1 Gauss 記号

定義 1.1. $a \in \mathbb{R}$ に対して,

$$[a] := \max\{x \in \mathbb{Z} \mid x \leq a\}$$

によって $[a]$ を定義する. つまり, a を超えない最大の整数を $[a]$ とする. 記号 $[*]$ を **Gauss 記号**という.

補題 1.2. 任意の $a \in \mathbb{R}$ に対して, ある $m \in \mathbb{Z}$ が一意的に存在して $m \leq a < m+1$ が成り立つ.

証明. **m の存在の証明** m の存在を背理法によって証明する.

もし仮に $m \leq a < m+1$ となるような $m \in \mathbb{Z}$ が存在しないとすると, 任意の $m \in \mathbb{Z}$ に対して, $a < m$ または $m+1 \leq a$ が成り立つ.

$a < m$ ならば, 背理法の仮定から $a < m-1$ でなければならない. したがって, もしある $m_0 \in \mathbb{Z}$ が存在して $a < m_0$ ならば,

$$m_0 > m_0 - 1 > m_0 - 2 > \cdots > a$$

となる. しかしこれは $m - i \to -\infty$ $(i \to \infty)$ に矛盾する.

よって, 任意の $m \in \mathbb{Z}$ に対して $m+1 \leq a$ でなければならない. ところがこれは $m+1 \to +\infty$ $(m \to \infty)$ に矛盾する.

以上より, ある $m \in \mathbb{Z}$ が存在して $m \leq a < m+1$ となることが示された.

m の一意性の証明 $m_1, m_2 \in \mathbb{Z}$ とし,

$$m_1 \leq a < m_1 + 1, \quad m_2 \leq a < m_2 + 2 \tag{1}$$

であるとする.

もし仮に $m_1 \neq m_2$ ならば, $m_1 < m_2$ または $m_2 < m_1$ である. $m_1 < m_2$ であるとしても一般性を失わない. このとき, $m_1 + 1 \leq m_2$ である. (1) の一番目の不等式より $a < m_1 + 1$ だから $a < m_2$ である. これは (1) の二番目の不等式における $m_2 \leq a$ に反する.

したがって $m_1 = m_2$ でなければならない. □

命題 1.3. 任意の $a \in \mathbb{R}$ に対して $[a]$ が一意的に定まる.

証明. $a \in \mathbb{R}$ とする. 補題 1.2 より, ある $m \in \mathbb{Z}$ が存在して $m \leq a < m+1$ となる. このとき, a を超えない最大の整数は m である. すなわち, $[a] = m$ である.

一意性は明らかである. 実際, 二つの $[a]$ をそれぞれ $[a]_1$, $[a]_2$ とすれば, $[a]_1 = m = [a]_2$ である. □

命題 1.4. 任意の $a \in \mathbb{R}$ に対して $[a] \leq a$.

証明. $[a]$ の定義 (定義 1.1) より $[a] \in \{x \in \mathbb{Z} \mid x \leq a\}$. ゆえに $[a] \leq a$. □

命題 1.5. $a \in \mathbb{R}$, $m \in \mathbb{Z}$ について,

$$m \leq a \Longleftrightarrow m \leq [a].$$

証明. ($\Rightarrow$) $a \in \mathbb{R}$, $m \in \mathbb{Z}$, $m \leq a$ とすれば,

$$m \in \{x \in \mathbb{Z} \mid x \leq a\}.$$

よって $[a]$ の定義 (定義 1.1) より $m \leq [a]$.
($\Leftarrow$) 命題 1.4 より $[a] \leq a$ だから. □

系 1.5.1. $a \in \mathbb{R}$, $m \in \mathbb{Z}$ について,

$$a < m \Longleftrightarrow [a] < m.$$

証明. 命題 1.5 の対偶をとればよい. □

命題 1.6. $a \in \mathbb{R}$, $m \in \mathbb{Z}$ について,

$$[a] = m \Longleftrightarrow m \leq a < m + 1$$

が成り立つ.

証明. ($\Rightarrow$) $[a] = m$ とする. このとき, $m \leq a < m + 1$ であることを背理法により証明する.
もし仮に $m \leq a < m + 1$ でないとすると, 実数の性質より $a < m$ または $m + 1 \leq a$ が成り立つ.
$a < m$ のとき, 命題 1.4 より $[a] < m$. これは $[a] = m$ に反する.
$m + 1 \leq a$ のとき, 命題 1.5 より $m + 1 \leq [a]$. これは $[a] = m$ に反する.
いずれにせよ, $m \leq a < m + 1$ でないと仮定すると矛盾が生じる. したがって $m \leq a < m + 1$ でなければならない.
($\Leftarrow$) $m \leq a < m + 1$ のとき, a を超えない最大の整数は m だから, 定義 1.1 より $[a] = m$. □

系 1.6.1. $a \in \mathbb{R}$, $m \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$ とする.

(i) $[na] = m \Longleftrightarrow m/n \leq a < (m + 1)/n$,

(ii) $[a/n] = m \Longleftrightarrow nm \leq a < n(m + 1)$.

証明. (i) $[na] = m \Leftrightarrow m \leq na < m + 1 \Leftrightarrow m/n \leq a < (m + 1)/n$. ここで, 最初の $\Leftrightarrow$ に命題 1.6 を用いた.
(ii) $[a/n] = m \Leftrightarrow m \leq a/n < m + 1 \Leftrightarrow nm \leq a < n(m + 1)$. ここで, 最初の $\Leftrightarrow$ に命題 1.6 を用いた. □

系 1.6.2. $a \in \mathbb{R}$, $m \in \mathbb{Z}$, $n \in \mathbb{Z}_{>0}$ とする.

(i) $n \mid m$ のとき, $n[a] = m \Longleftrightarrow m/n \leq a < m/n + 1$,

(ii)　$[a]/n = m \Longleftrightarrow nm \leq a < nm + 1$.

証明.　(i)　$n[a] = m \Leftrightarrow m \leq [a] = m/n \Leftrightarrow m/n \leq a < m/n + 1n$. ここで, 二番目の $\Leftrightarrow$ に命題 1.6 を用いた.

(ii)　$[a]/n = m \Leftrightarrow [a] = nm \Leftrightarrow nm \leq a < nm + 1$. ここで, 二番目の $\Leftrightarrow$ に命題 1.6 を用いた. □

命題 1.7.　$a \in \mathbb{R}$ について,

$$a \in \mathbb{Z} \Longleftrightarrow [a] = a.$$

証明.　($\Rightarrow$)　命題 1.4 より $[a] \leq a$ は明らか. 逆に, $a \in \{x \in \mathbb{Z} \mid x \leq a\}$ であるから, $[a]$ の定義 (定義 1.1) より $a \leq [a]$. したがって $[a] = a$.

($\Leftarrow$)　$[a] \in \mathbb{Z}$ だから, $a = [a]$ のとき $a \in \mathbb{Z}$. □

系 1.7.1.　任意の $a \in \mathbb{R}$ に対して, $[[a]] = [a]$.

証明.　$[a] \in \mathbb{Z}$ だから, 命題 1.7 より $[[a]] = [a]$. □

命題 1.8.　$a, b \in \mathbb{R}$ に対して,

$$a \leq b \Longrightarrow [a] \leq [b].$$

証明.　($\Rightarrow$)　$a \leq b$ と仮定する. $[a]$ の定義 (定義 1.1) より

$$[a] \in \{x \in \mathbb{Z} \mid x \leq a\}.$$

一方, $a \leq b$ と仮定したから,

$$\{x \in \mathbb{Z} \mid x \leq a\} \subseteq \{x \in \mathbb{Z} \mid x \leq b\}.$$

ゆえに,

$$[a] \in \{x \in \mathbb{Z} \mid x \leq b\}.$$

$[b]$ の定義 (定義 1.1) より,

$$[a] \leq [b]$$

となる. □

系 1.8.1.　$a, b \in \mathbb{R}$ に対して,

$$[a] < [b] \Longrightarrow a < b.$$

証明.　$[a] < [b]$ とする. このとき, $a < b$ であることを背理法によって証明する.

$a < b$ でないと仮定する. 実数の性質より, $b \leq a$ である. 命題 1.8 より, $[b] \leq [a]$ となる. これは $[a] < [b]$ に反する. □

注意 1.8.2. $a < b$ のとき, $[a] < [b]$ となる場合と, $[a] = [b]$ となる場合がある. 実際, $a < n \leq b$ を満たすような $n \in \mathbb{Z}$ があれば $[a] < [b]$ となり, なければ $[a] = [b]$ となる.

命題 1.9. $a \in \mathbb{R}$ に対して $[a+1] = [a] + 1$.

証明. $[a] \leq a$ より

$$[a] + 1 \leq a + 1.$$

命題 1.5 より

$$[a] + 1 \leq [a+1]. \tag{1}$$

逆に, $[a+1] \leq a+1$ より,

$$[a+1] - 1 \leq (a+1) - 1 = a.$$

命題 1.5 より

$$[a+1] - 1 \leq [a].$$

したがって

$$[a+1] \leq [a] + 1. \tag{2}$$

(1), (2) より $[a+1] = [a] + 1$. □

系 1.9.1. $a \in \mathbb{R}$, $m \in \mathbb{Z}$ に対して $[a+m] = [a] + m$.

証明. $m = 0$ のときは明らか.

$m > 0$ のときは, 命題 1.9 を有限回用いて

$$[a+m] = [a + (m-1) + 1] = [a + (m-1)] + 1 = \cdots = [a+1] + (m-1) = [a] + m.$$

(厳密には m に関する数学的帰納法によって示される).

$m < 0$ のとき, $m' := -m$, $a' := a + m$ とおけば, 主張を示すことは

$$[a' + m'] = [a'] + m'$$

を示すことに帰着される. □

命題 1.10. $a, b \in \mathbb{R}$ とする.

(i) $[a] + [b] \leq [a+b]$,

(ii) $[a-b] \leq [a] - [b]$.

証明. (i) $[a] \leq a$, $[b] \leq b$ より, $[a] + [b] \leq a + b$. 命題 1.5 より $[a] + [b] \leq [a+b]$.

(ii) $c = a - b$ とおくと, 主張は $[c] + [b] \leq [c+b]$ に帰着される. □

命題 1.11. 任意の $a \in \mathbb{R}$ に対して $a < [a] + 1$.

証明. 背理法で証明する.

もし仮に $[a] \leq a-1$ ならば, 命題 1.5 より $[a] \leq [a-1]$.

一方, 系 1.9.1 より,

$$[a-1] = [a] - 1 < [a].$$

これは矛盾である. □

系 1.11.1. 任意の $a \in \mathbb{R}$ に対して, ある $r \in \mathbb{R}$ がただ一つ存在して,

$$a = [a] + r, \quad 0 \leq r < 1$$

が成り立つ.

証明. 命題 1.11 より $r \in \mathbb{R}$ の存在は明らかである.

もし, 上記の r と同じ条件を満たす $r' \in \mathbb{Z}$ について,

$$r' = a - [a] = r$$

となる. よって r は一意的である. □

系 1.11.2.

(i) 任意の $a \in \mathbb{Z}$, $m \in \mathbb{Z}_{>0}$ に対して, ある $r \in \mathbb{Z}$ が存在して,

$$a = m \cdot \left[\frac{a}{m}\right] + r, \quad 0 \leq r < m$$

が成り立つ.

(ii) $a, q, r \in \mathbb{Z}$, $m \in \mathbb{Z}_{>0}$ とする. このとき,

$$a = mq + r, \quad 0 \leq r < m$$

が成り立つならば,

$$q = \left[\frac{a}{m}\right]$$

である.

証明. (i) 系 1.11.1 より, ある $r \in \mathbb{Z}$ が存在して

$$\frac{a}{m} = \left[\frac{a}{m}\right] + r_1, \quad 0 \leq r_1 < 1$$

となる. $r := mr_1$ とおけば

$$a = m \cdot \left[\frac{a}{m}\right] + r, \quad 0 \leq r < m$$

となる. よって r の存在が示された.

(ii) $0 \leq r < m$ より

$$0 \leq \frac{r}{m} < 1.$$

一方, $a = mq + r$ より

$$\frac{a}{m} = q + \frac{r}{m}.$$

よって

$$q = \left[q + \frac{r}{m}\right] = \left[\frac{a}{m}\right].$$

□

例 1.11.3. $m \in \mathbb{Z}_{>0}$, a, $b \in \mathbb{Z}$ とする.

$a = m \cdot [a/m] + \alpha$, $b = m \cdot [b/m] + \beta$ とおく (系 1.11.2). このとき, $0 \leq \alpha + \beta < 2m$ である.

(i) $0 \leq \alpha + \beta < m$ のとき, $0 \leq (\alpha - \beta)/m < 1$ であるから,

$$\left[\frac{a+b}{m}\right] = \left[\frac{([m/a] + [m/b]) \cdot m}{m} + \frac{\alpha + \beta}{m}\right] = \left[\frac{a}{m}\right] + \left[\frac{b}{m}\right].$$

(ii) $1 \leq \alpha + \beta < 2m$ のとき, $1 \leq (\alpha + \beta)/m < 2$ であるから,

$$\left[\frac{a+b}{m}\right] = \left[\frac{([m/a] + [m/b]) \cdot m}{m} + \frac{\alpha + \beta}{m}\right] = \left[\frac{a}{m}\right] + \left[\frac{b}{m}\right] + 1.$$

例 1.11.4. $m \in \mathbb{Z}_{>0}$, a, $b \in \mathbb{Z}$ とする.

$a = m \cdot [a/m] + \alpha$, $b = m \cdot [b/m] + \beta$ とおく (系 1.11.2). このとき, $-m < \alpha - \beta < m$ である.

(i) $0 \leq \alpha - \beta < m$ のとき, $0 \leq (\alpha - \beta)/m < 1$ であるから,

$$\left[\frac{a-b}{m}\right] = \left[\frac{([m/a] - [m/b]) \cdot m}{m} + \frac{\alpha - \beta}{m}\right] = \left[\frac{a}{m}\right] - \left[\frac{b}{m}\right].$$

(ii) $-m < \alpha - \beta < 0$ のとき, $0 < 1 + (\alpha - \beta)/m < 1$ であるから,

$$\left[\frac{a-b}{m}\right] = \left[\frac{([m/a] - [m/b]) \cdot m}{m} - 1 + \left(1 + \frac{\alpha - \beta}{m}\right)\right] = \left[\frac{a}{m}\right] - \left[\frac{b}{m}\right] - 1.$$

系 1.11.5. 任意の $n \in \mathbb{Z}_{>0}$ と $x \in \mathbb{R}$ に対して

$$\left[\frac{[nx]}{n}\right] = [x]$$

が成り立つ.

証明. 系 1.11.2 より, ある $r \in \mathbb{Z}$ が存在して

$$[nx] = n \cdot \left[\frac{[nx]}{n}\right] + r, \quad 0 \leq r \leq n - 1$$

と表せる. 一方, 系 1.11.1 より, ある $s \in \mathbb{R}$ が存在して

$$nx = [nx] + s, \quad 0 \leq s < 1$$

と表せる. よって

$$x = \left[\frac{[nx]}{n}\right] + \frac{r+s}{n}.$$

$r + s < n$ だから,

$$[x] = \left[\frac{[nx]}{n}\right]$$

となる. □

例 1.11.6. $x \in \mathbb{R}_{>0}$ に対して,

$$\frac{[10^k x]}{10^k} \quad (k \geq 0)$$

は, 小数点 $k+1$ 位以下を切り捨てた数になる.

例えば, $x := 3.14159$ について,

$$\begin{aligned} 10^2 x &= 314.159, \\ [10^2 x] &= 314, \\ \frac{[10^2 x]}{10^2} &= 3.14 \end{aligned}$$

となる.

命題 1.12. 任意の $a \in \mathbb{R} \setminus \mathbb{Z}$ に対して $[a] + [-a] = -1$.

証明. 系 1.11.1 より

$$a = [a] + r, \quad 0 < r < 1$$

と表せる. 命題 1.6 より

$$[r] = 0, \quad [-r] = -1$$

である. このとき

$$\begin{aligned} [a] + [-a] &= [[a] + c] + [-[a] - c] \\ &= [a] + [c] - [a] + [-c] \quad (\because \text{系 } 1.9.1) \\ &= -1. \end{aligned}$$

□

命題 1.13. 任意の $a \in \mathbb{R} \setminus \mathbb{Z}$ と $m \in \mathbb{Z}$ に対して $[a] + [m-a] = m - 1$.

証明. $a \in \mathbb{R} \setminus \mathbb{Z}$, $m \in \mathbb{Z}$ とする. 系 1.9.1 より

$$[m - a] = [-a] + m.$$

また, 命題 1.12 より

$$[a] + [-a] = -1.$$

よって

$$[a] + [m - a] = [a] + [-a] + m = m - 1.$$

□

命題 1.14. 任意の $a \in \mathbb{R}$ に対して $0 \leq a - [a] < 1$.

証明. 命題 1.4 と命題 1.11 からわかる. □

命題 1.15. $a, b \in \mathbb{R}$ とする.

(i) $[a+b] \leq [a] + [b] + 1$,

(ii) $[a] - [b] \leq [a-b] + 1$.

証明. (i) 命題 1.11 より

$$a < [a] + 1, \quad b < [b] + 1.$$

よって

$$a + b < [a] + [b] + 2.$$

一方, 命題 1.4 より $[a+b] \leq a + b$ だから

$$[a+b] < [a] + [b] + 2.$$

$[a+b] \in \mathbb{Z}$, $[a] + [b] + 2 \in \mathbb{Z}$ だから,

$$[a+b] \leq [a] + [b] + 1$$

となる.

(ii) 命題 1.12 と命題 1.10 (i) より

$$[a] - [b] = [a] + [-b] + 1 \leq [a-b] + 1.$$

□

命題 1.16. 任意の $a_1, \ldots a_n \in \mathbb{R}$ に対して

$$[a_1] + \cdots + [a_n] \leq [a_1 + \cdots + a_n] \leq [a_1] + \cdots + [a_n] + (n-1).$$

が成り立つ.

証明. $n = 2$ のときは命題 1.10 と命題 1.15 より明らか.

$n = k$ のときまで正しいと仮定すると,

$$[a_1] + \cdots + [a_k] \leq [a_1 + \cdots + a_k] \leq [a_1] + \cdots + [a_k] + (k-1).$$

このとき, 帰納法の仮定と $n = 2$ の場合の結果を用いれば

$$\begin{aligned}
[a_1] + \cdots + [a_k] + [a_{k+1}] &\leq [a_1 + \cdots + a_k] + [a_{k+1}] \\
&\leq [a_1 + \cdots + a_{k+1}] \\
&\leq [a_1] + \cdots + [a_{k-1}] + [a_k + a_{k+1}] + (k-1) \\
&\leq [a_1] + \cdots + [a_{k-1}] + [a_k] + [a_{k+1}] + k.
\end{aligned}$$

ゆえに $n = k + 1$ のときも正しい. □

命題 1.17. 任意の $a, b \in \mathbb{R}_{>0}$ に対して $[a][b] \leq [ab]$.

証明. $a = [a] + \alpha$, $b = [b] + \beta$ とおく (系 1.11.1) と,

$$ab = [a][b] + \alpha a + \beta b + \alpha\beta.$$

a, $b \in \mathbb{R}_{>0}$ より, $\alpha a + \beta b + \alpha\beta \geq 0$. ゆえに

$$[a][b] \leq ab.$$

したがって, 命題 1.5 より

$$[a][b] \leq [ab].$$

□

系 1.17.1. $a \in \mathbb{R}_{>0}$, $m \in \mathbb{Z}_{>0}$ とする.

(i) $m[a] \leq [ma]$.

(ii) $[a/m] \leq [a]/m$.

証明. (i) 命題 1.7 より $m = [m]$. よって, 命題 1.17 より

$$m[a] = [m][a] \leq [ma].$$

(ii) $a' = a/m$ とおけば, $[a/m] \leq [a]/m$ を示すことは $m[a'] \leq [ma']$ を示すことに帰着される. □

例 1.17.2. $m = 2$, $a = 1/2$ とすれば, $m[a] = 0$, $[ma] = 1$. よってこの場合, $m[a] < [ma]$.

命題 1.18. $x \in \mathbb{R}$, $m \in \mathbb{Z}_{>0}$, $0 \leq l \leq m-1$ とする. このとき,

$$\frac{l}{m} \leq x - [x] < \frac{l+1}{m} \Longrightarrow [mx] - m[x] = l$$

が成り立つ.

証明. $l/m \leq x - [x] < (l+1)/m$ と仮定する.

$$\begin{aligned}
\frac{l}{m} \leq x - [x] &\Longrightarrow l \leq mx - m[x] \\
&\Longrightarrow l + m[x] \leq mx \\
&\Longrightarrow l + m[x] \leq [mx] \quad (\because \text{命題 1.5}) \\
&\Longrightarrow l \leq [mx] - m[x].
\end{aligned}$$

ゆえに

$$l \leq [mx] - m[x]. \tag{1}$$

一方, 命題 1.4 より $[mx] \leq mx$ だから

$$[mx] - m[x] \leq mx - m[x].$$

一方,

$$x - [x] < \frac{l+1}{m} \Longrightarrow mx - m[x] < l + 1.$$

ゆえに

$$[mx] - m[x] < l + 1. \tag{2}$$

$[mx] - m[x] \in \mathbb{Z}$ だから, (1), (2) より

$$[mx] - m[x] = l.$$

□

命題 1.19. $a, b \in \mathbb{R}$ について

$$[a] = [b] \Longrightarrow -1 \leq a - b \leq 1.$$

証明.

$$\begin{aligned}
[a] = [b] &\Longleftrightarrow [a] - [b] = 0 \\
&\Longrightarrow [a - b] \leq 0 \leq [a - b] + 1 \quad (\because \text{命題 1.10 と命題 1.15}) \\
&\Longleftrightarrow -1 \leq [a - b] \leq 0 \\
&\Longleftrightarrow [a - 1] = -1 \text{ または } [a - b] = 0 \\
&\Longleftrightarrow -1 \leq a - b < 1. \quad (\because \text{命題 1.6})
\end{aligned}$$

□

命題 1.20. 任意の $x \in \mathbb{R}$, $n \in \mathbb{Z}_{>0}$ に対して,

$$\sum_{i=0}^{n-1} \left[x + \frac{i}{n} \right] = [nx]$$

が成り立つ.

証明. $l, m \in \mathbb{Z}$ とし,

$$m + \frac{l}{n} \leq x < m + \frac{l+1}{n}, \quad 0 \leq l \leq n - 1 \tag{1}$$

とする. (1) より

$$nm + l \leq nx < nm + l + 1$$

であるから

$$[nx] = nm + l.$$

一方, (1) より

$$m + \frac{i+l}{n} \leq x + \frac{i}{n} < m + \frac{i+l+1}{n}.$$

よって

$$\left[x + \frac{i}{n} \right] = \begin{cases} m+1, & i \geq n - l \\ m, & i < n - l \end{cases}$$

であるから

$$\sum_{i=0}^{n-1}\left[x+\frac{i}{n}\right]=nm+l.$$

したがって, 求める等式が得られる. □

命題 1.21. 任意の $n\in\mathbb{Z}_{>0}$ と $x_1,\ldots,x_n,a_1,\ldots,a_n$ に対して,

$$\sum_{i=1}^{n}a_i\geq n-1\Longrightarrow\left[\sum_{i=1}^{n}x_i\right]\leq\sum_{i=1}^{n}[x_i+a_i]$$

が成り立つ.

証明.

$$\begin{aligned}\left[\sum_{i=1}^{n}x_i\right]+(n-1)&=\left[\sum_{i=1}^{n}x_i+(n-1)\right]\quad(\because \text{系 1.9.1})\\&\leq\left[\sum_{i=1}^{n}(x_i+a_i)\right]\quad(\because \text{命題 1.8})\\&\leq\sum_{i=1}^{n}[x_i+a_i]+(n-1)\quad(\because \text{命題 1.16})\end{aligned}$$

より

$$\left[\sum_{i=1}^{n}x_i\right]\leq\sum_{i=1}^{n}[x_i+a_i].$$

□

命題 1.22. $a,b\in\mathbb{R}$ とする.

(i) $[x]+[y]+[x+y]\leq[2x]+[2y]$.

(ii) $[x]+[y]+[2x+y]+[x+2y]\leq[4x]+[4y]$.

証明. (i)

$$\begin{aligned}[2x]+[2y]&=[x]+[y]+\left[x+\frac{1}{2}\right]+\left[y+\frac{1}{2}\right]\quad(\because \text{命題 1.20})\\&\geq[x]+[y]+[x+y]\quad(\because \text{命題 1.21}).\end{aligned}$$

(ii)

$$\begin{aligned}[4x]+[4y]&=[2x]+[2y]+\left[2x+\frac{1}{2}\right]+\left[2y+\frac{1}{2}\right]\quad(\because \text{命題 1.20})\\&=[x]+[y]+\left[x+\frac{1}{2}\right]+\left[y+\frac{1}{2}\right]+\left[2x+\frac{1}{2}\right]+\left[2y+\frac{1}{2}\right]\quad(\because \text{命題 1.20})\\&\geq[x]+[y]+[2x+y]+[x+2y]\quad(\because \text{命題 1.21}).\end{aligned}$$

□

命題 1.23. $m,\ n \in \mathbb{Z}_{>0}$ とする. このとき, n の倍数で m 以下のものの個数は $[m/n]$ である.

証明. $m < n$ のとき, n の倍数で m 以下のものの個数は 0 である. 一方, $m < n$ ならば $[m/n] = 0$. よって $m < n$ のとき主張は正しい.

$n \leq m$ のとき, n の倍数で m 以下のものは

$$1 \cdot n, \quad 2 \cdot n, \quad \ldots, \quad \left[\frac{m}{n}\right] \cdot n$$

の $[m/n]$ 個である. 実際,

$$\left[\frac{m}{n}\right] \cdot n \leq \frac{m}{n} \cdot n = m \quad (\text{命題 } 1.4),$$
$$\left(\left[\frac{m}{n}\right] + 1\right) \cdot n > \frac{m}{n} \cdot n = m \quad (\text{命題 } 1.11)$$

である. □

系 1.23.1. $m \in \mathbb{Z}$ に対して

$$\mathrm{ord}_p(m) := \max\{k \in \mathbb{Z}_{\geq 0} \mid p^k \text{ は } m \text{ を割る } \}$$

とおく. このとき, 任意の $n \in \mathbb{Z}_{>0}$ に対して

$$\mathrm{ord}_p(n!) = \sum_{k=1}^{[\log_p n]} \left[\frac{n}{p^k}\right]$$

が成り立つ.

証明. $n!$ の因数

$$1, \quad 2, \quad 3, \quad \ldots, \quad n$$

の中に, p の倍数が n_1 個, p^2 の倍数が n_2 個, …, $p^{[\log_p n]}$ の倍数が $n_{[\log_p n]}$ 個あるとすれば,

$$\mathrm{ord}_p(n!) = n_1 + n_2 + \cdots + n_{[\log_p n]}$$

である. したがって命題 1.23 より求める等式が得られる. □

系 1.23.2. $p_1, p_2, \ldots, p_n$ は二つずつ互いに素な整数であるとする. $x \in \mathbb{R}$ に対して, x を超えない正の整数 m のうちで $p_i \nmid m\ (i = 1, 2, \ldots, n)$ であるものの個数を $N(x; p_1, p_2, \ldots, p_n)$ とする. このとき,

$$N(x; p_1, p_2, \ldots, p_n) = [x] - \sum_{i=1}^{n} \left[\frac{x}{p_i}\right] + \sum_{1 \leq i < j \leq n} \left[\frac{x}{p_i p_j}\right] - \sum_{1 \leq i < j < k \leq n} \left[\frac{x}{p_i p_j p_k}\right] + \cdots$$

が成り立つ.

証明. n に関する数学的帰納法により証明する.

$n = 1$ のとき, 命題 1.23 より,

$$N(x;\, p_1) = [x] - \left[\frac{x}{p_1}\right]$$

が成り立つ.

$n = l$ のとき主張が正しいと仮定する. このとき, 命題 1.23 より, $N(x/p_{l+1};\, p_1,\, p_2,\, \ldots,\, p_l)$ は $1 \cdot p_{l+1},\, 2 \cdot p_{l+1},\, \ldots,\, [x/p_{l+1}] \cdot p_{l+1}$ の中で $p_1,\, p_2,\, \ldots,\, p_l$ のいずれでも割れないものの個数に一致することがいえる. したがって,

$$\begin{aligned}
N(x;\, p_1,\, p_2,\, \ldots,\, p_{l+1}) &= N(x;\, p_1,\, p_2,\, \ldots,\, p_l) - N(x/p_{l+1};\, p_1,\, p_2,\, \ldots,\, p_l) \\
&= \left([x] - \sum_{i=1}^{l} \left[\frac{x}{p_i}\right] + \sum_{1 \le i < j \le l} \left[\frac{x}{p_i p_j}\right] - \cdots\right) \\
&\quad - \left(\left[\frac{x}{p_{l+1}}\right] - \sum_{i=1}^{l} \left[\frac{x}{p_i p_{l+1}}\right] + \sum_{1 \le i < j \le l} \left[\frac{x}{p_i p_j p_{l+1}}\right] - \cdots\right) \\
&= [x] - \sum_{i=1}^{l+1} \left[\frac{x}{p_i}\right] + \sum_{1 \le i < j \le l+1} \left[\frac{x}{p_i p_j}\right] - \cdots
\end{aligned}$$

となる. □

注意 1.23.3. φ を Euler の関数とする. すなわち, $x \in \mathbb{Z}$ に対して, $\varphi(x)$ を x 以下の正の整数で x と互いに素なものの個数とする.

$p_1,\, p_2,\, \ldots,\, p_n$ を x のすべての素因数として, 系 1.23.2 を適用すれば, $\varphi(x) = N(x;\, p_1,\, p_2,\, \ldots,\, p_n)$ が成り立つ.

命題 1.24. $x \in \mathbb{R}_{>0},\, n \in \mathbb{Z}_{>0}$ とする. このとき,

$$x, \quad 2x, \quad \ldots, \quad nx$$

がすべて整数でなければ,

$$\frac{1}{x}, \quad \frac{2}{x}, \quad \cdots, \quad \frac{[nx]}{x}$$

もまたすべて整数ではない.

証明. 対偶を証明する. ある $i \in \mathbb{Z}$ が存在して, $1 \le i \le [nx]$ かつ $i/x \in \mathbb{Z}$ と仮定する.

$j := i/x$ とおくと, $jx = i \in \mathbb{Z}$. また, $i/x > 0$ より $j \ge 1$. さらに, 命題 1.4 より $[nx] \le nx$ だから,

$$jx = i \le [nx] \le nx.$$

$x > 0$ だから, $j \le n$ が得られる. □

命題 1.25. $x \in \mathbb{R}_{>0},\, n \in \mathbb{Z}_{>0}$ とする. このとき,

$$x, \quad 2x, \quad \ldots, \quad nx$$

がすべて整数でなければ,

$$\sum_{i=1}^{n}[ix]+\sum_{j=1}^{[nx]}\left[\frac{j}{x}\right]=n[nx]$$

が成り立つ.

証明. $x\in\mathbb{R}_{>0}$ とすると, $i,\,j\in\mathbb{Z}$, $1\leq i\leq n$, $1\leq j\leq[nx]+1$ について,

$$\begin{aligned}[ix]=j-1&\iff j-1\leq ix<j\\&\iff\frac{j-1}{x}\leq i<\frac{j}{x}\\&\iff\frac{j-1}{x}\leq i\leq\left[\frac{j}{x}\right]\quad(\because\text{命題 1.5}).\end{aligned}$$

仮定と命題 1.24 より $(j-1)/x\neq i$. よって系 1.5.1 より

$$[ix]=j-1\iff\left[\frac{j-1}{x}\right]<i\leq\left[\frac{j}{x}\right].$$

さらに, 命題 1.11 より $nx\leq[nx]+1$. よって

$$n\leq\frac{[nx]+1}{x}.$$

命題 1.5 より

$$n\leq\left[\frac{[nx]+1}{x}\right].$$

したがって,

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

□

補題 1.26. $p,\,q\in\mathbb{Z}_{>0}$, $\gcd(p,\,q)=1$ とする. このとき,

$$\frac{q}{p},\quad\frac{2q}{p},\quad\ldots,\quad\frac{(p-1)q}{p}$$

はすべて整数ではない.

証明. ある $i\in\mathbb{Z}$ が存在して

$$1\leq j\leq p-1,\quad\frac{jq}{p}\in\mathbb{Z}$$

が成り立つと仮定する. $k:=jq/p$ とおくと,

$$jq=pk,\quad k\in\mathbb{Z}_{>0}.$$

$\gcd(p,\,q)=1$ だから, ある $k_1\in\mathbb{Z}_{>0}$ が存在して $k=qk_1$ となる. よって

$$jq=pqk_1.$$

ゆえに

$$j=pk_1\geq p.$$

これは仮定に反する. □

命題 1.27. $m,\,p,\,q\in\mathbb{Z}_{>0},\,\gcd(p,\,q)=1$ とする. このとき

$$p\equiv q\equiv 1 \pmod{m}$$

ならば,

$$\sum_{i=1}^{(p-1)/m}\left[\frac{iq}{p}\right]+\sum_{j=1}^{(q-1)/m}\left[\frac{jp}{q}\right]=\frac{(p-1)(q-1)}{m^2}$$

が成り立つ.

証明. $q<p$ としても一般性を失わない. このとき

$$p(q-1)=pq-p<pq-q=(p-1)q$$

より

$$\frac{q-1}{m}<\frac{(p-1)q}{mp}.$$

また, $(p-1)/p<1$ より

$$\frac{(p-1)q}{mp}<\frac{q}{m}\leq\frac{q-1}{m}+1.$$

ゆえに

$$\left[\frac{(p-1)q}{mp}\right]=\frac{q-1}{m}.$$

$x:=q/p,\,n:=(p-1)/m$ とすれば,

$$[nx]=\left[\frac{(p-1)q}{mp}\right]=\frac{q-1}{m}.$$

このとき, 補題 1.26 と命題 1.25 によって, 求める等式が得られる. □

系 1.27.1.

(i) $p,\,q\in\mathbb{Z}_{>0},\,\gcd(p,\,q)=1$ とする. このとき

$$\sum_{i=1}^{p-1}\left[\frac{iq}{p}\right]+\sum_{j=1}^{q-1}\left[\frac{jp}{q}\right]=(p-1)(q-1)$$

が成り立つ.

(ii)　$p,\, q \in \mathbb{Z}_{>0},\, \gcd(p,\, q) = 1$ とする．さらに，$p,\, q$ は奇数であるとする．このとき

$$\sum_{i=1}^{(p-1)/2} \left[\frac{iq}{p}\right] + \sum_{j=1}^{(q-1)/2} \left[\frac{jp}{q}\right] = \frac{(p-1)(q-1)}{4}$$

が成り立つ．

証明．(i) 命題 1.27 において，$m = 1$ の場合である．
(ii) 命題 1.27 において，$m = 2$ の場合である．

□

2　平方剰余の相互法則

p を奇素数とし，$a \in \mathbb{Z}$ とする．
合同式

$$x^2 \equiv a \pmod{p}$$

が解を持つとき，a を p の**平方剰余**といい，解を持たないとき**平方非剰余**という．$\gcd(a,\, p) = 1$ であるとき，

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & a \text{ が平方剰余のとき} \\ -1, & a \text{ が平方非剰余のとき} \end{cases}$$

と定める．(a/p) を **Legendre 記号**と呼ぶ．

定理 2.1.　p を奇素数，$a,\, b \in \mathbb{Z},\, \gcd(a,\, p) = \gcd(b,\, p) = 1$ とする．このとき

$$a \equiv b \pmod{p} \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

が成り立つ．
特に，p の平方剰余と合同なものはまた平方剰余であり，平方非剰余と合同なものはまた平方非剰余である．

証明．$a \equiv b \pmod{p}$ ならば，合同式 $x^2 \equiv a \pmod{p}$ が解を持つことと合同式 $x^2 \equiv b \pmod{p}$ が解を持つこととは同値である．□

p の平方剰余は $1,\, 2,\, \ldots,\, p-1$ の平方のいずれかと p を法として合同な整数である．

$$x^2 \equiv (p-x)^2 \pmod{p}$$

だから，p の平方剰余はすべて $1,\, 2,\, \ldots,\, (p-1)/2$ の平方のいずれかに p を法として合同である．
$x,\, y \in \mathbb{Z}$ に対して，

$$\begin{aligned} x^2 \equiv y^2 \pmod{p} &\Longrightarrow (x-y)(x+y) \equiv 0 \pmod{p} \\ &\Longrightarrow x - y \equiv 0 \pmod{p} \text{ または } x + y \equiv 0 \pmod{p}. \end{aligned}$$

$x,\, y$ の範囲を考慮して，$1 \le x \le (p-1)/2,\, 1 \le y \le (p-1)/2$ とすれば，

$$x^2 \equiv y^2 \pmod{p} \Longrightarrow x \equiv y \pmod{p} \Longrightarrow x = y$$

となる．ゆえに $1, 2, \ldots, (p-1)/2$ の平方はどの 2 つも p を法として合同ではない．

したがって, $1, 2, \ldots, p-1$ のうち, p の平方剰余, 平方非剰余はそれぞれ $(p-1)/2$ 個ずつある．

定理 2.2 (Euler の規準)．p を奇素数, $a \in \mathbb{Z}$, $\gcd(a, p) = 1$ とする．このとき

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

が成り立つ．

証明． $1 \leq x \leq p-1$ となる x に対し, $\gcd(x, p) = 1$ であるから,

$$xy \equiv a \pmod{p}, \quad 1 \leq y \leq p-1$$

となる $y \in \mathbb{Z}$ がただ一つ存在する．この y を a に関する x の配偶と呼ぶことにする．このとき,

$$a \text{ が平方剰余} \iff x \in \mathbb{Z} \text{ が存在して, } x \text{ 自身が } a \text{ に関する } x \text{ の配偶になる.}$$

と言いかえることができる．

a が平方剰余のとき, 合同式 $x^2 \equiv a \pmod{p}$ の解を x_0 $(1 \leq x_0 \leq p-1)$ とする．

$$(p - x_0)^2 = p^2 - 2px_0 + x_0^2 \equiv x_0^2 \equiv a \pmod{p}$$

であるから, $p - x_0$ も解となり, $1 \leq p - x_0 \leq p-1$ である．

p は奇数だから, $p - x_0 \neq x_0$ である．

よって, 1 から $p-1$ までの中で x_0 と $p - x_0$ の 2 つだけが自分自身を配偶に持ち, 他は自分と異なる配偶を持つ．

1 から $p-1$ までを並び替えて

$$x_0, \quad p - x_0, \quad x_1, \quad \ldots, \quad x_{(p-3)/2}, \quad y_1, \quad y_2, \quad \ldots, \quad y_{(p-3)/2}$$

とする．ただし y_i は a に関する x_i の配偶である．すると,

$$\begin{aligned}(p-1)! &= x_0(p - x_0)(x_1 \cdot y_1)(x_2 \cdot y_2) \cdots (x_{(p-3)/2} \cdot y_{(p-3)/2}) \\ &\equiv x_0(-x_0) \cdot a \cdot \cdots \cdot a \\ &\equiv -a^{\frac{p-1}{2}} \pmod{p}.\end{aligned}$$

特に $a = 1$ のとき, a は平方剰余であるから

$$(p-1)! \equiv -1 \pmod{p} \tag{1}$$

となる．この式を再び上の式に代入すると

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

を得る．

a が平方非剰余のときは, 自分自身を配偶に持つ整数はない. そこで, 1 から $p-1$ までの数を並べ替えて

$$x_1, \quad x_2, \quad \ldots, \quad x_{(p-1)/2}, \quad y_1, \quad y_2, \quad \ldots, \quad y_{(p-1)/2}$$

とおく．ただし y_i は a に関する x_i の配偶である．このとき,

$$\begin{aligned}(p-1)! &= (x_1 \cdot y_1)(x_2 \cdot y_2) \cdots (x_{(p-1)/2} \cdot y_{(p-1)/2}) \\ &\equiv a \cdot \cdots \cdot a \pmod{p} \\ &\equiv a^{\frac{p-1}{2}} \pmod{p}\end{aligned}$$

となる．よって (1) より

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

が得られる． □

系 2.2.1 (Wilson の定理). $n \in \mathbb{Z}$, $n > 1$ とするとき

$$n \text{ は素数である} \iff (n-1)! \equiv -1 \pmod{n}.$$

証明. ($\Rightarrow$) n が奇素数の場合は, Euler の規準を証明する途中で既に示されている．$n = 2$ のときは明らか.

($\Leftarrow$) n が合成数であるとすると, ある b, $c \in \mathbb{Z}$ によって

$$n = bc, \qquad 1 < b < n$$

と表せる．b は $(n-1)!$ の約数である．よって b は $(n-1)! + 1$ の約数ではない．n は b の倍数だから $(n-1)! + 1$ を割り切ることができない. □

系 2.2.2. p を奇素数, a, $b \in \mathbb{Z}$, $\gcd(a, p) = \gcd(b, p) = 1$ とする．このとき

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

証明. Euler の規準により

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

両辺とも ± 1 であり, $1 \not\equiv -1 \pmod{p}$ であるから等号が成り立つ. □

定理 2.3 (Gauss の補題). p を奇素数, $a \in \mathbb{Z}$, $\gcd(a, p) = 1$ とする．このとき

$$1 \cdot a, \quad 2 \cdot a, \quad \ldots, \quad \frac{p-1}{2} \cdot a$$

を p で割ったときの剰余の中に $p/2$ よりも大きいものが n 個あったとすれば

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

証明.

$$\pm 1, \quad \pm 2, \quad \ldots, \quad \pm\frac{p-1}{2}$$

の $p-1$ 個の整数は法 p に関する既約剰余系である.

$\gcd(a, p) = 1$ だから,

$$\pm 1 \cdot a, \quad \pm 2 \cdot a, \quad \ldots, \quad \pm\frac{p-1}{2} \cdot a$$

もまた法 p に関する既約剰余系である.

xa $(1 \leq x \leq (p-1)/2)$ を p で割ったときの剰余が $p/2$ より大きいということは, xa が -1, -2, …, $-(p-1)/2$ のいずれかと p を法として合同なことと同値である.

そこで, $1 \cdot a$, $2 \cdot a$, …, $(p-1)/2 \cdot a$ のうち -1, -2, …, $-(p-1)/2$ のいずれかと合同なものの個数を n とする. このとき,

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

$1 \cdot 2 \cdot \cdots \cdot (p-1)/2$ と p とは互いに素であるから, 両辺を $1 \cdot 2 \cdot \cdots \cdot (p-1)/2$ で割ると

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

Euler の規準により,

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

となる. □

p を奇素数, $q \in \mathbb{Z}_{>0}$, $\gcd(p, q) = 1$ とする.

$t := (p-1)/2$ とおく. 系 1.11.2 より, ある r_1, r_2, …, $r_t \in \mathbb{Z}$ が存在して

$$\begin{aligned} q &= p\left[\frac{q}{p}\right] + r_1, \quad 0 \leq r_1 < p \\ 2q &= p\left[\frac{2q}{p}\right] + r_2, \quad 0 \leq r_2 < p \\ &\cdots\cdots \\ tq &= p\left[\frac{tq}{p}\right] + r_t, \quad 0 \leq r_t < p \end{aligned}$$

となる.

系 2.3.1 (第一補充法則). p を奇素数とするとき,

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

証明. $q = p-1$ の場合を考える. このとき, r_1, r_2, …, r_t はすべて $p/2$ より大きい. ゆえに Gauss の補題により

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

□

補題 2.4. p, q, t, r_1, r_2, …, r_t は上述の通りとする.

r_1, r_2, …, r_t のうち, $p/2$ より大きいものの個数を s とし,

$$N := \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \cdots + \left[\frac{tq}{p}\right]$$

とおく. このとき

$$s \equiv N + \frac{1}{8}(p^2-1)(q-1) \pmod 2$$

が成り立つ.

証明. r_1, r_2, …, r_t のうち, $p/2$ より大きいものを a_1, a_2, …, a_s, そうでないものを b_1, b_2, …, b_{t-s} とする. さらに,

$$A := a_1 + a_2 + \cdots + a_s,$$
$$B := b_1 + b_2 + \cdots + b_{t-s}$$

とおく. このとき

$$\frac{1}{8}(p^2-1)q = Np + A + B. \tag{1}$$

一方,

$$\pm 1, \quad \pm 2, \quad \ldots, \quad \pm\frac{p-1}{2}$$

の $p-1$ 個の整数は法 p に関する既約剰余系である. $\gcd(p, q) = 1$ だから,

$$\pm 1 \cdot q, \quad \pm 2 \cdot q, \quad \ldots, \quad \pm\frac{p-1}{2} \cdot q$$

もまた法 p に関する既約剰余系である. よって $-a_1$, $-a_2$, …, $-a_s$, b_1, b_2, …, b_{t-s} は p を法として互いに合同ではない. ゆえに

$$\{p-a_1, p-a_2, \ldots, p-a_s, b_1, b_2, \ldots, b_{t-s}\} = \{1, 2, \ldots, \frac{1}{2}(p-1)\}.$$

これより

$$\frac{1}{8}(p^2-1) = 1 + 2 + \cdots + \frac{1}{2}(p-1) = sp - A + B. \tag{2}$$

(1), (2) より

$$\frac{1}{8}(p^2-1)(q-1) = (N-s)p + 2A.$$

p は奇数だから, 2 を法として考えれば, 求める等式が得られる. □

系 2.4.1 (第二補充法則). p を奇素数とするとき,

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

証明. $q = 2$ の場合を考えると, $N = 0$ である. よって, 補題 2.4 より

$$s \equiv \frac{1}{8}(p^2-1) \pmod 2.$$

Gauss の補題より,

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

□

定理 2.5 (平方剰余の相互法則). p, q を奇素数とし, $\gcd(p, q) = 1$ とする. このとき,

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

証明. p, q は奇数だから,

$$\frac{1}{8}(p^2-1)(q-1) \equiv 0 \pmod 2.$$

ゆえに, 補題 2.4 より,

$$s \equiv N \pmod 2.$$

さらに, Gauss の補題より

$$\left(\frac{q}{p}\right) = (-1)^s = (-1)^N.$$

同様に, $t' := (q-1)/2$ とおき,

$$N' := \left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \cdots + \left[\frac{t'p}{q}\right]$$

とおけば, 補題 2.4 と Gauss の補題より

$$\left(\frac{p}{q}\right) = (-1)^{N'}$$

が得られる.

さて, 系 1.27.1 (ii) より

$$N + N' = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

したがって,

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

□

参考文献

[1] 倉田令二朗: 平方剰余の相互法則, 日本評論社, 1992.