「平方剰余の相互法則」の解説（平成２５年）

0. 平方剰余の定義

$x^2 \equiv a \pmod{p}$ が可解 $\overset{\text{def}}{\Leftrightarrow}$ a を 法 p による平方剰余

1. ルジャンドルの記号

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

フェルマーの定理より

p：奇素数, $(a, p) = 1$ のとき

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

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}$$

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

a：平方非剰余 のとき $a^{\frac{p-1}{2}} \neq 1$

$\therefore\ a^{\frac{p-1}{2}} = -1$ としてよい.

2. オイラーの規準

p：奇素数 $(a, p) = 1$ のとき

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

3. ガウスの予備定理

p：奇素数 $(a, p) = 1$ のとき

$a, 2a, \cdots\cdots, \frac{p-1}{2}a$ の法 p による最小剰余が $\frac{p}{2}$ より大の個数をn とすると

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

Proof. 法 p の既約剰余は $\pm 1, \pm 2, \cdots\cdots, \pm \frac{p-1}{2}$ の p - 1 個である.

p の既約剰余 r は $1, 2, \cdots\cdots, p-1$ だから, 次の変換により

剰余 r が $\frac{p}{2}$ より小のとき

$$r' = r$$

剰余 r が $\frac{p}{2}$ より大のとき

$$r' = r - \frac{p}{2}$$

$-\frac{p}{2} < r' < \frac{p}{2}$ となる. 即ち $\pm 1, \pm 2, \cdots\cdots, \pm \frac{p-1}{2}$

p - 1 個の剰余は 2 個ずつ p に関して合同であり, $\frac{p-1}{2} + n = p - 1$

$$\therefore\ n = \frac{p-1}{2}$$

$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$ だから

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

4. 定理　p, q : 奇素数 のとき　$(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$

Proof1.（1）　$(\frac{a}{p}) = (\frac{b}{p}) = 1$ のとき

$$r_1^2 \equiv a,\quad r_2^2 \equiv b \pmod{p}$$

$$\therefore\quad (r_1\ r_2)^2 \equiv ab \pmod{p}$$

$$\therefore\quad (\frac{ab}{p}) = 1$$

$$\therefore\quad (\frac{ab}{p}) = 1 \times 1 = (\frac{a}{p})(\frac{b}{p})$$

（2）　$(\frac{a}{p}) = 1,\quad (\frac{b}{p}) = -1$ のとき

まず, 次のことを示す.

$(\frac{a}{p}) = 1$ のとき

$$(\frac{ab}{p}) = 1 \quad \Rightarrow (\frac{b}{p}) = 1$$

$\because\quad r_1^2 \equiv a,\quad r_3^2 \equiv ab \pmod{p}$

$$\therefore\ (r_1^{-1}\ r_3)^2 = b \pmod{p}$$

$$\therefore\ (\frac{b}{p}) = 1$$

対偶をとると,

$$(\frac{a}{p}) = 1 \quad \text{のとき} \quad (\frac{b}{p}) = -1 \quad \Rightarrow (\frac{ab}{p}) = -1$$

$$\therefore\ (\frac{ab}{p}) = -1 = 1 \times (-1) = (\frac{a}{p})(\frac{b}{p})$$

（3）　$(\frac{a}{p}) = -1,\quad (\frac{b}{p}) = 1$　のとき

2. と同様に示すことが出来る.

（4）　$(\frac{a}{p}) = -1,\ (\frac{b}{p}) = -1$ のとき

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

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

$$\therefore\ (ab)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

$$\therefore\ (\frac{ab}{p}) = 1$$

$$\therefore\ (\frac{ab}{p}) = 1 = (-1) \times (-1) = (\frac{a}{p})(\frac{b}{p})$$

qed.

proof 2.　$(\frac{ab}{p}) = (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}\ b^{\frac{p-1}{2}} = (\frac{a}{p})(\frac{b}{p})$　qed.

proof 3.　$a \equiv r^k \pmod{p},\ b \equiv r^l \pmod{p}$ とする

$$ab \equiv r^{k+l} \pmod{p}$$

$$\therefore\ (\frac{ab}{p}) = (-1)^{k+l} = (-1)^k(-1)^l = (\frac{a}{p})(\frac{b}{p})$$　qed.

注　proof 1 は Euler の規準までを前提とした証明.
proof 2 は Euler の規準だけによる証明.
proof 3 は Gauss の予備定理による証明である.

5. 第 2 補充法則　p：奇素数

$$(\frac{2}{p}) = \begin{cases} 1 & p \equiv 1, 7 \pmod{8} \\ -1 & p \equiv 3, 5 \pmod{8} \end{cases}$$

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

(Lagrange)

Proof. p：奇素数 だから

$$p \neq 2, 4$$

$$p \equiv 1, 3, 5, 7 \pmod{8}$$

1 の原始 8 乗根を ζ とする

$$\zeta^8 = 1$$

$\zeta^4 \neq 1$ だから $\zeta^4 = -1$

$$\zeta^3 = -\zeta^{-1}, \quad \zeta^2 = -\zeta^{-2}, \quad \zeta = -\zeta^{-3}$$

$\zeta + \zeta^{-1} = \alpha$ とおくと ……(1)

$\zeta^2 + \zeta^{-2} = 0$ だから

$\alpha^p = \zeta^p + \zeta^{-p}$ $\quad p \equiv 1, 3, 5, 7 \ (mod\ 8)$

$p \equiv 3$ のとき $\zeta^3 + \zeta^{-3} = -\alpha$

$p \equiv 5$ のとき $\zeta^5 + \zeta^{-5} = -\zeta - \zeta^{-1} = -\alpha$

$p \equiv 7$ のとき $\zeta^7 + \zeta^{-7} = \zeta^3\zeta^4 + \zeta^{-3}\zeta^{-4}$

$$= -(\zeta^3 + \zeta^{-3})$$

$$= -\alpha$$

$$\alpha^p = \begin{cases} \alpha & p \equiv 1, 7 \ (mod\ 8) \\ -\alpha & p \equiv 3, 5 \ (mod\ 8) \end{cases}$$

$$\alpha^{p-1} = \begin{cases} 1 & p \equiv 1, 7 \ (mod\ 8) \\ -1 & p \equiv 3, 5 \ (mod\ 8) \end{cases}$$

(1) より

$\alpha^2 = \zeta^2 + 2 + \zeta^{-2}$

$\zeta^2 + \zeta^{-2} = 0$ だから

$\alpha = \pm \sqrt{2}$

$\alpha = \sqrt{2}$ とおくと

$$2^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1, 7 \ (mod\ 8) \\ -1 & p \equiv 3, 5 \ (mod\ 8) \end{cases}$$

qed.

6. 相互法則

p, q : 奇素数 のとき $\quad \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Proof.

剰余系

$1, 2, \cdots\cdots, \frac{p-1}{2}$ に属す整数を x とする.

$$\frac{q}{p}x - \frac{1}{2} \in \mathbb{Z}$$

$$\because \ \frac{q}{p}x - \frac{1}{2} = \frac{2qx - p}{2p}$$

p, q : 奇素数 $\quad 2qx - p$: 奇数 $\quad 2p$: 偶数

$$\therefore \ \frac{q}{p}x - \frac{1}{2} \in \mathbb{Z}$$

いま整数 y をつぎのようにとる.

$$\frac{q}{p}x - \frac{1}{2} < y < \frac{q}{p}x + \frac{1}{2}$$

即ち $-\frac{p}{2} < qx - py < \frac{p}{2}$

(*i*) $y < \frac{q}{p}x + \frac{1}{2}$ かつ $0 < y < \frac{q}{2}$ のとき

剰余系 $-1, -2, \cdots\cdots, -\frac{p-1}{2}$ を 法 p に関して合同なるものは

$$1 \leqq y \leqq \frac{q-1}{2}, \quad -\frac{p}{2} < qx - px < 0$$

$qx - px$ の個数を n とすると,

Gauss 予備定理より

$$\left(\frac{q}{p}\right) = (-1)^n \quad \cdots\cdots\cdots\cdots\cdots\cdots (1)$$

同様にして 剰余系

$1, 2, \cdots\cdots, \frac{q-1}{2}$ に属す整数を y とする.

$\frac{p}{q}y - \frac{1}{2} < py - qx < \frac{q}{2}$ なる整数 x がとれる.

(*ii*) $x < \frac{p}{q}y + \frac{1}{2}$ かつ $0 < x < \frac{p}{2}$ のとき

剰余系 $-1, -2, \cdots\cdots, -\frac{q-1}{2}$ を 法 q に関して合同なるものは

$$1 \leqq x \leqq \frac{p-1}{2}, \quad -\frac{q}{2} < py - qx < 0$$

$py - qx$ の個数を m とすると,

Gauss の予備定理より

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

(i)(ii)より

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^n (-1)^m = (-1)^{n+m} \quad \cdots\cdots\cdots\cdots\cdots (3)$$

$qx - py$ の個数を考える.

整数 x, y は, それぞれ 剰余系 $1, 2, \cdots\cdots, \frac{p-1}{2}$ 剰余系 $1, 2, \cdots\cdots, \frac{q-1}{2}$ に属するから,

整数 x の個数は $\frac{p-1}{2}$, 整数 y の個数は $\frac{q-1}{2}$

よって $qx - py$ の個数は $\frac{p-1}{2}\,\frac{q-1}{2}$

この内　n 個は　　$-\frac{p}{2} < qx - py < 0$

　　m 個は　　$0 < qx - py < \frac{q}{2}$

を満足する.

残りは　$qx - py > \frac{q}{2}$ を満足するものと $qx - py < -\frac{p}{2}$ を満足するものは 同個数である.

$\because$ $qx - py > \frac{q}{2}$ のとき　次の変換をする.

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

$$qx - py = q\left(\frac{p+1}{2} - x\right) - p\left(\frac{q+1}{2} - y\right)$$

$$= \frac{q-p}{2} - (qx' - py')$$

$\frac{p-1}{2}\frac{q-1}{2} - (n+m)$：偶数

$\therefore$　$\frac{p-1}{2}\frac{q-1}{2} \equiv (n+m) \pmod 2$

$\therefore$　$(-1)^{n+m} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$　……(4)

(3) (4) より

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

qed.

文　　献

1. 数論入門　　山本　芳彦　著　岩波書店　２００３
2. 整数論　　草場　公邦　著　日本放送出版協会　１９７４
3. 数論入門　　北村　泰一　著　槙書店　１９９９
4. 相互法則入門　　平松　豊一　著　牧野書店　１９９８