ルジャンドル記号と平方剰余の相互法則

北海道大学理学部数学科4年 岩瀬 優也

指導教員 前田 芳孝

奇素数pについて、次の二次合同方程式を考える。

$$ax^2+bx+c\equiv 0 \mod p.$$

このとき、

$$ax^2+bx+c\equiv a(x+(2a)^{-1}b)^2+(4ac-b^2)(4a)^{-1} \mod p$$

であるから、奇素数を法とするすべての二次合同方程式は次の式に帰着される。

$$x^2\equiv a \mod p.$$

平方剰余の相互法則を用いることで、この方程式が解をもつかどうか容易に判断することができる。

ルジャンドル記号の導入

奇素数pに対し、$(\mathbf{Z}/p\mathbf{Z})^\times$は位数$p-1$の巡回群である。mod pの原始根をrとし、写像λを次のように定める。

$$\lambda : r^n\in(\mathbf{Z}/p\mathbf{Z})^\times \longmapsto (-1)^n\in\{\pm1\}.$$

このλは全射準同型で、Ker$(\lambda)=<r^2>$である。

定義 $\left(\dfrac{b}{p}\right)$を次のように定義し、平方剰余記号（ルジャンドル記号）という。

$$\left(\frac{b}{p}\right)=\begin{cases}\lambda\ (\ b\ (\bmod p)) & \text{if } p\nmid b,\\ 0 & \text{if } p\mid b.\end{cases}$$

定理 次が成り立つ。

$$\left(\frac{bc}{p}\right)=\left(\frac{b}{p}\right)\left(\frac{c}{p}\right).$$

ルジャンドル記号の定義より、次のことが成り立つ。($\bar{b}=b \bmod p$とする。)

$$\left(\frac{b}{p}\right)=1 \iff \bar{b}\in<r^2> \iff x^2\equiv b \mod p \quad (x\in\mathbf{Z})\ \text{が解をもつ},$$
$$\left(\frac{b}{p}\right)=-1 \iff \bar{b}\notin<r^2> \iff x^2\equiv b \mod p \quad (x\in\mathbf{Z})\ \text{が解をもたない}.$$

よって、$\left(\dfrac{b}{p}\right)$は原始根の取り方によらないことがわかる。

$\left(\dfrac{b}{p}\right)=1$のとき b は平方剰余、$\left(\dfrac{b}{p}\right)=-1$のとき b は平方非剰余であるという。

定理 次が成り立つ。

(1)（オイラー基準） $\left(\dfrac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \bmod p.$

(2)（第一補充法則） $\left(\dfrac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}.$

証明 (1) $p\mid a$のときは明らか。以下、$p\nmid a$とする。rをmod pの原始根とし、$a\equiv r^m \bmod p$ とする。$r^{\frac{p-1}{2}}\equiv -1 \mod p$であるから、$\left(\dfrac{a}{p}\right)\equiv\left(\dfrac{r}{p}\right)^m\equiv(-1)^m$, $a^{\frac{p-1}{2}}\equiv r^{m\cdot\frac{p-1}{2}}\equiv(-1)^m$である。 したがって$\left(\dfrac{a}{p}\right)\equiv a^{\frac{p-1}{2}} \bmod p$が成り立つ。

(2) (1)で $a=-1$ とすると、$\left(\dfrac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}} \mod p$ である。この両辺はともに±1であり、$p\geq 3$ であることから等号が成り立つ。 □

定義 $2<N\in\mathbf{Z}$に対し、mod Nのディリクレ指標とは、準同型

$$\chi:(\mathbf{Z}/N\mathbf{Z})^\times\longrightarrow\mathbf{T}$$

のことである。 ($\mathbf{T}=\{z\in\mathbf{C}\mid \ \mid z\mid=1\}$) ここで、

$$\chi(c)=\begin{cases}\chi(\ c(\bmod N\mathbf{Z})\ ) & \text{if} \quad \gcd(c,N)=1,\\ 0 & \text{if} \quad \gcd(c,N)\neq 1.\end{cases}$$

と定め、χの定義域を整数全体に拡張する。

定義 mod Nのディリクレ指標χが原始的であるとは、以下を満たすことである。

(1)χが自明でない。($\exists a\in\mathbf{Z}$ s.t. $\chi(a)\neq 1$);

(2)Nの任意の真の約数sに対して、次を満たすディリクレ指標ξが存在しない:

(i) ξはmod sのディリクレ指標である.

(ii)$\gcd(c,N)=1$となる任意のcに対して、$\chi(c)=\xi(c)$が成り立つ.

定義 $\zeta=\exp\left(\dfrac{2\pi i}{N}\right)$と定め、mod Nの原始的ディリクレ指標χに対して、次の和をガウス和という:

$$\tau(\chi)=\sum_{a=1}^{N}\chi(a)\zeta^a.$$

定理 次が成り立つ。($\overline{\chi}$はχの複素共軛)

(1) $\displaystyle\sum_{a=1}^{N}\chi(a)\zeta^{ab}=\overline{\chi}(b)\tau(\chi).$

(2) $\overline{\tau(\chi)}\tau(\overline{\chi})=\chi(-1)N.$

(3) $\overline{\tau(\chi)}=\chi(-1)\tau(\overline{\chi}).$

(4) $\mid\tau(\chi)\mid^2=N.$

補題 $\zeta=\exp\left(\dfrac{2\pi i}{N}\right)$ $(2<N\in\mathbf{Z}), R=\mathbf{Z}[\zeta]$ とおくと、$pR\bigcap\mathbf{Z}=p\mathbf{Z}$ である。

証明 $pR\bigcap\mathbf{Z}$ はpを含む$\mathbf{Z}$のイデアルであり、$p\mathbf{Z}\subset pR\bigcap\mathbf{Z}\subset\mathbf{Z}$であるから、$pR\bigcap\mathbf{Z}$は$p\mathbf{Z}$または$\mathbf{Z}$である。もし$pR\bigcap\mathbf{Z}=\mathbf{Z}$であると仮定すると、$p^{-1}\in R$であり、$\displaystyle\bigcup_{n=1}^{\infty}\sum_{i=1}^{n}\mathbf{Z}p^{-i}$は$R$の部分環となるので$\mathbf{Z}$上有限生成でなければならないが、これは矛盾である。したがって、$pR\bigcap\mathbf{Z}=p\mathbf{Z}$である。□

相互法則

定理（一般相互法則） χをmod Nの原始的ディリクレ指標、$\overline{\chi}=\chi$とする。このとき、次が成り立つ。

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

(ただし、pは$\gcd(p,N)=1$であるような奇素数。)

証明 $\tau=\tau(\chi),\zeta=\exp\left(\frac{2\pi i}{N}\right)\zeta, R=\mathbf{Z}[\zeta]$とおく。

まず、$\tau^2=\chi(-1)N$ だから $\tau^p=(\tau^2)^{\frac{p-1}{2}}=\chi(-1)^{\frac{p-1}{2}}N^{\frac{p-1}{2}}\tau$である。

次に、$\tau=\displaystyle\sum_{a=1}^{N}\chi(a)\zeta^a$ より $\tau^p=\left(\displaystyle\sum_{a=1}^{N}\chi(a)\zeta^a\right)^p\equiv\displaystyle\sum_{a=1}^{N}\chi(a)\zeta^{ap}\equiv\chi(p)\tau \mod pR$ である。よって、オイラー基準および $\tau\overline{\tau}=N$ より

$$\chi(p)N\equiv\chi(-1)^{\frac{p-1}{2}}\left(\frac{N}{p}\right)N \mod pR$$

が成り立つ。補題より上の合同式は mod $p\mathbf{Z}$ でも成り立ち、$\gcd(p,N)=1$ と $\chi(p),\left(\dfrac{N}{p}\right)=\pm1$より等号が成り立つ。□

定理（第二補充法則） 次が成り立つ。

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

証明 χ_1 を次のように定める:

$$\chi_1:a\in(\mathbf{Z}/8\mathbf{Z})^\times\longmapsto(-1)^{\frac{a^2-1}{8}}\in\{\pm1\}.$$

このとき χ_1 は mod 8 の原始的ディリクレ指標であり、$\chi_1(-1)=1$ である。したがって、一般相互法則より任意の奇素数pに対して $\left(\dfrac{2}{p}\right)=\left(\dfrac{8}{p}\right)=\chi_1(p)$ が成り立つ。□

定理 （平方剰余の相互法則） p,qを相異なる奇素数とすると、次が成り立つ:

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

証明 $\chi(x)=\left(\dfrac{x}{q}\right)$とおくと、$\chi(x)$はmod qの原始的ディリクレ指標であり、$\overline{\chi}=\chi$である。したがって、一般相互法則より

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

である。よって、第一補充法則より

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

である。ゆえに$\left(\dfrac{q}{p}\right)\left(\dfrac{p}{q}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$が成り立つ。 □

計算への応用

$\left(\dfrac{5}{47}\right)$の値を求める。まず、平方剰余の相互法則より$\left(\dfrac{5}{47}\right)\left(\dfrac{47}{5}\right)=(-1)^{\frac{5-1}{2}\frac{47-1}{2}}=1$であるから、$\left(\dfrac{5}{47}\right)=\left(\dfrac{47}{5}\right)$である。ここで$\left(\dfrac{47}{5}\right)=\left(\dfrac{2}{5}\right)$であり、

$$1^2\equiv 4^2\equiv 1,\quad 2^2\equiv 3^2\equiv 4 \mod 5$$

であるから、$x^2\equiv 2 \mod 5$ となる$x\in\mathbf{Z}$は存在しない。

したがって$\left(\dfrac{2}{5}\right)=-1$である。ゆえに$\left(\dfrac{5}{47}\right)=-1$である。

参考文献

[1] Goro Shimura, "Arithmetic of Quadratic Forms", Springer