『数学セミナー』2020年1月号 「高校数学ではじめる整数論」

連載●第 10 回

ルジャンドル記号　付録

谷口 隆◎神戸大学大学院理学研究科

※ 式番号は本誌 2020 年 1 月号の連載と通しで振っています.

◎——1　命題 3 と命題 4 の別証明

数学の専門的な学習が一定程度進むと，どの命題がどの命題に立脚しているか，という論理の関係が気になるようになってきます．1 月号本誌では，原始根の存在定理を用いて，命題 3 と命題 4 を平易に証明しました．ただし，6 月号の付録で紹介したように，原始根の存在定理の証明自体はあまり簡単ではありません．

ここでは参考のため，原始根の存在定理には依拠しない，命題 3 と命題 4 の証明を紹介します．まず命題 4 を証明し，それを用いて命題 3 を証明します．原始根の存在定理に基づく本誌の証明で問題はないのですが，論理の関係が気になる人は，証明を比較するなど，いろいろ考えてみると面白いと思います．(一方で，ルジャンドル記号の特徴づけを与える命題 7 については，原始根の存在定理に基づく本誌の証明が簡明だと思われます．)　ここの証明では，副産物として，ウィルソンの定理とフェルマーの小定理も得られるので，これも面白いでしょう．

本誌同様，p は常に奇素数を表します．次の二つの補題は単純な事実ですが，証明で基本的な役割を持つので，はっきりと述べておきます．

補題 8　$a, b \in \mathbb{F}_p$ について，$a^2 = b^2$ であれば，$a = b$ または $a = -b$ である．　□

証明　一般に，$u, v \in \mathbb{F}_p$ について，$uv = 0$ ならば $u = 0$ または $v = 0$ である．実際，$u \neq 0$ ならば，$u^{-1} \in \mathbb{F}_p$ が存在するから，$uv = 0$ の両辺に u^{-1} をかけて，$v = 0$ を得る．

$a^2 = b^2$ より，$0 = a^2 - b^2 = (a - b)(a + b)$ である．よって $a - b = 0$ または $a + b = 0$ である．　■

補題 9　$a \in \mathbb{F}_p$ について，$a = -a$ ならば $a = 0$ である．特に，$a \in \mathbb{F}_p^\times$ ならば，$a \neq -a$ である．　□

証明　$a=-a$ より $2a=0$ である．p は奇素数だから，2 は p の倍数でない．つまり $\mathbb{F}_p$ の元として，$2\neq 0$ である．$2^{-1}\in\mathbb{F}_p$ をかけて，$a=0$ を得る．■

ではまず，命題 4 の証明から．

命題 4 の証明　a を $\mathbb{F}_p^\times$ の元と考える．各 $b\in\mathbb{F}_p^\times$ に対して，$bc=a$ となる $c\in\mathbb{F}_p^\times$ を b の配偶と呼ぶことにする．$c=b^{-1}a$ だから b の配偶 c は $\mathbb{F}_p^\times$ の中で一意に定まり，また b の配偶が c ならば，c の配偶は b である．

b の配偶が b 自身になるのは，$b^2=a$ のときである．$\left(\dfrac{a}{p}\right)=-1$ のときは，このような b は存在しない．したがって $\mathbb{F}_p^\times$ の元 $1,2,\cdots,p-1$ は，2 つずつ互いに配偶となり，その組が $\dfrac{p-1}{2}$ 組になる．そのすべての積を考えて，$(p-1)!=a^{\frac{p-1}{2}}$ である．

$\left(\dfrac{a}{p}\right)=1$ のときは，このような b が存在する．b を $n^2=a$ の一つの解とすると，$a=b^2$ なので，$n^2=a$ の解は補題 8 より $n=b,-b$ である．$b\neq 0$ より，補題 9 から $b\neq -b$ である．$\mathbb{F}_p^\times$ の元のうち，配偶が自分自身となるのは b と $-b$ で，残りの $p-3$ 個は二つずつ互いに配偶となる．よってその $p-3$ 個の積は $a^{\frac{p-3}{2}}$ である．また $b\cdot(-b)=-b^2=-a$ である．よって $(p-1)!=-a^{\frac{p-1}{2}}$ である．

ここでいったん $a=1$ の場合を考える．すると，$\left(\dfrac{a}{p}\right)=1$ だから，$(p-1)!=-a^{\frac{p-1}{2}}=-1$ が得られる．したがって一般の a では，

$$\left(\frac{a}{p}\right)=1 \text{ のとき } a^{\frac{p-1}{2}}=1,\qquad \left(\frac{a}{p}\right)=-1 \text{ のとき } a^{\frac{p-1}{2}}=-1$$

である．これで命題 4 が示された．■

$\mathbb{F}_p$ 上で $(p-1)!=-1$ であることから，ウィルソンの定理が示されています．また，$a\in\mathbb{F}_p^\times$ について $a^{\frac{p-1}{2}}=\pm 1$ だから，$a^{p-1}=(a^{\frac{p-1}{2}})^2=1$ で，これはフェルマーの小定理です．

次に命題 3 の証明です．命題 4 を使うとすぐに示せます．

命題 3 の証明　命題 4 より，法 p の合同式の計算で

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

である．よって $\left(\dfrac{ab}{p}\right)$ と $\left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$ の差は p の倍数である．

$\left(\dfrac{ab}{p}\right)$ と $\left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$ はいずれも $1,-1$ のいずれかである．よってその差は $0,2,-2$ のいずれかだが，この中で p の倍数は 0 のみである．つまり $\left(\dfrac{ab}{p}\right)$ と $\left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)$ は一致する．■

なお，本誌では原始根を使って示した命題 6 も，直接簡単に証明できます．

命題 6 の証明　$\left(\dfrac{a}{p}\right)=1$ であるとは，a が

$$1^2,2^2,3^2,\cdots,(p-2)^2,(p-1)^2 \tag{10}$$

のいずれかであるということである．(10) のうちの相異なるものの個数を求める．$(p-1)^2=1^2,(p-2)^2=2^2,\cdots$ であり，逆に補題 8 より，$a^2=b^2$ であるのは $a=b$ または $a=-b$ に限るから，(10) のうち $1^2,2^2,\cdots,\left(\dfrac{p-1}{2}\right)^2$ はすべて異なる．したがって，$\left(\dfrac{a}{p}\right)=1$ となる a はこれら $\dfrac{p-1}{2}$ 個である．よって $\left(\dfrac{a}{p}\right)=-1$ となる a は，$p-1$ からこれらを引いて，やはり $\dfrac{p-1}{2}$ 個である．　■

◎——2　四平方定理

ここではルジャンドル記号を使って，次を証明します．(ルジャンドル記号が決定的に重要な役割を持つとまでは言えないのですが，命題 13 の証明でルジャンドル記号を活用します．)

定理 10　任意の正の整数 n は，4 個の平方数の和で表される．(ただし平方数は 0 を含む．)　□

証明には，オイラーによって発見された，次の見事な恒等式を使います．

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)&\\ =(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2&\\ +(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2&\\ +(x_1y_3-x_2y_4-x_3y_1+x_4y_2)^2&\\ +(x_1y_4+x_2y_3-x_3y_2-x_4y_1)^2&\end{aligned} \tag{11}$$

この恒等式は，両辺を展開して直接確かめても構いませんが，複素数 $\alpha,\beta,\gamma,\delta$ についての恒等式

$$(\alpha\overline{\alpha}+\beta\overline{\beta})(\gamma\overline{\gamma}+\delta\overline{\delta})=(\alpha\overline{\gamma}+\beta\overline{\delta})(\overline{\alpha}\gamma+\overline{\beta}\delta)+(\alpha\delta-\beta\gamma)(\overline{\alpha}\overline{\delta}-\overline{\beta}\overline{\gamma}) \tag{12}$$

で，$\alpha=x_1+x_2i,\beta=x_3+x_4i,\gamma=y_1+y_2i,\delta=y_3+y_4i$ とおいても得られます．(12) は展開すればすぐに確かめられます．余談ながらこれは，

$$\begin{pmatrix}\alpha & \beta\\ -\overline{\beta} & \overline{\alpha}\end{pmatrix}\begin{pmatrix}\overline{\gamma} & -\delta\\ \overline{\delta} & \gamma\end{pmatrix}=\begin{pmatrix}\alpha\overline{\gamma}+\beta\overline{\delta} & -(\alpha\delta-\beta\gamma)\\ \overline{\alpha}\overline{\delta}-\overline{\beta}\overline{\gamma} & \overline{\alpha}\gamma+\overline{\beta}\delta\end{pmatrix}$$

の両辺の行列式を考えていると見ることもできます．

定理 10 について考えましょう．(11) によると，正の整数 m,n が共に 4 つの平方数の和で書ければ，積 mn もそのように書けることになります．これを繰り返せば，n の素因数分解を考え，n の素因子がすべて 4 つの平方数の和で書ければ十分です．つまり，n が素数の場合に証明できれば十分です．$n=2$ の場合は明らかなので，次が示せればよいことになります．

命題 11　任意の奇素数 p は，4 個の平方数の和で表される．　□

10 月号付録で紹介した「降下法」によって，この命題を証明します．並行した議論が多いので，比較してみると面白いと思います．以下再び，p は必ず奇素数を表すものとします．

命題 12　m を $1 < m < p$ である整数とし，mp が 4 個の平方数の和で表されるとする．このとき，$1 \leqq r < m$ である整数 r で，rp が 4 個の平方数の和で表されるようなものが存在する．　□

証明　$x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp$ とする．各 $i = 1, 2, 3, 4$ について，

$$x_i \equiv y_i \pmod{m}, \qquad -\frac{m}{2} < y_i \leqq \frac{m}{2}$$

となる整数 y_i を取る．

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m}$$

だから，$y_1^2 + y_2^2 + y_3^2 + y_4^2 = mr$ と書ける．

$$\begin{aligned} z_1 &:= x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4, \\ z_2 &:= x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3, \\ z_3 &:= x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2, \\ z_4 &:= x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1 \end{aligned}$$

とおくと，(11) より $z_1^2 + z_2^2 + z_3^2 + z_4^2 = m^2rp$ である．さらに，$y_i \equiv x_i \pmod{m}$ から

$$\begin{aligned} z_1 &\equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m}, \\ z_2 &\equiv x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3 \equiv 0 \pmod{m} \end{aligned}$$

であり，同様に $z_3 \equiv 0 \pmod{m}$, $z_4 \equiv 0 \pmod{m}$ である．したがって，$w_i := \dfrac{z_i}{m}$ $(1 \leqq i \leqq 4)$ とおくと w_i は整数で，$w_1^2 + w_2^2 + w_3^2 + w_4^2 = rp$ である．以下，$1 \leqq r < m$ であることを示して証明を完了する．

$r = 0$ であるとすると，$y_1 = y_2 = y_3 = y_4 = 0$ だから，x_i はすべて m の倍数である．$x_i = mt_i$ とすると，$m(t_1^2 + t_2^2 + t_3^2 + t_4^2) = p$ となって，p が $1 < m < p$ となる約数を持つことになり，素数であることに反する．したがって $r \geqq 1$ である．

$$mr = y_1^2 + y_2^2 + y_3^2 + y_4^2 \leqq 4 \cdot \left(\frac{m}{2}\right)^2 = m^2$$

だから $r \leqq m$ である．$r = m$ だとすると，上で等号が成立することから，$y_1 = y_2 = y_3 = y_4 = \dfrac{m}{2}$ である．よって m は偶数であり，また $x_i \equiv y_i \pmod{m}$ により x_i はすべて $\dfrac{m}{2}$ の奇数倍である．$x_i = (2k_i + 1)\dfrac{m}{2}$ とおき，$x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp$ に代入して整理すると，

$$m \cdot \sum_{i=1}^{4} (2k_i + 1)^2 = 4p$$

となる．左辺の和の部分は 4 の倍数だから，これに m を乗じた左辺は 8 の倍数である．よって p が偶数となって奇素数であることに反する．　■

命題 12 の条件をみたすような m を探しましょう．そのために，次の命題を示します．この命題には証明を二つ挙げます．一つ目の証明はルジャンドル記号を活用した証明です．二つ目の証明では，ルジャンドル記号は重要ではありません．

命題 13　$x_1^2+x_2^2+1\equiv 0 \pmod p$ となる整数 x_1, x_2 が存在する．　□

証明 1　$\left(\dfrac{-1}{p}\right)=1$ のときは，$x_1^2+1\equiv 0 \pmod p$ となる整数 x_1 が存在する．この場合は $x_2=0$ と取ればよい．$\left(\dfrac{-1}{p}\right)=-1$ とする．このとき，数列 $\left(\dfrac{1}{p}\right), \left(\dfrac{2}{p}\right), \cdots, \left(\dfrac{p-1}{p}\right)$ は，$\left(\dfrac{1}{p}\right)=1$ で始まり，$\left(\dfrac{p-1}{p}\right)=\left(\dfrac{-1}{p}\right)=-1$ で終わるので，$\left(\dfrac{k}{p}\right)=1$ かつ $\left(\dfrac{k+1}{p}\right)=-1$ となる $1\leqq k\leqq p-2$ が存在する．$\left(\dfrac{-k-1}{p}\right)=\left(\dfrac{-1}{p}\right)\left(\dfrac{k+1}{p}\right)=(-1)\cdot(-1)=1$ である．したがって，$x_1^2\equiv k \pmod p$, $x_2^2\equiv -1-k \pmod p$ となる整数 x_1, x_2 を取ることができ，$x_1^2+x_2^2+1\equiv 0 \pmod p$ である．　■

証明 2　$\mathbb{F}_p$ の中で，$a^2+b^2+1=0$ となる $a, b\in\mathbb{F}_p$ を見つければよい．$\mathbb{F}_p$ の部分集合 $\{a^2 \mid a\in\mathbb{F}_p^\times\}$ は，命題 6 により，$\dfrac{p-1}{2}$ 個の元からなる．したがって $a=0$ を含めた集合 $A=\{a^2 \mid a\in\mathbb{F}_p\}$ は，0 を加えた $\dfrac{p+1}{2}$ 個の元からなる．したがって，$B=\{1-b^2 \mid b\in\mathbb{F}_p\}$ とおくと，B もまた $\dfrac{p+1}{2}$ 個の元からなる．

$\mathbb{F}_p$ は p 個の元からなるので，$\mathbb{F}_p$ の部分集合 A, B の元の数の和が $p+1$ 個であることから，$A\cap B\neq\emptyset$ である．つまり，$a^2=1-b^2$ となる $a, b\in\mathbb{F}_p$ が存在する．　■

以上の準備で,「降下法」によって命題 11 を示すのは容易です．命題 13 の整数 x_1, x_2 を取ります．この命題では，x_i を法 p で合同な整数で置き換えても構わないので，$|x_i|<\dfrac{p}{2}$ とできます．$x_1^2+x_2^2+1=mp$ とおくと，$x_1^2+x_2^2+1<\dfrac{p^2}{2}+1<p^2$ であることから，$1\leqq m<p$ です．$m=1$ なら既に命題 11 が示されていますが，$m>1$ の場合は，命題 12 によって，m をより小さな正の整数に置き換えることを 1 になるまで繰り返します．

[たにぐち たかし]
[絵／森脇かみん]