数理解析研究所講究録
第371巻 1979年 98-105

Fermat の大定理について

上智大 理工 和田秀男

奇素数 P に対して次の式が有理整数解を持つとする：

(1) $x^P + y^P + z^P = 0$, $(xyz, P) = 1$.

このとき $B_{P-3} \equiv B_{P-5} \equiv B_{P-7} \equiv B_{P-9} \equiv 0 \pmod P$ が成立つ (Mirimanoff [1]). B_{P-n} はベルヌイ数である. 最近, 計算機を用いて $B_{P-11} \equiv B_{P-13} \equiv B_{P-15} \equiv B_{P-17} \equiv B_{P-19} \equiv 0 \pmod P$ が得られたのでその方法を示そう.

§1. 方法 まず Kummer の criteria を用い Mirimanoff は

(2) $B_{P-n} \cdot P_n(t) \equiv 0 \pmod P$, $(n = 3, 5, \cdots, P-2)$

を示した. $P_n(x)$ は次のような整係数 $n-1$ 次多項式である：

$$P_n(x) = a_{n,1}x - a_{n,2}x^2 + \cdots - a_{n,n-1}x^{n-1},$$

$$a_{n,m} = m^{n-1} - \binom{n}{1}(m-1)^{n-1} + \binom{n}{2}(m-2)^{n-1} - \cdots + (-1)^{m-1}\binom{n}{m-1}.$$

また x, y, z を(1)の解としたとき, もは

$A=\{\frac{y}{x},\frac{x}{y},\frac{z}{x},\frac{z}{z},\frac{z}{y},\frac{y}{z}\}$ の任意の元である．

合同式(2)は左辺を既約分数に直したとき，分子がPで割れることを意味する．$a_{n,m}=a_{n,n-m}$ となるので $P_n(x)$ は $x(1-x)$ で割り切れる．たとえば $n=11$ のとき

$$P_{11}(x)=x(1-x)(1-1012x+46828x^2-408364x^3+901990x^4-408364x^5+46828x^6-1012x^7+x^8)$$

となる．$P_n(x)=x(1-x)Q_n(x)$ とおけば $Q_n(x)=0$ は逆数方程式となり，根はすべて正の単根である（Krasner [3]）．

もし $P_n(t)\not\equiv 0 \pmod P$ となる元 $t\in A$ が存在したならば，(2)より $B_{p-n}\equiv 0 \pmod P$ が得られる．Aの正体はわからないが $x+y+z\equiv x^p+y^p+z^p=0 \pmod P$ を使えば tをAの任意の元としたとき

$$A=\{t,\frac{1}{t},-1-t,-\frac{1}{t+1},-\frac{1+t}{t},-\frac{t}{1+t} \pmod P\}$$

となり，3通りの可能性がある．

<u>$|A|=3$ の場合．</u> このとき $A=\{1,-2,-\frac{1}{2} \pmod P\}$ となる．もし $Q_n(-2)\not\equiv 0 \pmod P$ が得られたならば，$B_{p-n}\equiv 0 \pmod P$ となる．$Q_n(x)=0$ の根は正根ばかりなので $Q_n(-2)\not\equiv 0$ である．たとえば $Q_{11}(-2)=3408251=11\cdot 41\cdot 7571$ となる．もし(1)が成立つならば

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

が成立つ (Wieferich [2]). 11, 41, 7557 は (3) を満たさないので $Q_{11}(-2) \not\equiv 0 \pmod P$ が得られた.

$|A|=2$ の場合. このとき $A=\{t \mid t^2+t+1 \equiv 0 \pmod P\}$ となる. もしAの2元に対し $Q_n(t) \equiv 0 \pmod P$ ならば $Q_n(x) \equiv (1+x+x^2) R_n(x) \pmod P$ となるはずである. よって $Q_n(x)$ を $(1+x+x^2)$ で割ってみる. $Q_n(x)$ も $(1+x+x^2)$ が逆数方程式なので、商も逆数方程式となるはずである. 計算量を半分にするために余りは $\frac{n-3}{2}$ 次の所とし, $S_n \cdot x^{\frac{n-3}{2}}$, $(S_n \in \mathbb{Z})$ とする. $S_n=0$ とすると $Q_n(x)=0$ が虚根を持ってしまうので $S_n \neq 0$ である. たとえば

$$Q_{11}(x)=(1+x+x^2)(1-1013x+47840x^2 - 455191x^3+47840x^4-1013x^5+x^6) + 1261501x^4$$

となる. $S_{11}=1261501=683 \cdot 1847$ であり 683, 1847 は (3) を満たさないので $Q_{11}(t) \not\equiv 0 \pmod P$ となる.

$|A|=6$ の場合 6つのAの元に対して $Q_n(t) \equiv 0 \pmod P$ ならば $Q_n(x)$ は

$$F(x)=(x-t)\left(x-\frac{1}{t}\right)(x+1+t)\left(x+\frac{1}{1+t}\right)\left(x+\frac{1+t}{t}\right)\left(x+\frac{t}{1+t}\right)$$
$$=1+3x+ax^2+(2a-5)x^3+ax^4+3x^5+x^6$$

$$\left(a=-(1+3t-5t^3+3t^5+t^6)\Big/\{t^2(1+t)^2\}\right)$$

で割り切れるはずである．a の値はわからないので，変数として扱い割り算を実行する：

(4) $$Q_n(x)=F(x)\cdot T_n(x)+U_n(a)\cdot\{x^{(n-7)/2}+x^{(n+1)/2}\}$$
$$+V_n(a)\cdot\{x^{(n-5)/2}+x^{(n-1)/2}\}+W_n(a)\cdot x^{(n-3)/2}$$
$$\left(T_n(x)\in\mathbb{Z}[a,x],\ U_n(a),\ V_n(a),\ W_n(a)\in\mathbb{Z}[a]\right).$$

さて $\mathbb{Q}[a]$ の中で考えると $U_n(a)$, $V_n(a)$, $W_n(a)$ の最大公約数は1であることを証明しよう．もし最大公約数 $D_n(a)\in\mathbb{Z}[a]$ の次数 m が1次以上ならば，(4)の両辺に適当な自然数 k を掛けると

(5) $$k\cdot Q_n(x)=k\cdot F(x)\cdot T_n(x)+D_n(a)\cdot E(x)$$
$$\left(E(x)\in\mathbb{Z}[a,x],\ \deg D_n(a)=m\geqq 1\right)$$

となる．$D_n(a)$ をもの有理式で表わすと

(6) $$D_n(a)=b_m a^m+b_{m-1}a^{m-1}+\cdots$$
$$=\frac{1}{t^{2m}(1+t)^{2m}}\{b_m(-t^6-\cdots-1)^m$$
$$+b_{m-1}t^2(1+t)^2(-t^6-\cdots)^{m-1}+\cdots\}$$
$$=\frac{1}{t^{2m}(1+t)^{2m}}\ G(t)$$
$$\left(G(x)\in\mathbb{Z}[x],\ \deg G(x)=6m\right)$$

となる．$Q_n(x)=0$ は正根しかないので $Q_n(x)$ と $Q_n(-1-x)$ の終結式 R は0でない．よって $0<|R|<P$ なる素数 P に対してはどのような $t\in\mathbb{Z}$ を持ってきても

同時に

(7) $Q_n(t) \equiv 0 \pmod{P}$

$Q_n(-1-t) \equiv 0 \pmod{P}$

が成立つことはない (Krasner [3]). 代数体には無限に多くの1次の素イデアルが存在することから $t \in \mathbb{N}$ を十分大きく取れば $P \mid G(t)$, $|R| < P$, $|b_m| < P$, $k < P$ となる素数Pが存在する. このPに対しては (5), (6) より (7) が両式とも成立し、矛盾である. よって $U_n(a)$, $V_n(a)$, $W_n(a)$ の最大公約数は1である. よって

(8) $A_n(a) \cdot U_n(a) + B_n(a) \cdot V_n(a) + C_n(a) \cdot W_n(a) = D_n \in \mathbb{N}$

$(A_n(a), B_n(a), C_n(a) \in \mathbb{Z}[a])$

となる $A_n(a)$, $B_n(a)$, $C_n(a)$, D_n が存在する. もしある a に対して $U_n(a) \equiv V_n(a) \equiv W_n(a) \equiv 0 \pmod{P}$ ならば (8) より $D_n \equiv 0 \pmod{P}$ となる. よって $D_n \not\equiv 0 \pmod{P}$ ならば (4) より $Q_n(t) \not\equiv 0 \pmod{P}$ となる. たとえば $D_{11} = 11$ となり $P = 11$ は (3) を満たさないので $B_{p-11} \equiv 0 \pmod{P}$ が得られる.

このような方法で3つの場合にそれぞれ例外的な素数を求め、次にこれらが (3) を満たさないことを確かめ

$$B_{p-11} \equiv B_{p-13} \equiv B_{p-15} \equiv B_{p-17} \equiv B_{p-19} \equiv 0 \pmod{P}$$

が得られた.

§2. アルゴリズム. まず苦労したのは自然数の素因子分解である. 今回は一番単純な方法で行なった.

まず, m が素数か否かは

$$\left.\begin{array}{l} {}^{\exists}b,\ (b,m)=1,\ b^{m-1}\not\equiv 1 \pmod m \\ m-1=q_1^{a_1}\cdots q_r^{a_r},\ q_i=\text{素数} \\ {}^{\forall}i,\ {}^{\exists}b_i,\ b_i^{m-1}\equiv 1 \pmod m \\ \qquad b_i^{(m-1)/q_i}\not\equiv 1 \pmod m \end{array}\right\} \Longrightarrow m=\text{素数}$$

で判定した. $m=$合成数のときは m を分解するために, $\sqrt{m}$ 以下の奇数(ただし3と5と7の倍数はぬかした)で小さい順に割っていった. 割り算は倍長の浮動小数計算で実行した. 精度内の整数に対して正しく四則算法は行なわれているはずで, もし正しい整数の答が得られないとしたら, その計算機は欠陥商品である.

次に (4) のような変数 a を含む割り算であるが, $U_n(a)$, $V_n(a)$, $W_n(a)$ の次数は $\left[\frac{n-5}{4}\right]$ 次以下なので, $a=-1, 0, 1, 2$ 等の $\left[\frac{n-5}{4}\right]+1$ 個の値を代入し, (4) を実行し, 連立1次方程式を解いて $U_n(a)$, $V_n(a)$, $W_n(a)$ の係数を求めた.

さて, 一番苦労したのは (8) 式を満たすなるべく小さな D_n を求めることであった. 勿論, ユークリッドの互除法で求めるのだけれど, たとえば $n=19$ のとき次のよう

に計算した．

(9)　$b_3 \cdot a^3 + b_2 \cdot a^2 + b_1 \cdot a + b_0$

(10)　$c_3 \cdot a^3 + c_2 \cdot a^2 + c_1 \cdot a + c_0$

(11)　$d_3 \cdot a^3 + d_2 \cdot a^2 + d_1 \cdot a + d_0$

の3式の最大公約数を求めるために，適当に整数倍して他の式より引くという同値な変形を繰り返し，たとえば $b_3 \neq 0$, $c_3 = d_3 = 0$ とすることが出来る．次に (10), (11) の2式に対して同様の変形を行ない $c_2 \neq 0$, $d_2 = 0$ と変形出来る．次に (9) を $(9) \times c_2 / (b_3, c_2) - (10) \times b_3 \cdot a / (b_3, c_2)$ と変形し次数をへらした．この変形は一般には同値な変形でない．このように大きな数が現われないように次数を下げてゆき，次数が0になるまで行なった．このようにして得られた D_n は一般には (8) で表わされる D_n の最小値とはかぎらない．しかし $n \leqq 19$ の場合，変形を吟味することにより，最小値を求めることが出来た．次に計算結果をまとめてみよう．少ないデーターではあるが，この表より，n が素数か否かにしたがって $D_n = n$ または 1 となるような気がする．

$Q_{11}(-2)=3408252l=11\cdot41\cdot75571$

$Q_{13}(-2)=9363855865=5\cdot7\cdot13\cdot20579903$

$Q_{15}(-2)=3547114323481=\text{prime}$

$Q_{17}(-2)=1771884893993785=5\cdot17\cdot20845704635221$

$Q_{19}(-2)=1128511554418948441=7\cdot19\cdot916933\cdot9253728769$

$S_{11}=1261501=683\cdot1847$

$S_{13}=-151846331=-7\cdot13\cdot13\cdot47\cdot2731$

$S_{15}=25201039501=11\cdot331\cdot419\cdot16519$

$S_{17}=-5515342166891=-23\cdot401\cdot13687\cdot43691$

$S_{19}=1538993024478301=7\cdot19\cdot7691\cdot8609\cdot174763$

$D_{11}=11$

$D_{13}=13$

$D_{15}=1$

$D_{17}=17$

$D_{19}=19$

References

[1] M.Mirimanoff, L'équation indéterminée $x^l+y^l+z^l=0$ et le criterium de Kummer, J. Reine Angew. Math.,128(1905), pp.45-68.

[2] A.Wieferich, Zum letzten Fermatschen Theorem, J. Reine Angew. Math., 136(1909), pp.293-302.

[3] M.M.Krasner, Sur le premier cas du théorème de Fermat, C. R. Acad. Sci. Paris, 199(1934), pp.256-258.