第11章　平方剰余

11.1　平方剰余記号

第 9 章では自然数を法とする整数のベキ乗数のふるまいについて述べ，第 10 章でその暗号への応用を紹介したが，本章ではとくに平方数について考察する．

定義 11.1 p を奇素数（つまり，2 でない素数）とし，a を p で割り切れない整数とする． 合同式

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

が整数解をもつとき，a は p を法として**平方剰余**であるといい，もたないとき**平方非剰余**であるという． さらに，

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & p\nmid a \text{ かつ } a \text{ が } p \text{ を法として平方剰余のとき,} \\ -1, & p\nmid a \text{ かつ } a \text{ が } p \text{ を法として平方非剰余のとき,} \\ 0, & p \mid a \text{ のとき} \end{cases}$$

と定め，これを p を法とする**平方剰余記号**という．

例 11.2　$1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 4,\ 4^2 \equiv 1 \pmod 5$ より，5 を法として $1, 4$ は平方剰余であり $2, 3$ は平方非剰余である． また，7 を法とすると，たとえば 2 は平方剰余，5 が平方非剰余であることが確かめられる． さらに，これらは次のように表すことができる;

$$\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = 1, \quad \left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1, \quad \left(\frac{2}{7}\right) = 1, \quad \left(\frac{5}{7}\right) = -1.$$

さて，奇素数 p と互いに素な整数 a に対して，$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) = a^{p-1} - 1 \equiv 0 \pmod p$ がフェルマーの定理からいえる． p は素数なので，$a^{\frac{p-1}{2}} - 1,\ a^{\frac{p-1}{2}} + 1$ のどちらかは p で割り切れ，したがって，$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$ を得る． 次の定理は，この ± 1 が平方剰余記号の値を決めることを示している．

定理 11.3 (オイラーの規準) 奇素数 p と整数 a に対して，

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

が成り立つ．

証明　$p|a$ のときは明らかなので，以下 $p\nmid a$ とする． a が法 p に関して平方剰余ならば，$x^2 \equiv a \pmod{p}$ をみたす整数 x がとれる． このとき，フェルマーの定理より

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

そこで，以下では a は平方非剰余であると仮定する． いま，$A = \{1, 2, \ldots, p-1\}$ として，$r_j, s_j \in A$ $(j = 1, \cdots, (p-1)/2)$ を次の手順で定める． まず，$r_1 \in A$ を任意にとり，$r_1 s_1 \equiv a \pmod{p}$ をみたす $s_1 \in A$ をとる． r_1 は p と互いに素だから，このような s_1 は一意的に存在し，仮定より $r_1 \neq s_1$ である． 次に，$\{r_1, s_1\}$ に属さない $r_2 \in A$ を任意にとって，$r_2 s_2 \equiv a \pmod{p}$ をみたす $s_2 \in A$ をとる． このとき，s_2 は r_1, s_1, r_2 のどれとも異なることが確かめられる． 次に，$\{r_1, s_1, r_2, s_2\}$ に属さない $r_3 \in A$ を任意にとって……，この操作を $A = \{r_1, s_1, \cdots, r_{(p-1)/2}, s_{(p-1)/2}\}$ となるまで繰り返す． そこで，A の元すべての積をとれば，

$$a^{\frac{p-1}{2}} \equiv (r_1 s_1)(r_2 s_2)\cdots(r_{(p-1)/2} s_{(p-1)/2}) = (p-1)! \underset{Why?}{\equiv} -1 = \left(\frac{a}{p}\right) \pmod{p}.$$

ここで，*Why?* の部分は次の補題による． □

補題 11.4 (ウィルソンの定理) 素数 p に対して $(p-1)! \equiv -1 \pmod{p}$ が成り立つ．

証明　上の証明で，A の代わりに $B = \{2, 3, \cdots, p-2\}$ を用いて，$r_j s_j \equiv 1 \pmod{p}$ をみたす $r_j, s_j \in B$ を順にとることを考えれば，$1 \equiv (r_1 s_1)\cdots(r_{(p-3)/2} s_{(p-3)/2}) = (p-2)! \pmod{p}$ が導かれる． よって，$(p-1)! = (p-1)\cdot(p-2)! \equiv p-1 \equiv -1 \pmod{p}$． □

定理 11.5 奇素数 p および整数 a, b に対して次が成り立つ．

(1)　$a \equiv b \pmod{p}$ ならば，$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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

証明　(1) は平方剰余記号の定義から直ちにわかる． また，定理 11.3 より

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

であるが，平方剰余記号は 0 または ± 1 なので，等式 (2) が確かめられる． □

11.2　平方剰余の相互法則，補充法則

整数 a が奇素数 p を法として平方剰余かどうかは，平方剰余記号をオイラーの規準 (定理 11.3) や定理 11.5 を使って計算すれば，原理的には決定することができる． しかし，一般に p が非常に大きいときは膨大な計算が必要となる．

次の 2 つの定理を用いることで，大きな素数を法とする平方剰余記号の計算が小さな素数を法とする計算に帰着され，簡単になる．

定理 11.6 (平方剰余の相互法則) 相異なる奇素数 p, q に対して，

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

別の書き方をすれば，

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\dfrac{p}{q}\right) & (p \equiv 1 \pmod 4 \text{ または } q \equiv 1 \pmod 4 \text{ のとき}), \\ -\left(\dfrac{p}{q}\right) & (p \equiv q \equiv 3 \pmod 4 \text{ のとき}). \end{cases}$$

定理 11.7 (補充法則) 奇素数 p に対して次が成り立つ．

[**第 1 補充法則**] $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & (p \equiv 1 \pmod 4 \text{ のとき}), \\ -1 & (p \equiv 3 \pmod 4 \text{ のとき}). \end{cases}$

[**第 2 補充法則**] $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & (p \equiv 1, 7 \pmod 8 \text{ のとき}), \\ -1 & (p \equiv 3, 5 \pmod 8 \text{ のとき}). \end{cases}$

証明は後回しにして，ここでは，これらの定理がどのように使われるかを解説しよう．いま，$1 < a < p$ のとき，その素因数分解を $a = \prod_{j=1}^{r} q_j^{e_j}$ とすれば，定理 11.5 (2) より，

$$\left(\frac{a}{p}\right) = \prod_{j=1}^{r}\left(\frac{q_j}{p}\right)^{e_j} = \prod_{e_j:\text{奇数}}\left(\frac{q_j}{p}\right).$$

ここで，$q_j = 2$ ならば第 2 補充法則が適用でき，$2 < q_j$ ならば相互法則を用いて p より小さな法 q_j の計算に帰着される．

例 11.8　17 を法とする -7 の平方剰余を調べてみる*．

$$\left(\frac{-7}{17}\right) = \left(\frac{10}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{5}{17}\right) \underset{\text{S2}}{=} \left(\frac{5}{17}\right) \underset{\text{R}}{=} \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) \underset{\text{S2}}{=} -1,$$

あるいは，はじめに第 *1* 補充法則を使って

$$\left(\frac{-7}{17}\right) \underset{\text{S1}}{=} \left(\frac{7}{17}\right) \underset{\text{R}}{=} \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) \underset{\text{R}}{=} -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

一方，オイラーの規準を使うとすれば，$(-7)^{\frac{17-1}{2}} = (-7)^8$ を計算すればよいが，$(-7)^2 = 49 \equiv -2 \pmod{17}$ より $(-7)^8 \equiv (-2)^4 = 16 \equiv -1 \pmod{17}$ なので，上と同じ結論を得る（もちろん！）．

*等号の下の R は相互法則を，S1, S2 はそれぞれ第 1，第 2 補充法則を適用したことを示す．

11.3　2次合同式

この節では，奇素数を法とする2次合同式の解が存在するかどうかの判定法について簡単に解説する． 次の定理の証明は，通常の2次方程式と同様，平方完成をすることで得られる（各自，証明してみ）.

定理 11.9　p を奇素数とし，a, b, c を整数，ただし $a \not\equiv 0 \pmod{p}$ とする． 合同式

$$ax^2 + bx + c \equiv 0 \pmod{p},$$

に対して，法 p に関する $b^2 - 4ac$ の平方剰余記号を δ とする; $\delta = \left(\dfrac{b^2 - 4ac}{p}\right)$ （分数じゃないよ，平方剰余記号だよ）． このとき，次が成り立つ.
(1)　$\delta = 0$ ならば，p を法としてただひとつの整数解をもつ.
(2)　$\delta = 1$ ならば，p を法として相異なる2つの整数解をもつ.
(3)　$\delta = -1$ ならば，整数解をもたない.

例 11.10　$2x^2 + 3x + 5 \equiv 0 \pmod{7}$ を解け.

解　判別式は $3^2 - 4 \cdot 2 \cdot 5 \equiv 4 \pmod{7}$ より，7 を法として相異なる2つの解をもつ． 解を求めるには，はじめに2次の係数 2 の逆元 4 をかけることで，

$$x^2 + 12x + 20 \equiv 0 \pmod{7}, \quad \text{簡単化して} \quad x^2 - 2x - 1 \equiv 0 \pmod{7},$$

1次の係数を絶対値の小さな偶数にするところがミソで，1/2 を出さずに平方完成できて

$$(x-1)^2 - 1 - 1 \equiv 0 \pmod{7}, \quad \text{すなわち} \quad (x-1)^2 \equiv 2 \pmod{7}$$

を得る． 最後に $3^2 \equiv 2 \pmod{7}$ より，解 $1 \pm 3 \equiv 4, -2 \equiv 4, 5 \pmod{7}$ が得られる.

例 11.11　$x^2 + x + 7 \equiv 0 \pmod{23}$ を解け.

解　判別式の平方剰余記号を計算すると，

$$\left(\frac{1 - 4 \cdot 7}{23}\right) = \left(\frac{-27}{23}\right) = \left(\frac{-4}{23}\right) = \left(\frac{-1}{23}\right) \underset{\text{S1}}{=} -1$$

なので解をもたない.

例 11.12　$p \equiv 5 \pmod{11}$ をみたす素数 p について，$x^2 + 3x + 5 \equiv 0 \pmod{p}$ が整数解をもつかどうか判定せよ.

解　p を法とする判別式の平方剰余を計算して，

$$\left(\frac{3^2 - 4 \cdot 5}{p}\right) = \left(\frac{-11}{p}\right) \underset{\Uparrow}{=} \left(\frac{p}{11}\right) = \left(\frac{5}{11}\right) \underset{\text{R}}{=} \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$$

より整数解をもつ． ここで，等号 $\Uparrow$ は，$p \equiv \pm 1 \pmod{4}$ で場合分けして，相互法則，第1補充法則を援用して確かめられる（ホントかよ！ すぐにはわかんねえよ……，自分の頭で考えなきゃな）.