

第12章 平方剰余

12.1 平方剰余記号

第9章では自然数を法とする整数のべき乗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 12.1 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 12.2 $1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 4, 4^2 \equiv 1 \pmod{5}$ 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；

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

一般に、整数 a, b が $a \equiv b \pmod{p}$ をみたすならば $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ が成り立つことが、定義から直ちに確認できる。

補題 12.3 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. 逆に a が平方剰余であると仮定して k が偶数であることを示そう. a が平方剰余ならば, $x^2 \equiv a \pmod{p}$ をみたす $x \in \mathbf{Z}$ が存在する. g が原始根であることより $x \equiv g^l \pmod{p}$ となる整数 l がとれて,

$$g^{2l} \equiv x^2 \equiv a \equiv g^k \pmod{p}$$

より, $g^{2l-k} \equiv 1 \pmod{p}$. よって命題 10.2 (1) より $2l-k$ は g の位数 $p-1$ の倍数であるが, $p-1$ は偶数なので $2l-k$ は偶数, よって k も偶数でなければならない. \square

補題 12.4 奇素数 p と整数 a, b に対して, $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ が成り立つ.

証明 $p|a$ または $p|b$ とすると, 両辺とも 0 で成り立つ. $p \nmid a$ かつ $p \nmid b$ のときは, 法 p に関する原始根 g をとり, $a \equiv g^k, b \equiv g^l \pmod{p}$ とすると, 前補題より, 左辺 = $(-1)^k(-1)^l = (-1)^{k+l} =$ 右辺 となる. \square

奇素数 p と互いに素な整数 a に対してフェルマーの定理を適用すれば, $a^{\frac{p-1}{2}}$ は合同式 $x^2 \equiv 1 \pmod{p}$ の解となる. 一方, この二次合同式は補題 10.7 より p を法として ± 1 以外の解をもたないので, $a^{\frac{p-1}{2}}$ は p を法として 1 または -1 と合同となる. 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 12.5 (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. 上の注意から, 法 p に関する原始根 g に対して $g^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$ であるが, g は位数 $p-1$ なので, $g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ でなければならない. そこで, $a \equiv g^k \pmod{p}$ なる整数 k をとれば, 補題 12.3 より

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

を得る. \square

12.2 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 12.5) や定理 12.4 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 12.6 (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,

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

定理 12.7 (補充法則) 奇素数 p に対して次が成り立つ.

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

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

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 $a = q_1^{e_1} \dots q_r^{e_r}$ とすれば, 定理 12.4 (2) より,

$$\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right)^{e_1} \dots \left(\frac{q_r}{p}\right)^{e_r} = \prod_{e_j: \text{奇数}} \left(\frac{q_j}{p}\right).$$

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 12.8 17 を法とする -7 の平方剰余を調べてみる*.

$$\left(\frac{-7}{17}\right) = \left(\frac{10}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{5}{17}\right) \stackrel{S_2}{=} \left(\frac{5}{17}\right) \stackrel{R}{=} \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) \stackrel{S_2}{=} -1,$$

あるいは, はじめに第 1 補充法則を使って

$$\left(\frac{-7}{17}\right) \stackrel{S_1}{=} \left(\frac{7}{17}\right) \stackrel{R}{=} \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) \stackrel{R}{=} -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

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.

12.3 二次合同式

この節では、奇素数を法とする二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、通常の二次方程式と同様、平方完成をすることで得られる（各自、証明してみ）。

定理 12.9 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； $\delta = \left(\frac{b^2 - 4ac}{p}\right)$ （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 12.10 $2x^2 + 3x + 5 \equiv 0 \pmod{7}$ 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、はじめに二次の係数2の逆元4をかけることで、

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

一次の係数を絶対値の小さな偶数にするところがコツで、 $1/2$ を出さずに平方完成できて

$$(x-1)^2 - 1 + 6 \equiv 0 \pmod{7}, \quad \text{すなわち} \quad (x-1)^2 \equiv -5 \equiv 9 \pmod{7}$$

と変形して、解 $1 \pm 3 \equiv 4, -2 \equiv 4, 5 \pmod{7}$ が得られる。

例 12.11 $x^2 + x + 7 \equiv 0 \pmod{23}$ を解け。

解 判別式の平方剰余記号を計算すると、

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

なので解をもたない。

例 12.12 $p \equiv 5 \pmod{11}$ 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、

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

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）。