。これから $\left(\frac{k}{p}\right) = (-1)^{\mu}$ が出る。 **証明終**

補題 2.4 x は、$x, 2x, 3x, \cdots, nx$ がいずれも非整数であるような正の実数とする。このとき $[nx] = h$ とおけば

$$\frac{1}{x}, \frac{2}{x}, \frac{3}{x}, \cdots, \frac{h}{x}$$

もまた非整数である ($\frac{i}{x} = j, i \leqslant h$ で i と j が整数なら、$j \leqslant n$ で $xj = i$ となるから) . このとき

$$[x] + [2x] + [3x] + \cdots + [nx] + \left[\frac{1}{x}\right] + \left[\frac{2}{x}\right] + \left[\frac{3}{x}\right] + \cdots + \left[\frac{h}{x}\right] = nh$$

である .

証明 $a_i = [ix]$ とおく。$\Omega = a_1 + a_2 + \cdots + a_n$ とする。このとき、

$$\begin{aligned}
a_i &= 0 \ \left(i = 1, 2, \cdots, \left[\frac{1}{x}\right]\right) \\
a_i &= 1 \ \left(i = \left[\frac{1}{x}\right] + 1, \cdots, \left[\frac{2}{x}\right]\right) \\
a_i &= 2 \ \left(i = \left[\frac{2}{x}\right] + 1, \cdots, \left[\frac{3}{x}\right]\right) \\
&\vdots \\
a_i &= h \ \left(i = \left[\frac{h}{x}\right] + 1, \cdots, n\right)
\end{aligned}$$

であるから、

$$\begin{aligned}
\Omega &= 0 \cdot \left[\frac{1}{x}\right] \\
&\quad +1 \cdot \left\{\left[\frac{2}{x}\right] - \left[\frac{1}{x}\right]\right\} \\
&\quad +2 \cdot \left\{\left[\frac{3}{x}\right] - \left[\frac{2}{x}\right]\right\} \\
&\quad +3 \cdot \left\{\left[\frac{4}{x}\right] - \left[\frac{3}{x}\right]\right\} \\
&\quad \vdots \\
&\quad +(h-1)\left\{\left[\frac{h}{x}\right] - \left[\frac{h-1}{x}\right]\right\} \\
&\quad +h\left\{n - \left[\frac{h}{x}\right]\right\} \\
&= h \cdot n - \left[\frac{1}{x}\right] - \left[\frac{2}{x}\right] - \left[\frac{3}{x}\right] - \cdots - \left[\frac{h}{x}\right].
\end{aligned}$$

証明終

命題 2.5 *k*,*p* を異なる奇素数とするとき

$$\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]+\cdots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]+\left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\left[\frac{3p}{k}\right]+\cdots+\left[\frac{\frac{1}{2}(k-1)p}{k}\right]$$
$$= \frac{1}{4}(k-1)(p-1)$$

証明 $k < p$ としても一般性は失わない。$\frac{1}{2}(k-1) < \frac{\frac{1}{2}(p-1)k}{p} < \frac{1}{2}k$ が成立する。($pk-p < pk-k$ より $p(k-1) < k(p-1)$, $\frac{\frac{1}{2}(p-1)k}{p} < \frac{1}{2}k$ は明らかである。). ゆえに

$$\left[\frac{\frac{1}{2}(p-1)k}{p}\right] = \frac{1}{2}(k-1)$$

となる。$\frac{k}{p} = x$, $\frac{1}{2}(p-1) = n$ とおいて補題 2.3 を適用する（このとき $h = \frac{1}{2}(k-1)$）.

$$\left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]+\cdots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]+\left[\frac{p}{k}\right]+\left[\frac{2p}{k}\right]+\left[\frac{3p}{k}\right]+\cdots+\left[\frac{\frac{1}{2}(k-1)p}{k}\right]$$
$$= \frac{1}{4}(k-1)(p-1)$$

となる。 **証明終**

3 第 III 証明 (ディリクレによる平易化)

補題 3.1 *p* は奇素数 , $p \nmid k$ とし、

$$L = \left[\frac{k}{p}\right]+\left[\frac{2k}{p}\right]+\left[\frac{3k}{p}\right]+\cdots+\left[\frac{\frac{1}{2}(p-1)k}{p}\right]$$

とおく。
(1) *k* が奇数のときは、

$$\left(\frac{k}{p}\right) = (-1)^L$$

となる。
(2) (第 2 補充法則) $k = 2$ のときは、

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

となる。

証明

$$\begin{aligned} k &= p\left[\frac{k}{p}\right] + r_1 \\ 2k &= p\left[\frac{2k}{p}\right] + r_2 \\ &\vdots \\ \frac{1}{2}(p-1)k &= p\left[\frac{\frac{1}{2}(p-1)k}{p}\right] + r_{\frac{1}{2}(p-1)} \end{aligned}$$

$r_1, r_2, \cdots, r_{\frac{1}{2}(p-1)}$ は、k と $A = \left\{1, 2, \cdots, \frac{1}{2}(p-1)\right\}$ の数の積の最小正剰余とする (補題 2.3)。$r_1, r_2, \cdots, r_{\frac{1}{2}(p-1)}$ のうち $\frac{p}{2}$ より小さいものを $a_1, a_2, \cdots, a_\nu$ とし、 $\frac{p}{2}$ よりも大きいものを $b_1, b_2, \cdots, b_\mu$ として、

$$A' = \sum_i a_i, \quad B' = \sum_j b_j$$

とおけば , 上式を加えて

$$\frac{1}{8}(p^2-1)k = pL + A' + B'$$

となる。$a_1, a_2, \cdots, a_\nu, p-b_1, p-b_2, \cdots, p-b_\mu$ は全体として $1, 2, \cdots, \frac{1}{2}(p-1)$ だったから

$$\frac{1}{8}(p^2-1) = 1 + 2 + 3 + \cdots + \frac{1}{2}(p-1) = A' + \mu p - B'.$$

これより

$$\frac{1}{8}(p^2-1)(k-1) = (L-\mu)p + 2B'.$$

上式を $mod\ 2$ で考えると, $p \equiv -1 \pmod 2$ だから

$$\mu \equiv L + \frac{1}{8}(p^2-1)(k-1) \pmod 2$$

を得る。よって、
(1) k が奇数のとき、$\mu \equiv L \pmod 2$ となる。ガウスの補題 (補題 2.3) より、

$$\left(\frac{k}{p}\right) = (-1)^L.$$

(第 2 補充法則)
(2) $k = 2$ のときは $L = 0$ だから $\mu \equiv \frac{1}{8}(p^2-1) \pmod 2$ であるので、ガウスの補題 補題 2.3 より、

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

が示された。
　平方剰余の相互法則の証明に戻る。
さて k, p を異なる奇素数とし

$$M = \left[\frac{p}{k}\right] + \left[\frac{2p}{k}\right] + \left[\frac{3p}{k}\right] + \cdots + \left[\frac{\frac{1}{2}(k-1)p}{k}\right]$$

とおけば、上と同様にして

$$\left(\frac{p}{k}\right) = (-1)^M$$

となる。命題 2.5 より

$$L + M = \frac{1}{4}(p-1)(k-1)$$

だから

$$\left(\frac{p}{k}\right)\left(\frac{k}{p}\right) = (-1)^{M+L} = (-1)^{\frac{1}{4}(p-1)(k-1)}$$

である。 **証明終**

参考文献

[1] 倉田令二朗、平方剰余の相互法則–ガウスの全証明– (日本評論社)

[2] 高木貞治、初等整数論講義　第２版　（共立出版）