第11章　平方剰余

11.1　平方剰余記号

第９章では，ある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． 以下，2 でない素数を奇素数と略す.

定義 11.1　p を奇素数とし，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.

たとえば，$1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 4,\ 4^2 \equiv 1 \pmod{5}$ 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． 同様に，7 を法とすると，$1, 2, 4$ が平方剰余，$3, 5, 6$ が平方非剰余となることがわかる.

補題 11.2 奇素数 p を法とする原始根 g は p を法として平方非剰余である.

証明　もし g が p を法として平方剰余ならば，$x^2 \equiv g \pmod{p}$ をみたす $x \in \boldsymbol{Z}$ が存在する． g は原始根なので $x \equiv g^k \pmod{p}$ となる整数 k がとれ，$g^{2k} \equiv x^2 \equiv g \pmod{p}$ より $g^{2k-1} \equiv 1 \pmod{p}$． よって命題 9.7(2) より $2k-1$ は g の位数 $p-1$ の倍数である．しかし $p-1$ は偶数なので矛盾である． □

定義 11.3 奇素数 p と整数 a に対して

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

と定める． これを p を法とする**平方剰余記号**という.

補題 11.4　p を奇素数とし，g を法 p に関する原始根とする． p と互いに素な整数 a に対して $a \equiv g^k \pmod{p}$ なる整数 k をとれば,

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

すなわち，a が p を法として平方剰余であることと k が偶数であることは同値である.

証明　k が偶数ならば明らかに a は平方剰余である．次に k が奇数であるとする．g の位数は $p-1$ なので，$g \equiv g^p \equiv ag^{p-k} \pmod{p}$．ここで $p-k$ は偶数だから，a が平方剰余だとすると g もそうであり，補題 11.2 に矛盾する．□

補題 11.5　p を奇素数とすると，$a, b \in \boldsymbol{Z}$ に対して次が成り立つ．

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

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

証明　(1) は明らか．(2) も前補題より直ちにわかる．□

定理 11.6 (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　$p \mid a$ のときは明らかなので，以下 $p \nmid a$ とする．まず，フェルマーの定理より $a^{\frac{p-1}{2}}$ は 2 次合同式 $x^2 \equiv 1 \pmod{p}$ の解であるが，この合同式は補題 9.12 より p を法として ± 1 以外の解をもたないので，$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$．とくに，法 p に関する原始根 g は位数 $p-1$ なので，$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ を得る．そこで，$a \equiv g^k \pmod{p}$ なる整数 k をとれば，補題 11.4 より

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

を得る．□

11.2　平方剰余の相互法則

整数 a が奇素数 p を法として平方剰余かどうかは，平方剰余記号を補題 11.5 やオイラーの規準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，p が非常に大きいときは膨大な計算が必要となる場合がある．次の定理は，法 p の平方剰余記号をより小さな法の計算に帰着する方法を与える．

定理 11.7 (平方剰余の相互法則)　相異なる奇素数 p, q に対して，

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

すなわち

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

証明は少し長くなるので「春休みの研究課題」とし，ここでは，定理がどのように使われるかを解説しよう． その前に，補充法則とよばれる補助的な公式を紹介する．

定理 11.8 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] $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & (p \equiv 1, 7 \pmod 8 \text{ のとき}), \\ -1 & (p \equiv 3, 5 \pmod 8 \text{ のとき}). \end{cases}$

第1補充法則はオイラーの規準から直ちに導かれる． 第2補充法則の証明は「春休みの研究課題」ってことでよろしく。

さて，$1 < a < p$ のとき，その素因数分解を $a = \prod_{j=1}^{r} q_j^{e_j}$ とすれば，補題 11.5 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ることで p より小さな法 q_j の計算に帰着される． 一例として，-7 が 17 を法として平方剰余かどうかを調べてみよう． $-7 \equiv 10 \pmod{17}$ より

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

あるいは，はじめに第1補充法則を使って

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

ここで，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し，他は補題 11.5 等を用いて変形している． 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！）．

このように，平方剰余の計算法は一通りではなく，工夫次第で簡単な方法を見つけることができるが，一般に，オイラーの規準を使うと扱う数が大きくなるので，相互法則を使う方が計算間違いも少なく結果的には効率がよいであろう．

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，および解が存在する場合は解の求め方について解説する．

まず，奇素数 p と互いに素な整数 a に対して，

$$\text{合同式 } x^2 \equiv a \pmod{p} \text{ の解が存在する} \iff \left(\frac{a}{p}\right) = 1$$

であることは，平方剰余記号の定義より明らかである． 一般の 2 次合同式についても，次の定理のように平方剰余記号を用いた判定法がある． 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（各自試みよ）．

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 $\varepsilon = \left(\dfrac{b^2 - 4ac}{p}\right)$ とおくとき，p を法とする解について次が成り立つ．

(1) $\varepsilon = 0$ ならば，ただひとつの解をもつ．
(2) $\varepsilon = 1$ ならば，相異なる 2 つの解をもつ．
(3) $\varepsilon = -1$ ならば，解をもたない．

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

解 1　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．解は通常の 2 次方程式と同じ形の公式により得られる． すなわち，$2 \cdot 2 = 4$ の法 7 に関する逆元 2 を用いて，解

$$\frac{-3 \pm 2}{2 \cdot 2} \equiv 2 \cdot (4 \pm 2) \equiv 2 \cdot 2,\ 2 \cdot 6 \equiv 4, 5 \pmod{7}$$

を得る．

解 2　はじめに 2 次の係数 2 の逆元 4 をかけることで，

$$x^2 + 12x + 20 \equiv 0 \pmod{7}, \quad \text{簡単化して} \quad x^2 - 2x + 6 \equiv 0 \pmod{7},$$

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

$$(x-1)^2 - 1 + 6 \equiv 0 \pmod{7}, \quad \text{すなわち} \quad (x-1)^2 \equiv 2 \pmod{7}$$

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　$x^2 + 3x + 5 \equiv 0 \pmod{11}$ を解け．

解　判別式は $3^2 - 4 \cdot 5 \equiv 0 \pmod{11}$ より，11 を法としてただひとつの解をもつ． また $x^2 + 3x + 5 \equiv x^2 - 8x + 5 \equiv (x-4)^2 \pmod{11}$ と変形して，解 4 が求まる．

例 11.12　$x^2 + x + 7 \equiv 0 \pmod{23}$ 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．