入試の良問と平方剰余の相互法則

宮川（みやかわ）　幸隆（ゆきたか）

'96年の有名大学の数学の良問としては，京都大学の後期理系の1番の問題が私好みの問題でした．

まず問題を再録します：

> n は自然数とする．
> (1) すべての実数 θ に対し
> $$\cos n\theta = f_n(\cos\theta),$$
> $$\sin n\theta = g_n(\cos\theta)\sin\theta$$
> を満たし，係数がともにすべて整数である n 次式 $f_n(x)$ と $n-1$ 次式 $g_n(x)$ が存在することを示せ．
> (2) $f_n'(x)=ng_n(x)$ であることを示せ．
> (3) p を3以上の素数とするとき，$f_p(x)$ の $p-1$ 次以下の係数はすべて p で割り切れることを示せ．
> [京都大・理系・後期]

ド・モアブルの定理から，

$$\cos n\theta + i\sin n\theta = (\cos\theta + i\sin\theta)^n$$
$$= {}_nC_0\cos^n\theta + i\,{}_nC_1\cos^{n-1}\theta\sin\theta + i^2\,{}_nC_2\cos^{n-2}\theta\sin^2\theta + i^3\,{}_nC_3\cos^{n-3}\theta\sin^3\theta + \cdots\cdots + i^{n-1}\,{}_nC_{n-1}\cos\theta\sin^{n-1}\theta + i^n\,{}_nC_n\sin^n\theta$$

であるから，n が奇数のときは

$$\cos n\theta = {}_nC_0(1-\sin^2\theta)^{\frac{n-1}{2}}\cos\theta - {}_nC_2(1-\sin^2\theta)^{\frac{n-3}{2}}\sin^2\theta\cos\theta + \cdots\cdots + (-1)^{\frac{n-1}{2}}\,{}_nC_{n-1}(\sin^2\theta)^{\frac{n-1}{2}}\cos\theta$$
$$= \{(-1)^{\frac{n-1}{2}}({}_nC_0 + {}_nC_2 + \cdots\cdots + {}_nC_{n-1})\sin^{n-1}\theta + A\sin^{n-3}\theta + \cdots\cdots\}\cos\theta,$$

$$\sin n\theta = {}_nC_1(1-\sin^2\theta)^{\frac{n-1}{2}}\sin\theta - {}_nC_3(1-\sin^2\theta)^{\frac{n-3}{2}}\sin^3\theta + \cdots\cdots + (-1)^{\frac{n-1}{2}}\,{}_nC_n\sin^n\theta$$
$$= (-1)^{\frac{n-1}{2}}({}_nC_1 + {}_nC_3 + \cdots\cdots + {}_nC_n)\sin^n\theta + B\sin^{n-2}\theta + \cdots\cdots$$

となることにより，上の京都大の問題を多少修正して得られる次の問題を考えます．

> nは奇数の自然数とする．
> (i) すべての実数 θ に対し
> $$\sin n\theta = P_n(\sin\theta),$$
> $$\cos n\theta = Q_n(\sin\theta)\cos\theta$$
> を満たし，係数がともにすべて整数である n 次式 $P_n(x)$ と $n-1$ 次式 $Q_n(x)$ が存在することを示せ．
> (ii) $P_n'(x)=nQ_n(x)$ であることを示せ．
> (iii) pを3以上の素数とするとき，$P_p(x)$ の $p-1$ 次以下の係数はすべて p で割り切れることを示せ．

さて，上の考察により(i)は既に示されています．そこでまず，(ii)，(iii)を示してみましょう：

(ii) $\sin n\theta = P_n(\sin\theta)$ の両辺を θ で微分すると，

$$n\cos n\theta = P_n'(\sin\theta)\cos\theta$$
$$\therefore\ nQ_n(\sin\theta)\cos\theta = P_n'(\sin\theta)\cos\theta \quad \cdots\cdots ①$$

これが任意の θ に対して成り立つから，①の両辺を $\cos\theta$ で割って $\sin\theta = x$ とおいた $nQ_n(x)=P_n'(x)$ も成り立つ．

(iii) (ii)により，$P_p'(x)=pQ_p(x)$ であり，一方，(i)により $Q_p(x)$ の係数は整数であるから，$P_p'(x)$ の係数は p の倍数である．そこで，

$$P_p'(x) = pa_px^{p-1} + pa_{p-1}x^{p-2} + \cdots\cdots + pa_1$$
$$(a_p,\ a_{p-1},\ \cdots\cdots,\ a_1 \text{は整数})$$

とおく．このとき，

$$P_p(x) = a_px^p + \frac{pa_{p-1}}{p-1}x^{p-1} + \cdots\cdots + pa_1x + a_0$$

これの x^i $(i=1,2,\cdots\cdots,\ p-1)$ の係数 $\frac{pa_i}{i}$ … ②

は整数であるが，p は素数なので p と i とは互いに素となり，$\frac{a_i}{i}$ は整数であるから②は p の倍数である．また，$a_0=P_p(0)=P_p(\sin 0)=\sin p0=0$ により，a_0 も p の倍数となって題意は示された．

以上の考察と同様にして，京都大の問題も証明されます．

さて，以下においては(iii)を用いて平方剰余の相

互法則を証明してみます．そのために，まず，いくつかの準備をします．

実は筆者は，「数研通信・数学No.21」で，ある意味で上の京都大の問題の類題である，'90年の東京工大後期の三角関数に関する問題の背景を探りました．そこでの議論を以下の平方剰余の相互法則の証明に際しても用いることになるのですが，「数研通信・数学No.21」をお持ちでない方もいらっしゃるでしょうから，ここでは，その概略を簡潔にまとめてみたいと思います(後で用いる結果のみを証明なしで述べる場合もあります)．

§0．複素関数としてのsin

オイラーの公式

(1) $e^{iy}=\cos y+i\sin y$ (y：実数)

によれば

(2) $e^{-iy}=\cos y-i\sin y$

であるから，(1)と(2)から，

(3) $\sin y=\dfrac{e^{iy}-e^{-iy}}{2i}$

である．

ここでyは実数であるが，(3)においてyを任意の複素数として，sin を複素変数にまで拡張する．

すなわち，$\sin z=\dfrac{e^{iz}-e^{-iz}}{2i}$で，$z$は複素変数とする．

すると，自然数 n に対し

$$\frac{\sin nz}{\sin z}=\frac{e^{niz}-e^{-niz}}{e^{iz}-e^{-iz}}$$

であるが

$$\frac{x^n-y^n}{x-y}=x^{n-1}+x^{n-2}y+\cdots\cdots+xy^{n-2}+y^{n-1}$$

を用いて，

$$\frac{\sin nz}{\sin z}$$
$$=e^{(n-1)iz}+e^{(n-2)iz}e^{-iz}+\cdots\cdots+e^{-(n-1)iz}$$
$$=e^{(n-1)iz}+e^{(n-3)iz}+\cdots\cdots+e^{-(n-1)iz}$$

ここに $\sin z\neq 0$，すなわち，

任意の整数 m に対して $z\neq m\pi$

となる．そこで，

$$F_n(z)=e^{(n-1)iz}+e^{(n-3)iz}+\cdots\cdots+e^{-(n-1)iz}$$

とおくと，

$$\frac{d}{dz}e^z=e^z$$

により，$F_n(z)$は全複素平面において微分可能である．

§1．正則周期関数 $F_n(z)$ の性質

前節の最後でみたように，$F_n(z)$ は全複素平面において微分可能(正則)である．しかも 2π を基本周期とする周期関数でもある．これらの事実により $F_n(z)$ は $w=w(z)=\sin^2 z$ の関数とみなすことができる．そして，その関数を $G_n(w)$ としたとき，

すなわち

$$F_n(z)=G_n(w)$$

としたとき，$G_n(w)$はwの関数として全w平面において微分可能である[詳しくは「数研通信・数学No.21」参照]．

§2．Liouvilleの定理

Liouvilleの定理

全複素平面Cにおいて微分可能な関数 $F(z)$ に対して，

$$M(r)=\max_{|z|=r}|F(z)|$$

とおくとき，$M>0$ および $K\geqq 0$ なる定数 M,K に対して，

$$M(r_n)\leqq Mr_n{}^K \text{ かつ } \lim_{n\to\infty} r_n=\infty$$

なる数列 $\{r_n\}$ が存在するならば，$F(z)$ は高々 $[K]$ 次の(zの)多項式である．ここに $[K]$ は K を越えない最大の整数である．

以前と同様，本稿でも，この定理を証明しませんが，自由に用いることにします．

§3．(iii)を用いた平方剰余相互法則の証明

補助定理

mを3以上の奇数とすると次の等式が成り立つ：

$$\frac{\sin mz}{\sin z}=(-4)^{\frac{m-1}{2}}\prod_{j=1}^{\frac{m-1}{2}}\left(\sin^2 z-\sin^2\frac{2j\pi}{m}\right)$$

証明　$F_m(z)=G_m(w)$，$w=\sin^2 z$で，$G_m(w)$は全w平面において微分可能であった(§1)．

$$\max_{|w|=r}|G_m(w)|=\max_{|\sin^2 z|=r}|F_m(z)|$$
$$=\max_{e^{-2y}+e^{2y}-2\cos 2x=4r}\left|e^{(m-1)i(x+iy)}+\cdots+e^{2(1-m)i(x+iy)}\right|$$
$$\leqq\max_{e^{-2y}+e^{2y}-2\cos 2x=4r}\left\{e^{(1-m)y}+\cdots+e^{(m-1)y}\right\}$$
$$<\max_{e^{-2y}+e^{2y}-2\cos 2x+4r}(m-1)\left\{(e^{-2y})^{\frac{m-1}{2}}+(e^{2y})^{\frac{m-1}{2}}\right\}$$
$$\leqq(m-1)(4r+2)^{\frac{m-1}{2}}$$

であるから，

$$M(r)=\max_{|w|=r}|G_m(w)|$$

とおくとき，

$$M(r)<(m-1)\left(4+\frac{2}{r}\right)^{\frac{m-1}{2}}r^{\frac{m-1}{2}}$$

であって，$r_n=n$ とおくと，

$$M(r_n)<(m-1)\left(4+\frac{2}{n}\right)^{\frac{m-1}{2}}r_n^{\frac{m-1}{2}}\leqq(m-1)6^{\frac{m-1}{2}}r_n^{\frac{m-1}{2}}$$

かつ $\lim_{n\to\infty}r_n=\infty$

となるから，liouville の定理により，$G_m(w)$ は高々 $\frac{m-1}{2}$ 次の($w=\sin^2z$の)多項式である．

さて，$j=1,2,\cdots\cdots,\frac{m-1}{2}$ に対して，

$$0<\frac{2j\pi}{m}<\pi,\ \text{かつ},\ F_m\left(\frac{2j\pi}{m}\right)=\frac{\sin 2j\pi}{\sin\frac{2j\pi}{m}}=0$$

であるから

$$G_m\left(\sin^2\frac{2j\pi}{m}\right)=0,\left(j=1,2,\cdots\cdots,\frac{m-1}{2}\right)$$

であり，w の $\frac{m-1}{2}$ 次以下の代数方程式 $G_m(w)=0$ が $\frac{m-1}{2}$ 個の解をもつから，$G_m(w)$ は w の $\frac{m-1}{2}$ 次の多項式であって，Cを定数($\neq0$)として，

$$G_m(\sin^2z)=C\prod_{j=1}^{\frac{m-1}{2}}\left(\sin^2z-\sin^2\frac{2j\pi}{m}\right)$$

となる．そして，$z\neq n\pi$ (nは整数)なるすべての複素数zに対して，

$$\frac{\sin mz}{\sin z}=F_m(z)=G_m(\sin^2z)$$

が成り立ち，前々頁の左段の考察により，

$$C=(-1)^{\frac{m-1}{2}}({}_mC_1+{}_mC_3+\cdots+{}_mC_m)=(-4)^{\frac{m-1}{2}}$$

である．　(証明終)

さて，以下pを3以上の素数とする．微分方程式

(4) $$\frac{dy}{\sqrt{1-y^2}}=p\frac{dx}{\sqrt{1-x^2}}$$

の代数的積分(=y が x の代数的な式で表されるような解)のうち，「$x=0$ のとき $y=0$」という初期条件を満たすものを求めよう：

$$\int_0^y\frac{dy}{\sqrt{1-y^2}}=p\int_0^x\frac{dx}{\sqrt{1-x^2}}$$

により，$\theta=\int_0^x\frac{dx}{\sqrt{1-x^2}}$，*i.e.* $x=\sin\theta$とおくと $y=\sin p\theta$ であるから，

$$\begin{aligned}\sin p\theta&=(-4)^{\frac{p-1}{2}}\sin^p\theta\\&\quad+A_{\frac{p-3}{2}}\sin^{p-2}\theta+\cdots\cdots+A_0\sin\theta\\&=(-4)^{\frac{p-1}{2}}\sin\theta\prod_{j=1}^{\frac{p-1}{2}}\left(\sin^2\theta-\sin^2\frac{2j\pi}{p}\right)\end{aligned}$$

[∵前々頁の左段の考察と補助定理による]により，

(5) $$y=x\left\{(-4)^{\frac{p-1}{2}}(x^2)^{\frac{p-1}{2}}+A_{\frac{p-3}{2}}(x^2)^{\frac{p-3}{2}}\right.$$
$$\left.+\cdots\cdots+A_2(x^2)^2+A_1(x^2)+A_0\right\}=P_p(x),$$

(各A_jは整数)

という(4)の代数的積分が求まる．$K=x^2$ とおいて

K の $\frac{p-1}{2}$ 次方程式

(6) $$(-4)^{\frac{p-1}{2}}K^{\frac{p-1}{2}}+A_{\frac{p-3}{2}}K^{\frac{p-3}{2}}$$
$$+\cdots\cdots+A_2K^2+A_1K+A_0=0$$

を考える．p を法とする既約剰余系は

$$r_1,\ r_2,\ r_3,\ \cdots\cdots,\ r_{\frac{p-1}{2}},$$
$$-r_1,\ -r_2,\ -r_3,\ \cdots\cdots,\ -r_{\frac{p-1}{2}}$$

のように表される($r_j=j,j=1,2,\cdots\cdots,\frac{p-1}{2}$と考えて良い)が，方程式(6)の $\frac{p-1}{2}$ 個の根は

$$\sin^2\left(\frac{r_j\cdot2\pi}{p}\right)\ \left(j=1,2,3,\cdots\cdots,\frac{p-1}{2}\right)$$

である．方程式(6)を関数 sin の周期 p 等分方程式と呼ぶ．(5)から

$$\frac{dy}{dx}=(-4)^{\frac{p-1}{2}}x^{p-1}+A_{\frac{p-3}{2}}x^{p-3}+\cdots\cdots+A_1x^2+A_0$$
$$+x\left(\frac{y}{x}\right)'$$

であるから，(4)とから，

$$A_0=\left[\frac{dy}{dx}\right]_{x=0}=\left[p\frac{\sqrt{1-y^2}}{\sqrt{1-x^2}}\right]_{x=0}=p$$

よって，前々頁の(iii)とから次の定理が成り立つ：

定理　$A_0=p,A_1,A_2,\cdots,A_{\frac{p-3}{2}}$ は p の倍数である．

方程式(6)の $\frac{p-1}{2}$ 個の根は

$$\sin^2\left(\frac{r_j\cdot2\pi}{p}\right)\ \left(j=1,2,3,\cdots\cdots,\frac{p-1}{2}\right)$$

であるから，根と係数との関係により

(7) $$\prod_{j=1}^{\frac{p-1}{2}}\sin^2\left(\frac{r_j\cdot2\pi}{p}\right)=(-1)^{\frac{p-1}{2}}\cdot\frac{p}{(-4)^{(p-1)/2}}$$

q を p と異なる奇素数とすると，

$$qr_j\neq0\pmod p$$

であるから，各 j に対して j' が一意的に定まり

$$\begin{cases}qr_j\equiv(-1)^ur_{j'}\pmod p,\\ j\neq k\ \Rightarrow\ j'\neq k'\end{cases}$$

となる．それゆえ $\frac{qr_j}{p}-\frac{(-1)^ur_{j'}}{p}$ は整数である．

$$\therefore\ \sin\left(\frac{qr_j\cdot2\pi}{p}\right)=(-1)^u\sin\left(\frac{r_{j'}\cdot2\pi}{p}\right),$$

$$\therefore\ qr_j \equiv r_{j'}\cdot\frac{\sin\left(\frac{qr_j\cdot 2\pi}{p}\right)}{\sin\left(\frac{r_{j'}\cdot 2\pi}{p}\right)}\pmod{p},$$

したがって

$$q^{\frac{p-1}{2}}\equiv\prod_{j=1}^{\frac{p-1}{2}}\left\{\frac{\sin\left(\frac{qr_j\cdot 2\pi}{p}\right)}{\sin\left(\frac{r_j\cdot 2\pi}{p}\right)}\right\}\pmod{p}.$$

この右辺は ±1 であるから $\left(\frac{q}{p}\right)$ に等しい.

さて, $r_j\cdot 2\pi=p\theta_j$ とおく. 上の定理によって

$$\begin{aligned}&\sin q\theta_j\\&=\sin\theta_j\{(-4)^{\frac{q-1}{2}}\sin^{q-1}\theta_j\\&\quad+q(B'_{\frac{q-3}{2}}\sin^{q-3}\theta_j+\cdots\cdots+B'_1\sin 2\theta_j+1)\},\end{aligned}$$

ここに, 各 B'_k は整数である.

このようにして,

$$\begin{aligned}(8)\ &\left(\frac{q}{p}\right)\\&=\prod_{j=1}^{\frac{p-1}{2}}\{(-4)^{\frac{q-1}{2}}\sin^{q-1}\theta_j\\&\quad+q(B'_{\frac{q-3}{2}}\sin^{q-3}\theta_j+\cdots\cdots+B'_1\sin^2\theta_j+1)\}.\end{aligned}$$

ここで例えば $p=5, q=7$ の場合を考えると, 2次方程式 $(-4)^2K^2+A_1K+p=0$ の2つの根が $\sin^2\theta_1=\alpha$, $\sin^2\theta_2=\beta$ であるから,

(8)の右辺は

$$\begin{aligned}&\{(-4)^3\alpha^3+q(B'_2\alpha^2+B'_1\alpha+1)\}\\&\quad\times\{(-4)^3\beta^3+q(B'_2\beta^2+B_1'\beta+1)\}\\&=(-4)^6\alpha^3\beta^3+(-4)^3q\\&\quad\times\{\alpha^2\beta^2(\alpha+\beta)B'_2+\alpha\beta(\alpha^2+\beta^2)B'_1+\alpha^3+\beta^3\}\\&\quad+q^2\{\alpha^2\beta^2B'^2_2+\alpha\beta(\alpha+\beta)B'_2B'_1+(\alpha^2+\beta^2)B'_2\\&\qquad+(\alpha+\beta)B'_1+\alpha\beta B'^2_1+1\}\end{aligned}$$

となる. そこで, 方程式(6)の $\frac{p-1}{2}$ 個の根が $\sin^2\theta_j$ $\left(j=1,2,\cdots\cdots,\frac{p-1}{2}\right)$ であることと(8)により

$$(9)\ \left(\frac{q}{p}\right)=\prod_{j=1}^{\frac{p-1}{2}}(-4)^{\frac{q-1}{2}}\sin^{q-1}\theta_j+a_1q+\cdots\cdots+a_{\frac{p-1}{2}}q^{\frac{p-1}{2}},$$

ここに, 各 $(-4)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}a_j$ は整数である.

そして(7)によって

$$\begin{aligned}(10)\ &\prod_{j=1}^{\frac{p-1}{2}}(-4)^{\frac{q-1}{2}}\sin^{q-1}\theta_j\\&=(-4)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}\prod_{j=1}^{\frac{p-1}{2}}(\sin^2\theta_j)^{\frac{q-1}{2}}\\&=(-4)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\prod_{j=1}^{\frac{p-1}{2}}\sin^2\theta_j\right)^{\frac{q-1}{2}}\\&=(-4)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left\{(-1)^{\frac{p-1}{2}}\cdot\frac{p}{(-4)^{(p-1)/2}}\right\}^{\frac{q-1}{2}}\\&=\{(-1)^{\frac{p-1}{2}}\cdot p\}^{\frac{q-1}{2}}.\end{aligned}$$

さて, (9)から

$$\begin{aligned}(-4)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)&=(-4)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\prod_{j=1}^{\frac{p-1}{2}}(-4)^{\frac{q-1}{2}}\sin^{q-1}\theta_j\\&\quad+b_1q+\cdots\cdots+b_{\frac{p-1}{2}}q^{(p-1)/2}\end{aligned}$$

ここに, 各 b_j は整数であるから, (10)とから

$$(-4)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)\equiv(-4)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}p^{\frac{q-1}{2}}\pmod{q},$$

$$\therefore\ \left(\frac{q}{p}\right)\equiv(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\cdot p^{\frac{q-1}{2}}\pmod{q},$$

$$\therefore\ (11)\ p^{\frac{q-1}{2}}\equiv(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)\pmod{q}$$

一方 $(12)\ p^{\frac{q-1}{2}}\equiv\left(\frac{p}{q}\right)\pmod{q}$

(11), (12)の右辺はともに ±1 であり, その差が q で割り切られることから

$$(13)\ \left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$$

となる. (13)は**平方剰余相互法則**に他ならない.

〈参考文献〉

[1] 雑誌「大学への数学」1996年5月号, 「入試特集 1996年大学入試問題」, 東京出版刊

[2] Gotthold Eisenstein, MATHEMATISCHE WERKE,BAND I, pp.299−308,CHELSEA PUBLISHING COMPANY, NEW YORK.

[3] 宮川幸隆著, 大学入試の背景を探る, 数研通信・数学 No.21, p.7−11, 数研出版刊

(静岡県立三島北高等学校)