Fermat の問題に関して

若　松　忠　道

On the Fermats Problem

Tadamichi WAKAMATSU

1 p を素数とする。法 p についての整数の剰余類より，0 に congrnent な物を除いた p−1 個の類は，乗法に関して巡回群を作る。それを

L: $l_0=1,\ l_1,\ l_2,\cdots\cdots l_{p-2}$

とする。この中の l_i の各数を p 乗すると，法 p^2 について同一の剰余類に属する。その類を s_i とする。

S: $s_0=1,\ s_1,\ s_2,\cdots\cdots s_{p-2}$

は L と同型な群を作る事が分る。

全文を通じて l_i, s_i は夫々p, p^2 に関する最小正剰余を以て表はし，同時にそれ等の文字はその数字をも示すとする。又 l_i, s_i 或はこれに類する文字の脚符が p−1 以上になる時は，脚符の数値は常に法 p−1 についての最小正剰余で置き換える。p−1 は 0 とする。$q=\frac{p-1}{2}$ とすると

$$l_i+l_{i+q}=p,\qquad s_i+s_{i+q}=p^2 \qquad ①$$

2 S の三元素間に

$$s_0+s_a+s_b=p^2 \qquad ②$$

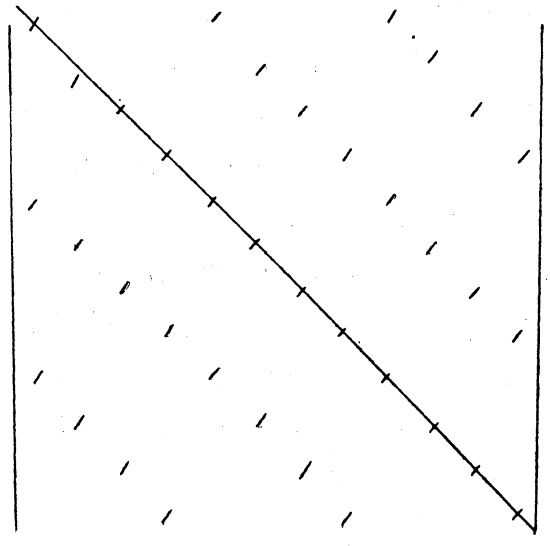
なる関係があると仮定する。この三項の代りに，それ等に同一の元素 s_j を乗じて得られる S の元素を用いると

$$s_j+s_{a+j}+s_{b+j}=k'_j\,p^2 \qquad ③$$

k'_j は1又は2となる。

③の右辺は三項式であるが，これを，S の各元の一次式で，その三項以外の項の係数が 0 なるものと見做し，且項を s_0, s_1, $s_2,\cdots\cdots$, s_{p-2} の順に揃えて，j につき 0 より p−2 迄取つた p−1 個の一次等式を考え，その左辺の作る行列式を D とする。

D=



例　p=13 の場合

L: 1, 2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7

S: 1, 80, 147, 99, 146, 19, 168, 89, 22, 70, 23, 150

$s_0+s_4+s_8=1+146+22=169=p^2$

空所の文字は 0 である。

③ が成立てば

$$l_j+l_{a+j}+l_{b+j}=k_jp \qquad ④$$

も成立つ。③より出発して上に考察したのと全く同様に，④より出発して L の元素の p−1 個の一次等式が得られる。その左辺の係数の作る行列式はやはり D で，k_j は1又は2であるが必ずしも k'_j に等しくない。

D の第 i+1 列の各第 j+1 行元素に k_j を代入して出来る行列式と，D の第一列の各 j+1 行元素に k_{i+j} を代入して出来る行列式は，偶数回の行，列の互換で互に他に移るから，相等しい。これを D_i で表わす。その k を k′ にかえたものをD'_i と書く事にする。

ここで，以下第6節迄る渉る帰謬法の仮設として

$$D\neq 0$$

とおけば

$$l_i=\frac{D_i}{D}p, \qquad s_i=\frac{D'_i}{D}p^2 \qquad ⑤$$

更に又

$$\tau_i=2k_i-3, \qquad \tau'_i=2k'-3 \qquad ⑥$$

とおきかえて，D_i, D'_i の第一列元素 k_j, k'_j の代りに夫々 τ_j, τ'_j をおきかえた行列式を $\overline{D}_i$, $\overline{D'}_i$ と書けば，⑤より少し計算して

$$2l_i-p=\frac{\overline{D}_i}{D}p, \qquad 2s_i-p^2=\frac{\overline{D'}_i}{D}p^2. \qquad ⑦$$

3．第 j 分値が τ_{i+j} なる 2q 次元 vector を v_i，その τ_{i+j} の代りに τ'_{i+j} を用いたものを v'_i とおこう。

v_0, v_1, ……, v_{p-2} はすべて一次独立ではない。先づ①により次の関係を得る。

$$v_{i+q}=-v_i \qquad ⑧$$

v_0, v_1, ……v_{r-1} は互に一次独立で，v_r を入れると，その r+1 個は一次従属となる様な番号 r がある。⑧より r<q，第3，4，5節は r=q−1 を証明する事を目標とする。

r の条件より一意的に

$$c_0v_0+c_1v_1+\cdots\cdots+c_rv_r=0$$

その各分値を考えると

$$c_0\tau_j+c_1\tau_{j+1}+\cdots\cdots c_r\tau_{j+r}=0 \qquad (9)$$

$$(j=0,1,\cdots\cdots, p-2)$$

一般に 0 内至 p−2 の脚符をもつ p−1 個の数 z_i がある時，p−2 次の整式 f(x) の x^i に z_{j+1} を代入した式を $f(z_j)$ と書き，j の如何にかゝわらず $f(z_j)=0$ が成立する事を $f(z)=0$ と書く事にして，(9)を次式で示す。

$$\varphi(\tau)=0 \qquad (10)$$

$f(x)$ が $\varphi(x)$ の倍式なる時は $f(\tau)=0$.

(証)　$f(x)=\varphi(x)\cdot h(x)$, $h(x)=b_0+b_1x+\cdots\cdots b_mx^m$

とすれば，j の如何にかゝわらず

$$f(\tau_j)=[b_0\varphi(x)+b_1x\cdot\varphi(x)+\cdots\cdots b_mx^m\varphi(x)]_{x^i\to\tau_{j+i}}$$
$$=b_0\varphi(\tau_j)+b_1\varphi(\tau_{j+1})+\cdots\cdots+b_m\varphi(\tau_{j+m})=0.$$

となるから

逆に $f(\tau)=0$ ならば，$f(x)$ は $\varphi(x)$ の倍式である。

(証)　$f(x)=\varphi(x)\cdot h(x)+R(x)$　　($R(x)$ は r より低次)

とおけば，上述より $[\varphi(x)\cdot h(x)]_{x^i\to\tau_{j+i}}=0$，$f(\tau)=0$ (仮設) より $R(\tau)=0$．然る時は v_0, v_1, $\cdots\cdots v_{r-1}$ が一次従属となり，矛盾，故に $R(x)=0$ でなければならぬ。証終

$F(x)=x^q+1$　とおけば　$F(\tau)=0$

(証)　①と④より $k_j+k_{j+q}=3$，故に⑥より $\tau_j=-\tau_{j+q}$ となるから，　証終

以上の事から $\varphi(x)$ は x^q+1 の約式である。

$$\varphi(x)\cdot\mu(x)=x^q+1$$

4．1の原始 d 乗根のすべてを零点とし，且つその外に零点をもたぬ整式を $\Phi_d(x)$ と書けば，$\Phi_d(x)$ は有理数体において既約で，而もその係数はすべて整数となる。又 $\Phi_1(x)$ 以外は係数が対称的である。即ち $\Phi_d(x)$ を n次とすれば x^k と x^{n-k} の係数は相等しい。又任意の整数 h に対し

$$x^h-1=\prod_{d\mid h}\Phi_d(x). \qquad ⑪$$

$\varphi(x)$ は前節の最後により $h=2q$ とおいた場合の $x^{2q}-1=(x^q+1)(x^q-1)$ の右辺第一因数の中に含まれる $\Phi_d(x)$ の積となるわけである。

q が含む最大の2の幕因数を 2^m とする時，x^q+1 の因数たる $\Phi_d(x)$ は x^{2m} の整式である。

(証)　⑪によれば，d が q の約数であれば $\Phi_d(x)$ は x^q-1 の因数となるので，d が 2q の約数で且 q の約数でない時，即ち 2^{m+1} の倍数なる時，且その時のみ x^q+1 の因数となる。而も $\Phi_d(x)=\prod_{e/d}(x^e-1)^{\mu(d/e)}$ における Möbius の函数 $\mu(d/e)$ が O にならない為には e が 2^m の倍数でなければならない。証終

x^q+1 の因数たる $\Phi_d(x)$ の中で，$\Phi_{2^{m+1}}(x)$ のみ二項式で，他はすべて係数の和が1となる。

(証)　$x^{2^m}=y$ とおくと　$\Phi_d(x)=\Phi_{d'}(y)$ $\left(d'=\dfrac{d}{2^m}\right)$ この $\Phi_{d'}(y)$ について考えればよい。

$d'=2\cdot o_1\cdot o_2\cdots\cdots o_m$ ($o_1\cdots\cdots o_m$ は奇素数)．$\Phi_{d'}(y)$ はそれ等を算出する過程からすぐ分る様に

$$1-y^{o_1}+y^{o_1}\cdots\cdots+y^{to_1}$$

の形の式（即ちその係数の和は1）の若干個の乗除によつて得られる。$y=1$ として考えると，積の係数の和は，各因数の係数の和の積に等しい。従つて除法を行つた結果も同様になる。故に $\Phi_{2^{m+1}}(x)=x^{2^m}+1$ 以外の x^q+1 の因数の係数の和は1に等しい。

故に若し $\varphi(x)$ が $\Phi_{2^{m+1}}(x)$ を因数に持たなければ，⑨における τ_i は ±1 であり，奇数個の1又 -1 の和が 0 になる事はないので，⑩に矛盾する。従つて

$\varphi(x)$ の係数の和は 2 である。$\varphi(1)=2$ ⑫

5. $\gamma<q-1$, 即ち$\mu(x)=\dfrac{x^q+1}{\varphi(x)}$が定数1でないとすると，$\mu(x)$ に因数 $\Phi_h(x)$ が存在する。

$L_j(x)=l_j+l_{j+1}x+\cdots\cdots+l_{j-1}x^{2q-1}$

に $\varphi(x)$ を乗ずる時，$\varphi(x)$ の係数の対称性から，x_i の項の係数は $\varphi(l_{j-\gamma+i})$. 但し x^{2q} 以上の高次の項は $x^{2q}=1$ を用いて 2q よりも低次の項に直す。この事は普通の整式で書けば

$$L_j(x)\cdot\varphi(x)=\sum_{i=0}^{2q-1}\varphi(l_{j-\gamma+i})x^i+(x^{2q}-1)\cdot H(x) \qquad ⑬$$

ここに $H(x)$ は或る整係数の整式

所が ⑦, ⑩, ⑫ を用いると

$$\varphi(l_i)=p$$

故に ⑬ の右辺は $x-1$ 以外の $x^{2q}-1$ の因数を，すべて因数として含む。

$\therefore\ L_j(x)\cdot\varphi(x)=\Phi_h(x)\cdot Q(x)$ $\quad$ ($Q(x)$ は整式)

$\varphi(x)$ は $\Phi_h(x)$ を含まないから

$L_j(x)=\Phi_h(x)\cdot R(x)$ $\quad$ ($R(x)$は或る整式)…… ⑭

然るに ① を用いて

$$\begin{aligned}L_j(x)&=l_j+l_{j+1}x+\cdots\cdots l_{j+q}x^q+l_{j+q+1}x^{q+1}+\cdots\cdots+l_{j-1}x^{2q-1}\\&=(1-x^q)(l_j+\cdots\cdots+l_{j+q-1})+p\cdot x^q(1+x+\cdots\cdots+x^{q-1})\\&=(1+x+\cdots\cdots+x^{q-1})\{M_j(1-x)+p\cdot x^q\}\cdots\cdots\end{aligned} \qquad ⑮$$

$\Phi_h(x)=0$ の根 ρ は x^q+1 の根であつて，x^q-1 従つて ⑮ の右辺第一因数の根とはならない。又 $\rho^q=\pm1$ で ρ は複素数であるから

$$M_j(1-\rho)\pm p\neq 0$$

$\Phi_h(x)$ は既約だから，上の事から $L_j(x)$ の約数とはならない。これと ⑭ は矛盾する。

従つて $\gamma=q-1$, 即ち $\varphi(x)=x^q+1$ でなければならない。

6. 前節の結論：$\varphi(x)=x^q+1$ は q 個の vector v_0, v_1, $\cdots\cdots v_{q-1}$ が一次独立である事を示す。これに v_0' を合せると，この q+1 個の vector は一次的に独立ではあり得ない。何となれば，是等の vector に2 q 次元であるが，第 i 分値と第 i+q 分値は必ず反数になつていなければならないから，実質的には q 次元であるからである。故に一意的に

$$v_0'=m_0v_0+m_1v_1+\cdots\cdots+m_{q-1}v_{q-1}$$

D の第1列に v_i, v_i' の分値を代入したものが夫々 $\overline{D}_i$, $\overline{D}_i'$ となつている。

$\therefore\ \overline{D}_0'=m_0\overline{D}_0+m_1\overline{D}_1+\cdots\cdots+m_{q-1}\overline{D}_{q-1}$ ⑯

然るに D の含む最大の p 巾因数を $p^k(k\geqq2)$ とる時 l_i, s_1 は p と互に素であるから，⑦から $\overline{D}_i$ は丁度 p^{k-1}, $\overline{D}_i'$ は丁度 p^{k-2} なる p 巾因数をもつ。⑯は之に反する事を示す。

この矛盾は $D\neq0$ とした所から来る。

$\therefore\ D=0$

7．次に D＝0 となる為の条件を求める。D の第 i+1 行 vector を u_i で表わす。D＝0 なる事より，u_0，u_1，……$u_{\lambda-1}$ は一次独立で，u_0，u_1，……$u_{\lambda-1}$，u_λ は一次従属なる様な番号 $\lambda(<2q)$ がある。

$$\psi(u_0)=d_0u_0+d_1u_1+\cdots\cdots+d_\lambda u_\lambda=0 \cdots\cdots \quad ⑰$$

をその従属関係を示す一次式とすると

$$\varphi(x)=d_0+d_1x+\cdots\cdots d_\lambda x^\lambda$$

は第3節の所論と同様にして $x^{2q}-1$ の約式となる。

$$g(x)=1+x^a+x^b$$

とおくと，等式（＝0）⑰ の分値を考える事により，第5節の初めの方と同様にして

$$g(x)\cdot\varphi(x)=(x^{2q}-1)\cdot k(x)$$

故に $g(x)$ は $x^{2q}-1/\varphi(x)$ （$\lambda<2q$ より1次以上）で割り切れる。即ち或る1の 2q 乗根 η によつて

$$1+\eta^a+\eta^b=0$$

この様になるのは ω を1の複素三乗根として $\eta^a=\omega$，$\eta^b=\omega^2$ なる場合の外ない。故に 2q は3の倍数で b＝2a

$g(x)$ の代りに $g_1(x)=1+x^{b-a}+x^{2q-a}$ をとつても同様の論が成立ち，$2q-a=2(b-a)$

$$\therefore\quad a=\frac{2q}{3}$$

故に巡回群の S の三元 s_0，s_a，s_b が部分群を作る事が D＝0 なる為の条件である。

8．m を p と互に素な整数とする時 $q(m)=\dfrac{m^{p-1}-1}{p}$ を Fermat の商と呼ぶ。1909年ヴィツフェリフヒの証した下の定理がある。

定理　$x^p+y^p=z^p$ （x，y，z，p は互に素，$p>2$）……　⑱

が整数解を有する為には

$$q(2)\equiv 0\ (\mathrm{mod}\ p)\cdots\cdots \quad ⑲$$

なる事が必要である。

後ミリマノフは

$$q(3)\equiv 0\quad (\mathrm{mod}\ p)\cdots\cdots \quad ⑳$$

の必要な事をも証明している。

⑲，⑳ は吾人の記法を以てすれば

或る a，b に対し，$l_a=2$ なる時 $s_a=2$，$l_{q+b}=3$ なる時 $s_{q+b}=3$

なる事を示す。然る時 ① により

$$s_0+s_a+s_b=p^2$$

即ち ③ が成立する。故に前節の結論により

$$s_0=1,\ s_a=2,\ s_b=p^2-3$$

は法 p^2 に関して乗群を作る。

$$\therefore \quad 2(p^2-3)\equiv 1 \pmod{p^2}$$

$$\text{i. e} \quad 7\equiv 0 \pmod{p^2}$$

その様な p は存在しない。

故に ⑱ の解は存在しない。或は Fermat の問題 $x^p+y^p=z^p$（p は素数）の整数解は，x，y，z の何れかが p の倍数なるものの外にはない。