平方剰余の相互法則

都築 暢夫

平成 18 年度「先端数学」

6 月 30 日（金） 2 時限

1. はじめに

平方剰余はオイラーの時代から考察されていて、素数の不思議な関係を表す「平方剰余の相互法則」の存在は意識されていた。平方剰余の相互法則はガウスにより最初に厳密に証明され、現在までに多くの別証明が与えられている。平方剰余の相互法則は、「類体論」の最初の顕在化ともいうべきもので、ガウスの考察は現在の整数論の序章である。

この時間は、p 元体の導入と平方剰余について解説をし、「平方剰余の相互法則」を紹介する。

2. p 元体 $\mathbb{F}_p$

p を素数とする。

定義 2.1. 整数 a, b に対して

$$a \equiv b \pmod{p} \Leftrightarrow p \mid a - b$$

と定めて、a と b は p を法として合同という。

命題 2.2. $\equiv$ は整数環 $\mathbb{Z}$ 上の同値関係になり

$$\left.\begin{array}{l} a \equiv b \pmod{p} \\ c \equiv d \pmod{p} \end{array}\right\} \Rightarrow \left\{\begin{array}{l} a + c \equiv b + d \pmod{p} \\ ac \equiv bd \pmod{p} \end{array}\right.$$

を満たす。特に、同値類の集合 $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\equiv$ は環になる。

定理 2.3. 環 $\mathbb{Z}/p\mathbb{Z}$ は体である。

証明. p と互いに素な整数 a に対して

$$ax + py = 1$$

となる整数 x, y が存在するから

$$ax \equiv 1 \pmod{p}$$

となり、a の像は $\mathbb{Z}/p\mathbb{Z}$ の中で可逆である。 □

定義 2.4. 環 $\mathbb{Z}/p\mathbb{Z}$ を $\mathbb{F}_p$ で表し、p 元体という。

3. 平方剰余

以下、p を 2 でない素数とする。

定義 3.1. p と素な整数 a に対して、p を法として a が平方数になるとき a は p を法として平方剰余といい、そうでないとき平方非剰余という。すなわち、

$$a \text{ は平方剰余} \quad \Leftrightarrow \quad a \equiv b^2 \pmod{p} \, (\exists b \in \mathbb{Z})$$

と定める。

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

とおき、$\left(\frac{a}{p}\right)$ をルジャンドル記号という。

命題 3.2. $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

特に、$\left(\frac{a}{p}\right)$ は $\mathbb{F}_p^\times$ から $\{\pm 1\}$ への写像と見なせる。

例 3.3. $p = 7$ **のとき次のようになる。**

b	0	1	2	3	4	5	6
b^2	0	1	4	9	16	25	36
$b^2 \pmod{p}$	0	1	4	2	2	4	1

a	1	2	3	4	5	6
$\left(\frac{a}{p}\right)$	1	1	-1	1	-1	-1

4. p 元体 と平方剰余

定理 4.1. $\mathbb{F}_p$ **の乗法群** $\mathbb{F}_p^\times$ **は位数** $p-1$ **の巡回群である。**

証明. **有限アーベル群の基本定理から、**

$$\mathbb{F}_p^\times \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_r\mathbb{Z}$$
$$1 < n_1 \,|\, n_2 \,|\, \cdots \,|\, n_r$$

となり、位数が n_1 **の元の個数は** n_1^r **個である。一方、**$\mathbb{F}_p$ **は体なので、**$x^{n_1}-1=0$ **の解は高々** n_1 **個である。したがって、**$r=1$ **となり、**$\mathbb{F}_p^\times$ **は巡回群である。** □

定理 4.2. $a \in \mathbb{F}_p^\times$ **とすると**

$$a^{\frac{p-1}{2}} = 1 \Leftrightarrow \exists b \in \mathbb{F}_p \text{ s.t. } a = b^2$$

が成り立つ。特に

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

である。これを、オイラー規準という。

証明. α **を** $\mathbb{F}_p^\times$ **の生成元とし** $a = \alpha^r$ **とすると、 位数はちょうど** $p-1$ **なので**

$$a^{\frac{p-1}{2}} = \alpha^{\frac{p-1}{2}r} = 1 \Leftrightarrow p-1 \,\Big|\, \frac{p-1}{2}r \Leftrightarrow 2 \,|\, r \Leftrightarrow a = (\alpha^{\frac{r}{2}})^2$$

となる。$\mathbb{F}_p^\times$ **は位数が** $p-1$ **なので、**$a^{\frac{p-1}{2}} = \pm 1$ **である。** □

5. ガウスの準備定理

$\mathbb{F}_p^\times$ の部分集合 S と T を

$$S = \{1, 2, \cdots, \tfrac{p-1}{2}\}$$
$$T = \{\tfrac{p+1}{2}, \cdots, p-1\}$$

とする。$a \in \mathbb{F}_p^\times$ に対して、

$$n_p(a) = \sharp\{s \in S \,|\, as \in T\}$$

と定める。

例 5.1. $\mathbb{F}_p$ において $-i = p - i$ なので、$-S = T$ である。よって

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

となる。

定理 5.2. *bf (*ガウスの準備定理*)* $\left(\frac{a}{p}\right) = (-1)^{n_p(a)}$.

証明. $T = -S$ **なので、**$as = \epsilon_s(a)u_s(a)\,(\epsilon_s(a) = \pm 1, u_s(a) \in S)$ **と表せる。**$s_1 \neq s_2$ **ならば** $u_{s_1}(a) \neq u_{s_2}(a)$ **なので、**

$$a^{\frac{p-1}{2}} \prod_{s\in S} s = \prod_{s\in S} as = \prod_{s\in S} \epsilon_s(a)u_s(a) = (-1)^{n_p(a)} \prod_{s\in S} s$$

となる。$\prod_{s\in S} s \neq 0$ **なので、**

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

となる。 □

定理 5.3. p **を奇素数とする。**

$$(1)\,(\text{第 } 1 \text{ 補充則})\ \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases}$$

$$(2)\,(\text{第 } 2 \text{ 補充則})\ \left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1, 7 \pmod 8 \\ -1 & p \equiv 3, 5 \pmod 8. \end{cases}$$

証明. **(2)** $p \equiv 1 \pmod 8$ **とする。** $2s \in T$ **となる** $s \in S$ **は**

$$\frac{p+1}{2} \leq 2s \leq p-1$$

のときのみ。 $p \equiv 1 \pmod 8$ **より、** $s = \frac{p+3}{4}, \cdots, \frac{p-1}{2}$ **となり**

$$n_p(2) = \frac{p-1}{2} - (\frac{p+3}{4} - 1) = \frac{p-1}{4}$$

である。これは偶数なので、 $\left(\frac{2}{p}\right) = 1$ **である。** □

6. 平方剰余の相互法則

定理 6.1. (平方剰余の相互法則) p, q **を互いに異なる奇素数とする。**

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

例 6.2. $p = 3, q = 7$ **とすると**

$$\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1, \left(\frac{3}{7}\right) = -1$$

$$(-1)^{\frac{3-1}{2}\times\frac{7-1}{2}} = (-1)^{1\times 3} = -1$$

となるので、相互法則が成り立つ。

例 6.3. 平方剰余の相互法則を用いて計算してみる。

$$
\begin{aligned}
\left(\frac{1009}{2003}\right) &= \left(\frac{2003}{1009}\right) = \left(\frac{994}{1009}\right) \\
&= \left(\frac{2}{1009}\right)\left(\frac{7}{1009}\right)\left(\frac{71}{1009}\right) \\
&= 1 \times \left(\frac{1}{7}\right)\left(\frac{15}{71}\right) \\
&= 1 \times \left(\frac{3}{71}\right)\left(\frac{5}{71}\right) \\
&= (-1) \times \left(\frac{71}{3}\right)\left(\frac{71}{5}\right) \\
&= -\left(\frac{2}{3}\right)\left(\frac{1}{5}\right) \\
&= -(-1) \times 1 \\
&= 1
\end{aligned}
$$

レポート問題. 次から 2 題以上解答せよ。

(1) $p = 11, 13, 17, \cdots$ **に対して、平方剰余のリストを作れ。**

(2) 第 2 補充則の証明を完成させよ。

(3) $\left(\dfrac{3}{p}\right)$ **を求めよ。**

(4) 適当な a, p **に対し、平方剰余の相互法則を用いて** $\left(\dfrac{a}{p}\right)$ **を求めよ。**

(5) 平方剰余の相互法則を証明せよ。

(6) 0 **でない整数** a **に対して、素数** $q(a)$ **(ないこともある) を**

$$q(a) = \min\left\{p : \text{素数} \;\middle|\; \left(\frac{b}{p}\right) = 1\,(\forall b < a), \left(\frac{a}{p}\right) = -1\right\}$$

と定める。 $q(a)$ **を (計算機を用いて) 求めよ。**

(7) 感想を書け。

◯ 夏休みに読むことを薦め本

1. 高木貞治「解析概論」(岩波書店)

   言わずと知れた解析学の古典。3 年生が読むと面白さがわかる？

2. G.H.ハーディ、E.M.ライト「数論入門 I・II」
   (シュプリンガー・フェアラーク東京)

   整数論の古典的入門書・素数定理の証明が最大の目標