

平方剰余の相互法則の証明 Ver.2

福沢正男

1. 準備

以下、文字 p, q および $a, b, c, \dots$ は整数を表し、特に p, q は奇素数を表す。 p を法とする剰余として**絶対的最小剰余**を用いる。また、任意の奇素数は整数 n を用いて $p = 4n \pm 1$ と表され得ることは既知とする¹。

奇素数 p の絶対的最小剰余の集合を F_p と表す。

$$F_p = \{0, \pm 1, \pm 2, \dots, \pm(p-1)/2\}$$

F_p は「**有限体**」の構造を持つ（四則計算が可能）。また F_p から元 0 を除いた集合を F_p^* で表す。

$$F_p^* = \{\pm 1, \pm 2, \dots, \pm(p-1)/2\}$$

p を F_p および F_p^* の**法**という。 F_p および F_p^* の正の元（の集合）を**正剰余**、負の元を**負剰余**という。 F_p^* では F_p での乗法を演算として**群**、とくに**アーベル群**となる。 F_p^* を F_p の乗法群という。有限体や群の基本的性質も既知²とするが、 F_p や F_p^* の独自の性質については逐次説明する。

一般に集合 A の元の個数を $|A|$ で表す。 F_p, F_p^* の元の個数も $|F_p|, |F_p^*|$ で表す。 $|F_p| = p, |F_p^*| = p - 1$ 。 $|F_p^*|$ を特に**群の位数**という。

有限体 F_p の元はすべて 2 で割り切れる（2 の逆元 2^{-1} をかける）ので、通常の数・奇数という概念はないが、2 で割っても符号を変えない剰余を**偶剰余**、符号を変える剰余を**奇剰余**と呼ぶことにする。0 は偶剰余とする。とくに F_p^* において、

$p = 4n + 1$ のときの偶剰余は $\pm 2, \pm 4, \dots, \pm 2n$ の $2n$ 個

奇剰余は、 $\pm 1, \pm 3, \dots, \pm(2n-1)$ の $2n$ 個

$p = 4n - 1$ のときの偶剰余は $\pm 2, \pm 4, \dots, \pm 2(n-1)$ の $2(n-1)$ 個

奇剰余は、 $\pm 1, \pm 3, \dots, \pm(2n-1)$ の $2n$ 個

奇剰余を 2 で割ったものを 2 倍すればまた符号が変わる（もとに戻る）。

例： $p=17$ のとき、 $F_p = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7, \pm 8\}$ 。正剰余は $\{1, 2, 3, 4, 5, 6, 7, 8\}$ 。負剰余は

$\{-1, -2, -3, -4, -5, -6, -7, -8\}$ 。 F_{17}^* の偶剰余は $\{\pm 2, \pm 4, \pm 6, \pm 8\}$ 。奇剰余は $\{\pm 1, \pm 3, \pm 5, \pm 7\}$ 。ちなみにこの奇剰余を 2 で割る（ $2^{-1} = -8$ をかける）と、 $\{\mp 8, \mp 7, \mp 6, \mp 5\}$ 。

体 F_p において一次方程式 $ax + b = c$ ($a \neq 0$) を次のようにして解くことができる。

$$ax + b = c$$

$$ax = c - b$$

$$x = a^{-1}(c - b)$$

方程式の係数が F_p の元でない場合でも、 F_p の合同な元に置き換えることで解くことが可能である。一般に、 $(a \pm lp)x + (b \pm mp) = c \pm np$ (l, m, n は通常の数) ならば、体 F_p では $p = 0$ であるから、これは $ax + b = c$ と同じものとされる。

¹ 簡易的な証明を付録 1 に付けた。

² 付録 2 参照。

次に、体 F_p 上の方程式 $x^2 = a$ について、次の定理が成り立つ。

【命題 1.1】 体 F_p で、 $x^2 = a$ の解は 2 個以下である（2 個より多くはない）。

【証明】 まず、 $a = 0$ ならば、明らかに $x = 0$ だけが F_p での解である。次に $a \neq 0$ として群 F_p^* で考える。 $r \in F_p^*$ のとき、 $r^2 = a$ ならば、 $-r \in F_p^*$ かつ $(-r)^2 = a$ であるから、方程式 $x^2 = a$ の解は $\pm r$ の 2 個ある。もし $\pm r$ 以外の元 $s \in F_p^*$ も $x^2 = a$ の解ならば、 $s^2 = a$ 。これと $r^2 = a$ を辺々引けば $s^2 - r^2 = 0$ 。 $\therefore (s+r)(s-r) = 0$ 、よって $s = \pm r$ となる。したがって群 F_p^* においては $x^2 = a$ の解は必ず 2 個となる。 $\parallel$

F_p^* の元 a において、 $x^2 = a$ が解を持つとき、 a を**平方剰余**といい、持たないとき、**平方非剰余**という。 F_p^* の元 2 個ずつが一つの平方剰余に対応するから、平方剰余の個数は、命題 1.1 より $(p-1)/2$ となる。

F_p^* の平方剰余の集合を N とするとき、集合 $F_p^* - N$ は F_p^* の平方非剰余の集合となる。これを L で表わす。 $F_p^* = N + L$ と表わされる。その個数は N と同じ $(p-1)/2$ である。

【命題 1.2】 F_p^* の平方剰余の集合 N は F_p^* の部分群となる。

【証明】 F_p^* の元を $a, b, c, \dots, r, s, t, \dots$; N の元を $r^2, s^2, t^2, \dots$ で表す。部分群の定義は既知とする。

まず、 $1^2 = 1 \in N$ （単位元）。 F_p^* が群であるから N においても $r^2(s^2t^2) = (r^2s^2)t^2$ （結合法則）が成り立つ。

N の元 r^2, s^2 の積は、 $r^2s^2 = (rr)(ss) = (rs)(rs) = (rs)^2$ 。 $rs = t$ となる F_p^* の元 t があるから積 $r^2s^2 = t^2$ は平方剰余である。よって $t^2 \in N$ 。ゆえに乗法が成立する。また、逆元の存在については $r^2x = s^2$ が成り立つ N の元 x が存在すればよい。まず、 x は F_p^* の元としては存在するのでそれを c とする。すなわち $r^2c = s^2$ 。この c が平方剰余であることをいえばよい。次に、 r, s から方程式 $rx = s$ を作れば、これはただひとつの解 $t = sr^{-1} \in F_p^*$ を持つ。これによって $rt = s$ 。これを $r^2c = s^2$ に代入すれば $r^2c = r^2t^2$ 、簡約して $c = t^2$ 。ゆえに c が平方剰余であることが確かめられた。すなわち、 N は F_p^* の部分群である。 $\parallel$

【命題 1.3】 F_p^* の平方剰余の集合を N 、平方非剰余の集合を L とするとき、

- ① $a, b \in N$ ならば $ab \in N$; ② $a \in N, b \in L$ ならば $ab \in L$; ③ $a, b \in L$ ならば $ab \in N$ 。

【証明】 ① N は群であるから $a, b \in N$ ならば $ab \in N$ である。

② $a \in N, b \in L$ で、もし $ab \in N$ なら $ab = c$ とおいて $b = a^{-1}c \in N$ となって矛盾。ゆえに $ab \in L$ 。 $a \in L, b \in N$ でも同じ。

③ 仮に $ab \in L$ とする. N の元を d とすると, ②より $ad \in L$ となるから ab はある ad と等しくななければならない. それを $d = d_i$ とすれば $ab = ad_i$ となり, 簡約して $b = d_i$. これは b が N の元であることになり, 矛盾する. ゆえに $ab \in N$. $\parallel$

一般に, 群 G の元を a, b とするとき, $ab = e$ (e は単位元) ならば, a, b は互いに逆元という. 特に $a^2 = e$ となる a を「**自逆元**」, 自逆元でない元を「**他逆元**」という. 単位元はすべての群の自逆元である. a, b が他逆元ならば $a \neq b$ であるから他逆元の個数はつねに偶数である. このことから自逆元の個数によって群の位数の**偶奇性**³が決まる. これについて, 次の命題が成り立つ.

【命題 1.4】 (平方剰余の相互法則の第一補充法則) p を奇素数とすると,

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

-1 は $4n+1$ 型の素数の平方剰余であり, $4n-1$ 型の素数の平方非剰余であることをルジャンドルの記号で表している. 右辺の指数の $(p-1)/2$ は $p = 4n+1$ では偶数なので右辺は 1 (平方剰余), $p = 4n-1$ ならば奇数なので右辺は -1 (平方非剰余)となる.

【証明】 F_p^* の自逆元を a とすれば $a^2 = 1$, その解は明らかに $a = \pm 1$ である. 命題 1.1 により ± 1 以外に自逆元はない.

$p = 4n+1$ のとき, $|N| = (p-1)/2 = 2n$ で偶数. ここから他逆元の個数 (偶数) を引けば自逆元の個数となるから自逆元は偶数個. そして, ± 1 以外の自逆元 $r \in N$ があるとすると $r \in F_p^*$ となって矛盾する. ゆえに $-1 \in N$.

$p = 4n-1$ のとき, $|N| = (p-1)/2 = 2n-1$ で奇数. ここから他逆元の個数 (偶数) を引けば自逆元の個数となるから自逆元は奇数個となるが, $+1 \in N$ 以外に自逆元が存在すれば上記の通り矛盾するので, $-1 \in N$. $\parallel$

命題 1.3 と命題 1.4 からさらに次の命題が出てくる.

【命題 1.5】 p を奇素数, a を p の倍数でない整数とすれば,

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

すなわち, p が $4n+1$ 型の素数ならば, 整数 a が平方剰余／非剰余であるに従って $-a$ も平方剰余／非剰余である. また $4n-1$ 型の素数ならば, a が平方剰余／非剰余のとき $-a$ は平方非剰余／剰余である.

【証明】 F_p^* の平方剰余の群を N , 平方非剰余の集合を L とする. p が $4n+1$ 型ならば命題 1.4 より $-1 \in N$. ゆえに $a \in N$ ならば $-1a = -a \in N$. また $a \notin N$ ならば $-1a = -a \notin N$ (命題 1.3 ②). p が $4n-1$ 型のときは命題 1.5 より $-1 \in L$. よって $a \in N$ のとき $-1a \in L$ (命題 1.3 ②). 同様に $a \notin N$ のとき $-1a \in N$ (命題 1.3 ③). $\parallel$

³ 偶奇性とはある整数が偶数か奇数かを表す語. 偶数のときを 0 で, 奇数のときを 1 で表す.

例： $p = 17$ のとき、 $(p-1)/2 = 8, \pm 4 \in N$ だから $\left(\frac{4}{17}\right)\left(\frac{-4}{17}\right) = 1^8 = 1$, $p = 19$ のとき、 $(p-1)/2 = 9$, $4 \in N, -4 \notin N$ だから $\left(\frac{4}{19}\right) = 1, \left(\frac{-4}{19}\right) = -1$. ゆえに $\left(\frac{4}{19}\right)\left(\frac{-4}{19}\right) = (-1)^9 = -1$.

命題1.5 では p の $4n \pm 1$ の型によって整数 $\pm a$ のルジャンドル記号が同符号か異符号かはわかるが, $a, -a$ それぞれが平方剰余か否かは決定できない. 「相互法則」たる所以である.

ここで以後の議論を見やすくするために新しい記号を導入する. すなわち, F_p^* の正剰余 $\{1, 2, 3, \dots, (p-1)/2\}$ に p の倍数でない任意の整数 a をかけた (F_p^* の元としての) 集合を $P(a)$ で表す (記号 P は素数 p に対応する). $a = 1$ のときは正剰余の集合自身で $P(1)$ と表される.

$$P(a) = \{1a, 2a, 3a, \dots, \frac{p-1}{2}a\}$$

$a \neq 1$ の場合, この中のいくつかは負剰余になるが, 絶対値は $P(1)$ の元と同じ $1, 2, 3, \dots, (p-1)/2$ である. $P(-1)$ は負剰余の集合を表す. $P(-a)$ は $P(a)$ のすべての元が符号を変えたものとなる. ゆえに $P(-a)$ の正/負剰余は, 絶対値が同じ $P(a)$ の負/正剰余が符号を変えたものになる.

例: $a = 4$ とする.

$$p = 13 \text{ のとき, } P(1) = \{1, 2, 3, 4, 5, 6\}, P(4) = \{-1, -2, 3, 4, -5, -6\}, P(-4) = \{1, 2, -3, -4, 5, 6\}.$$

$$q = 11 \text{ のとき, } Q(1) = \{1, 2, 3, 4, 5\}, Q(4) = \{1, -2, -3, 4, 5\}, Q(-4) = \{-1, 2, 3, -4, -5\}.$$

さらに $P(a)$ の元をすべてかけ合わせた積 (F_p^* の元) を $P(a)!$ で表そう. したがって $P(1)! = 1 \times 2 \times \dots \times (p-1)/2 = \{(p-1)/2\}!$ である. $a \neq 1$ のとき $P(a)$ の元にはいくつかの負剰余が表れる. その個数を m 個とすると, m が偶数なら $P(a)!$ と $P(1)!$ は同符号, 奇数なら異符号となる. このことを式で表すと,

$$\begin{aligned} P(a)! &= 1a \times 2a \times 3a \times \dots \times a(p-1)/2 \\ &= \{(p-1)/2\}! \times a^{(p-1)/2} \\ \therefore P(a)! &= P(1)! \times a^{(p-1)/2} \end{aligned}$$

この式から, m が偶数なら $a^{(p-1)/2} = 1$, 奇数なら $a^{(p-1)/2} = -1$ ということがわかる. $P(a)!$ の符号は $a^{(p-1)/2}$ によって決まるのである. 以上から, m を $P(a)$ 中の負剰余の個数とすると,

$$a^{(p-1)/2} = \begin{cases} 1 & (a \in N) \\ -1 & (a \notin N) \end{cases} \quad \text{または} \quad a^{(p-1)/2} = (-1)^m$$

これが「**オイラーの基準**」である. さらにオイラーの基準の両辺を 2 乗すれば,

$$a^{p-1} = 1$$

これは「**フェルマの小定理**」と呼ばれている. この定理の意味は, F_p^* の任意の元 a を $p-1$ 乗すれば 1 になるというのである. これらによって a が平方剰余であるための必要十分条件が $a^{(p-1)/2} = 1$ であることが示される.

【命題 1.6】 a を p の倍数でない整数とする. F_p^* において, a が平方剰余であるための必要十分条件は $a^{(p-1)/2} = 1$ となることである.

【証明】まず必要であることを示す. $a \in N$ ならば $r^2 = a$ となる $r \in \mathbb{F}_p^*$ が存在する. $(p-1)/2 = f$ とおくと $p-1 = 2f$. $r^2 = a$ の両辺を f 乗すれば $r^{2f} = a^f$ で, 左辺はフェルマの小定理によって 1 になるので $a^f = 1$.

次に, 任意の $r \in \mathbb{F}_p^*$ はフェルマの定理から $r^{p-1} = r^{2f} = 1$. ゆえに $a^f = 1$ とすれば, $(r^2)^f = a^f$ より $r^2 = a$ となる r が存在する. すなわち a は平方剰余である. $\parallel$

以上から, $a \in N \Leftrightarrow a^{(p-1)/2} = 1$, $a \in L \Leftrightarrow a^{(p-1)/2} = -1$ が成り立つ.

オイラーの基準からただちに次の「**ガウスの予備定理**」が示される. ガウスの予備定理とは, $P(a)$ に含まれる負剰余の個数の偶奇性によって平方剰余の可否を判定するというものである.

【命題 1.7】 (**ガウスの予備定理**) a を p の倍数でない整数とする. $\mathbb{F}_p^*$ において, $P(a)$ に含まれる負剰余の個数が偶数なら a は平方剰余, 奇数なら平方非剰余である.

【証明】 $P(a)$ の負剰余の個数が偶数ならオイラーの基準 $a^{(p-1)/2} = 1$ から $a \in N$. 奇数なら $a^{(p-1)/2} = -1$, すなわち $a \notin N$. $\parallel$

このように, 「 $P(a)$ の負剰余の個数」は a が平方剰余・平方非剰余であることを決定する数値となるので, 新たに記号を設けて, $P(a)$ の負剰余の個数を $|P(a)|'$ で表す (「'」に注意).

p の型による $|P(a)|'$ と $|P(-a)|'$ の偶奇性の関係を見よう.

$p = 4n + 1$ のとき, $|P(a)|$ は $(p-1)/2 = 2n$ で偶数になる. このとき $|P(a)|'$ が偶数または奇数なら a は平方剰余または平方非剰余. そして $-a$ も命題 1.5 から平方剰余または非剰余. 実際 $P(-a)$ は $P(a)$ の元の符号がすべて変わったもので, $|P(a)|'$ は $|P(a)|$ の正の元の個数になるから $|P(-a)|' = |P(a)| - |P(a)|'$ は偶数 - (偶数または奇数) となり, $|P(-a)|'$ は偶数または奇数となる. すなわち $|P(a)|'$ と $|P(-a)|'$ の偶奇性が一致する.

$p = 4n - 1$ のとき, $|P(a)|$ は $(p-1)/2 = 2n - 1$ で奇数. このとき $|P(a)|'$ が偶数または奇数なら a は平方剰余または平方非剰余である. 一方 $-a$ は命題 1.5 から逆に平方非剰余または平方剰余になる. 実際 $|P(-a)|'$ は $|P(a)|$ の正の元の個数に等しいから $|P(-a)|' = |P(a)| - |P(a)|'$ は奇数 - (偶数または奇数) となり, $|P(a)|'$ は奇数または偶数になる. よって $|P(a)|'$ と $|P(-a)|'$ は偶奇性が反対になる.

以上から, $p = 4n + 1$ 型の場合には $|P(a)|'$ と $|P(-a)|'$ の偶奇性が一致, $p = 4n - 1$ 型の場合には偶奇性が反対になる.

【命題 1.9】 (**平方剰余の相互法則の第二補充法則**)

$p = 4n + 1$ ならば, n の偶/奇数にしたがって ± 2 はともに平方剰余/非剰余である. また $p = 4n - 1$ のとき, n の偶/奇数にしたがって 2 は平方剰余/非剰余であり, -2 は逆に平方非剰余/剰余である. ($\pm$, 偶/奇数, 平方剰余/非剰余, 平方非剰余/剰余は同順とする.)

【証明】 $P(2)$ の負剰余は 2 で割れば $P(1)$ の正剰余になるから $P(2)$ の奇剰余である．任意の奇素数の F_p における奇剰余は， $\pm 1, \pm 3, \dots, \pm (2n-1)$ の $2n$ 個である（1 ページ参照），ゆえに負の奇剰余はその半分の n 個すなわち $|P(2)|' = n$ ． p が $4n \pm 1$ 型いずれの場合でも n の偶／奇数によって 2 の平方剰余・非剰余が決まる．次に， -2 では，命題 1.6 によって， $p = 4n + 1$ のとき n の偶／奇数によって平方剰余／非剰余， $p = 4n - 1$ のときは逆に平方非剰余／剰余となる //

平方剰余の相互法則の第二補充法則は，通常ルジャンドル記号で，

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

と表される． -2 についてはこの公式だけではなく，第一補充法則と併用することで導かれる．

「ガウス整数論」では，2 は $p=8n \pm 1$ のとき平方剰余で， $8n \pm 3$ のとき平方非剰余であるとするが（第 112 条），これは $p=4n \pm 1$ の n を偶数なら $n=2m$ ，奇数なら $2m+1$ とおくことで $p=8m \pm 1$ ， $8m \pm 3$ と変形できる．本論では全体的に偶奇性を重んじているのでこのようにした．

以上の準備をもって，次章で平方剰余の相互法則を証明する．

2. 平方剰余の相互法則

今後、本論において誤解のない場合には「平方剰余・平方非剰余」の意味として「剰余・非剰余」と表す。

平方剰余の相互法則をルジャンドル記号で示す。

【命題 2.1】（平方剰余の相互法則） p, q を異なる奇素数とすると、

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

法則の意味は、「 p, q のうち少なくとも一つが $4n+1$ の形の素数ならば、 $\left(\frac{p}{q}\right)$ と $\left(\frac{q}{p}\right)$ はともに $+1$ またはともに -1 で、すなわち相等しい。 p も q も $4n-1$ の形の素数であるときに限って $\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right)$ 。」

(高木貞治「初等整数論講義」§13.)

(例： $p=17, q=13$ (ともに $4n+1$ 型) のとき、 17 は 13 の剰余($2^2=4=17$)、 13 も 17 の剰余($8^2=64=13$)である。

よって $\left(\frac{17}{13}\right) = \left(\frac{13}{17}\right) = 1$ 、ゆえに左辺 $= 1 \times 1 = 1$ 、右辺の指数は $(17-1)/2=8$ 、 $(13-1)=6$ より $8 \times 6 = 48$ (偶数)。

よって右辺 $= (-1)^{48} = 1$ 。

また $p=19, q=11$ (ともに $4n-1$ 型) ならば、 19 は 11 の非剰余、 11 は 19 の剰余($7^2=49=11$)。ゆえに $\left(\frac{19}{11}\right) = -1$ 、 $\left(\frac{11}{19}\right) = 1$ 。ゆえに左辺 $= (-1) \times 1 = -1$ 。右辺の指数は $(19-1)/2=9$ 、 $(q-1)=5$ より $9 \times 5 = 45$ (奇数)。よって右辺 $= (-1)^{45} = -1$ 。

【証明】 証明は次の三段階を示した後に与えられる。以下、 p, q ($p > q$) を奇素数とするが、 $p < q$ のときは逆にするだけである。

【1】まず $Q(-p) \subset P(q)$ を示す。

【2】次に集合 $R = P(q) - Q(-p)$ のある対称性を示す。

【3】最後に集合 R が奇数個の元を持つ場合を示す。

以下、有限体 F_p, F_q を前提する。 $P(1), Q(1)$ はそれぞれ F_p^*, F_q^* の正剰余の集合を表す。

【1】 $Q(-p) \subset P(q)$ を示す。 $r \in Q(p)$ とすれば、整数計算で $kp = lq + r$ となる正整数 k, l が存在する。よって $lq = kp - r$ 。これは $-r$ が $P(q)$ の元であることを示す。一方、 $-r \in Q(-p)$ であるから $Q(-p) \subset P(q)$ となる。

例： $p = 19, q = 7$ とする。 $P(7) = \{-1, 2, -3, 4, -5, 6, 7, -8, 9\}$ 。同様に $Q(19) = Q(-2) = \{1, -2, 3\}$ 。

よって、 $Q(-19) = Q(2) = \{-1, 2, -3\}$ 、すなわち $Q(-19) \subset P(13)$ 。

【2】次に、集合 $R = P(q) - Q(-p)$ の元を絶対値の昇順に並べた数列を $\{s_k\}$ とする。

上の例では $R = \{4, -5, 6, 7, -8, 9\}$ 、 $\{s_k\} : 4, -5, 6, 7, -8, 9$

この数列の項数は $m = (p - q)/2$ で、各項を絶対値として見れば、初項は $|s_1| = (q + 1)/2$ 、末項は $|s_m| = (p - 1)/2$ 、公差は+1である。 $\{s_k\}$ の著しい性質は、初項と第 m 項（末項）；第二項と第 $m - 1$ 項；等々の符号が等しいことである。以下、このことを証明しよう。

$$|s_1| = \frac{q+1}{2}, |s_2| = \frac{q+3}{2}, \dots, |s_k| = \frac{q+(2k-1)}{2}, \dots$$

同様に今度は R を絶対値の降順に並べた数列を $\{t_k\}$ とすると、

$$|t_1| = \frac{p-1}{2}, |t_2| = \frac{p-3}{2}, \dots, |t_k| = \frac{p-(2k-1)}{2}, \dots$$

このとき、 s_k の符号と t_k の符号が等しいことを示す。

s_k は $P(1)$ のある元 r (正) と q の積 $qr = s_k$ である。ということは $q(-r) = -(qr) = -s_k$ となる。ゆえに F_p における二つの方程式 $qx = s_k$ および $qx = -s_k$ は、一方は正の解を持ち、他方は負の解を持つ。一方を解くことで他方も明らかになるので $|s_k| = s$ を正数として $qx = s$ を解けばよい。

$qx = s$ の解を x_1 とする。もし x_1 が正数ならば、正の x_1 に q をかけた結果、正の s になったのだから $qr = s_k$ の s_k も正でなくてはならない。すなわち s_k の符号は x_1 の符号に等しい。

もし x_1 が負ならば、負の x_1 に q をかけて正の s になったことになる。だから $-x_1$ (これが $P(1)$ の元) に q をかければ $q(-x_1) = -qx_1 = -s$ 、すなわち負になる。ということは $qr = s_k$ の s_k は $s_k = -|s_k|$ 、すなわち負であり、この場合も x_1 の符号に等しくなる。以上から出てくる結論は、「 s_k の符号は方程式 $qx = |s_k|$ の解の符号に等しい」ということである。

このことを利用して s_k, t_k の符号を求めよう。 F_p における2つの方程式 $qx = |s_k|$, $qy = |t_k|$,

$$qx = \frac{q+(2k-1)}{2}, \quad qy = \frac{p-(2k-1)}{2}$$

を解く。各方程式の両辺に q の逆元 q^{-1} をかけて、

$$x = q^{-1} \cdot \frac{q+(2k-1)}{2}, \quad y = q^{-1} \cdot \frac{p-(2k-1)}{2}$$

体 F_p においては $p \neq 0$, $q^{-1}q = 1$ だから、

$$x = \frac{1+q^{-1}(2k-1)}{2}, \quad y = \frac{-q^{-1}(2k-1)}{2}.$$

x, y に共通する $q^{-1}(2k-1)$ を $q' = q^{-1}(2k-1)$ とおけば、 $0 < q' < (p-q)/2$ で、

$$x = \frac{1+q'}{2}, \quad y = -\frac{q'}{2}.$$

q' を F_p^* の ① 偶剰余, ② 奇剰余に分けて論を進める (以下、複号 $\pm, \mp$ は同順で、正/負の順序も複号の順序にならう)。

① まず q' が $\pm$ 偶剰余 ($\pm 2, \pm 4, \dots$) の場合。 x は分子 $1+q'$ が $\pm$ 奇剰余となるので2で割れば $\mp$ になる。一方、 y の分子の $-q'$ は $\mp$ 偶剰余になり、2で割っても符号は変わらず $\mp$ のままである。

② 次に、 q' を $\pm$ 奇剰余 ($\pm 3, \pm 5, \dots$) とする。このとき x の分子 $1+q'$ は $\pm$ 偶剰余になるから、2で割っても $\pm$ のままである。一方、 y は $-q'$ が $\mp$ 奇剰余になり、2で割れば符号が変わり、 $\pm$ になる。

①②いずれの場合も x, y は同符号である。

以上から数列 $\{s_k\}$, $\{t_k\}$ で s_k, t_k の符号が等しいことが証明された. ということは, R の個数 $m = (p - q)/2$ が偶数のときには, R 内の負の元の個数 $|R|'$ は偶数である. 言い換えると, p, q がともに $4n + 1$ 型, またはともに $4n - 1$ 型なら, m は偶数になる.

例: $p = 19, q = 7$ のとき, $R = \{4, -5, 6, 7, -8, 9\}$ の第 2 項, 第 5 項の符号を求めると, $k = 2$ とおいて,

$$7x = \frac{7 + (2 \cdot 2 - 1)}{2} = 5, \quad 7y = \frac{19 - (2 \cdot 2 - 1)}{2} = 8$$

$$x = 7^{-1} \cdot 5 = -2, \quad y = 7^{-1} \cdot 8 = -7.$$

ゆえに R の第 2 項, 第 5 項の符号はともに負となる. そして R の項数は $9 - 3 = 6$ なので $|R|'$ は偶数となる.

【3】最後に $m = (p - q)/2$ が奇数の場合は $\{s_k\}$ の真ん中の項の符号によって $|R|'$ の偶奇性が決定される. $\{s_k\}$ の真ん中の項は $s_{(1+m)/2}$ で, その絶対値は初項と末項の絶対値の和の半分であるから,

$$|s_{(1+m)/2}| = \frac{|s_1| + |s_m|}{2} = \left(\frac{q+1}{2} + \frac{p-1}{2} \right) / 2 = \frac{p+q}{4} = 4^{-1}q$$

となる. ここで $qx = 4^{-1}q$ とおいて【2】のように解 x を求めると,

$$x = 4^{-1}q \cdot q^{-1} = 4^{-1}$$

ゆえに $s_{(1+m)/2}$ の符号は F_p^* における 4 の逆元 4^{-1} の符号に等しい. ここで $p = 4n \pm 1$ とおけば F_p の元では $4n \pm 1 = 0$. ゆえに $4n = \mp 1 \therefore 4(\mp n) = 1$. よって $\mp n$ は F_p^* における 4 の逆元 4^{-1} である. このとき,

$$1 \leq n = \frac{p \mp 1}{4} < \frac{p-1}{2}$$

であるから n 自身は F_p の元としても正の元である. ゆえに $-n$ は負を表わし, $+n$ は正を表わしている. よって F_p^* の 4^{-1} は $p = 4n + 1$ の場合は負剰余で, $p = 4n - 1$ の場合は正剰余となる.

(例: $p=37=4 \times 9+1$, F_{37}^* での 4 の逆元は -9 で負, $p=43=4 \times 11-1$, F_{43}^* での 4 の逆元は 11 で正.)

【1】, 【2】, 【3】の結果をもって命題 2.1 が証明される. ここでも ±, ∓, 偶/奇数, 奇/偶数 は同順とする.

(1) p, q が同じ型 ($4n \pm 1$ 型) のときは $|P(q)|, |Q(p)|$ の偶奇性が同じなので $|R|$ は偶数.

① p, q がともに $4n + 1$ 型の場合には $|P(q)|, |Q(p)|$ はいずれも偶数. $\left(\frac{q}{p}\right) = \pm 1$ のとき $|P(q)|'$ は偶/奇数になるから $|Q(-p)|' = |P(q)|' - |R|'$ も偶/奇数. そして $|Q(p)|'$ も偶/奇数になるので $\left(\frac{p}{q}\right) = \pm 1$.

ゆえに $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = 1$. 右辺の指数は $(p-1)/2$ も $(q-1)/2$ も偶数なので積も偶数. ゆえに右辺 $= 1$. ゆえに命題は成り立つ.

例: $p=17, q=13$ のとき $(13/17)=(17/13)=1$. または $p=29, q=17$ のとき $(17/29)=(29/17)=-1$.

② p, q がともに $4n - 1$ 型の場合には, $|P(q)|, |Q(p)|$ はいずれも奇数, $\left(\frac{q}{p}\right) = \pm 1$ のとき $|P(q)|'$ は偶／奇数になるから $|Q(-p)|' = |P(q)|' - |R|'$ も偶／奇数. そして $|Q(p)|'$ は奇／偶数になるので $\left(\frac{p}{q}\right) = \mp 1$. ゆえに $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1$. 右辺の指数は $(p-1)/2$ も $(q-1)/2$ も奇数なので積も奇数. ゆえに右辺 $= -1$. ゆえに命題は成り立つ.

例: $p=19, q=7$ のとき $(7/19)=1, (19/7)=-1$. または $p=23, q=19$ のとき, $(19/23)=-1, (23/19)=1$.

(2) p, q が異なる型のときは $|P(q)|, |Q(p)|$ の偶奇性が反対なので $|R|$ は奇数.

① p は $4n + 1$ 型, q が $4n - 1$ 型のとき $|P(q)|$ は偶数, $|Q(p)|$ は奇数. $4^{-1} \in \mathbb{F}_p$ は【3】より負. ゆえに $|R|'$ は奇数. $\left(\frac{q}{p}\right) = \pm 1$ のとき, $|P(q)|'$ は偶／奇数, ゆえに $|Q(-p)|' = |P(q)|' - |R|'$ は奇／偶数. したがって $|Q(p)|'$ は偶／奇数になる. ゆえに $\left(\frac{p}{q}\right) = \pm 1$. よって命題の左辺は $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = 1$. 右辺の指数は偶数 $\times$ 奇数で偶数. ゆえに右辺 $= 1$. よって命題は成り立つ.

例: $p=17, q=11$ のとき, $\left(\frac{11}{17}\right) = \left(\frac{17}{11}\right) = -1$. どちらも -1 なので $\left(\frac{11}{17}\right)\left(\frac{17}{11}\right) = 1$.

② p は $4n - 1$ 型, q が $4n + 1$ 型のとき $|P(q)|$ は奇数, $|Q(p)|$ は偶数. $4^{-1} \in \mathbb{F}_p$ は【3】より正. ゆえに $|R|'$ は偶数. $\left(\frac{q}{p}\right) = \pm 1$ のとき, $|P(q)|'$ は偶／奇数, ゆえに $|Q(-p)|' = |P(q)|' - |R|'$ は偶／奇数. したがって $|Q(p)|'$ は奇／偶数になる. ゆえに $\left(\frac{p}{q}\right) = \mp 1$. よって命題の左辺は $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = 1$. 右辺の指数は偶数 $\times$ 奇数で偶数. ゆえに右辺 $= 1$. よって命題は成り立つ. $\parallel$

例: $p=23, q=13$ のとき, $(13/23)=(23/13)=1$.

以上をもって平方剰余相互法則の証明とする.

以上の議論が既存の証明に等しいものがあるかについてはわからない. しかし初等的であることについては, 有限体についてごく初歩的な知識を得ることを厭わなければ, 中高生諸氏にも理解されるものと自負している.

【付録】

【1】 (p.1 注1) すべての奇素数は $4n \pm 1$ の形で表すことができる.

【証明】 任意の正の奇数を $2n+1$ とすれば, $n=0,1,2,3,\dots$. このとき $n=2m, 2m-1$ とおくことで

$$2n+1=2(2m)+1=4m+1=1,5,9,13,\dots$$

$$2n+1=2(2m-1)+1=4m-1=3,7,11,15,\dots$$

したがってすべての奇数を $4m \pm 1$ のどちらかの形で表す事ができる. ゆえに任意の奇素数も $4m \pm 1$ の形に表す事ができる.

(注: ディリクレの定理「初項と公差が互いに素である算術級数(等差数列)には無限に素数が存在する」とは別の定理で, 単に任意の素数を $4n \pm 1$ 型に変形できるというもの. 例: $7368787=4 \times 1842197-1$ など)

【2】 (p.1 注2) 群の定義とは, 一般に, 集合 G における一つの演算について

A 演算の成立とその一意性

B 結合法則

C 逆演算可能

の三つの条件がみたされるとき, 集合 G はこの演算に関して**群**であるという.

(参考: 稲葉栄次 著「群論入門」 培風館発行 新数学シリーズ7)

また, 有限体については, 詳しい定義はここでは示せないが, F_p のように四則計算が可能な有限個の元からなる集合で, E.ガロアの発見によることから**ガロア体**ともいう.

【あとがき】

この小論は、同じテーマで書いた前論文が2022年10月に完成し、2023年10月までここに掲載していた同名の小論文の書き直しである。あえてVer.2としたのは、最後の相互法則証明の部分を大幅に変更したことによる。したがって前の論文と別物とはせずに差し替えることにした。

有限体の性質を利用するなどの証明の根幹は変えないで、表現を簡便かつ短縮することを前論文以上に心がけた。ただ、複号の多用によって読みにくくなった感も否めない。

証明自体の平易さは高木貞治先生の格子の利用による証明（「初等整数論講義」§13）に劣らないと自負している。先生の証明はわずか2ページを費やすのみであるのに、本論文では有限体の性質を説明するのに多くの頁を割く（10ページ余）ことになったことはやむを得ないと思っている。

有限体（ガロア体）の精妙さ、奥の深さは計り知れない。このまま3次、4次剰余の研究にまで発展させられる可能性を秘めている。ただ、自分にはもう時間がない。いろいろな誘惑がそれを許さないのだ。

それでも、相互法則のガウスの他の証明と、自分の行なった証明との関係などは引き続き検討していきたい。そうでなくてはおよそ10年をかけたこの研究の意義を見つけないような気になっている。さいわい高瀬正仁氏の「ガウス数論論文集」（ちくま学芸文庫）なる小冊子を手に入れたのを機にその方向に進むきっかけを掴むことができたようだ。

まだまだ平方剰余の相互法則とは縁が切れそうにない、幸か不幸か。

2023年12月1日 76歳を目前に
福沢正男

【索引】

	あ行		た行
位数	1, 3	第一補充法則	3
オイラーの基準	5	第二補充法則	6
	か行	他逆元	3
ガウスの補助定理	5	高木貞治	7
奇剰余	1, 6, 8, 9		は行
偶剰余	1, 8	フェルマの定理	5
偶奇性	3, 5, 6	非剰余	2, 3, 4, 5, 6, 7
群	1	負剰余	1, 4, 5, 6, 9
	さ行	部分群	2
自逆元	3		
正剰余	1, 4, 6, 7, 9		
絶対的最小剰余	1		
相互法則	1, 3, 4, 6, 7		