TOKYO J. MATH.
VOL. 3, No. 1, 1980

Some Computations on the Criteria of Kummer

Hideo WADA

Sophia University

If $x^p+y^p+z^p=0$ with an odd prime p has any integer solution such that $(xyz, p)=1$, then Mirimanoff [1] proved

$$B_{p-3}\equiv B_{p-5}\equiv B_{p-7}\equiv B_{p-9}\equiv 0(\mathrm{mod}\ p)$$

where B_{p-n} are Bernoulli numbers. In this paper, the author proves that

$$B_{p-11}\equiv B_{p-13}\equiv B_{p-15}\equiv B_{p-17}\equiv B_{p-19}\equiv 0(\mathrm{mod}\ p)$$

are also necessary.

§1. Method.

Let p be an odd prime number and x, y, z be rational integers such that $(xyz, p)=1$. If x, y, z satisfy the Fermat's equation:

$$x^p+y^p+z^p=0 \tag{1}$$

then using the criteria of Kummer, Mirimanoff [1] proved

$$B_{p-n}\cdot P_n(t)\equiv 0(\mathrm{mod}\ p)\ , \qquad (n=3, 5, \cdots, p-2) \tag{2}$$

where $B_1=-1/2$, $B_2=1/6$, $B_3=0$, $B_4=-1/30$, $\cdots$ are Bernoulli numbers, $P_n(x)$ are polynomials such that

$$P_n(x)=a_{n,1}x-a_{n,2}x^2+\cdots+(-1)^n a_{n,n-1}x^{n-1} \tag{3}$$

$$a_{n,m}=m^{n-1}-\binom{n}{1}(m-1)^{n-1}+\binom{n}{2}(m-2)^{n-1}-\cdots+(-1)^{m-1}\binom{n}{m-1} \tag{4}$$

and t is an arbitrary element of $A=\{y/x, x/y, z/x, x/z, z/y, y/z\}$. All roots of $P_n(x)=0$ are real positive numbers (Krasner [3]). If $P_n(t)\not\equiv 0(\mathrm{mod}\ p)$ for some $t\in A$, then from (2) we get $B_{p-n}\equiv 0(\mathrm{mod}\ p)$. These coefficients $a_{n,m}$ satisfy $a_{n,m}=a_{n,n-m}$. Therefore $P_n(x)$ can be divisible by $x(1-x)$:

$$P_n(x)=x(1-x)Q_n(x) \tag{5}$$

Received September 4, 1979

$$(6)\qquad Q_n(x)=b_{n,0}+b_{n,1}x+b_{n,2}x^2+\cdots+b_{n,n-3}x^{n-3}\ ,\qquad (b_{n,i}\in \boldsymbol{Z})$$

$$(7)\qquad b_{n,i}=b_{n,n-3-i}\ .$$

There are three possibilities.

Case 1. $|A|=3$, $A=\{1, -2, -1/2(\mathrm{mod}\ p)\}$.

In this case we get $Q_n(-2)\neq 0$, because all roots of $P_n(x)=0$ are positive. If $Q_n(-2)\not\equiv 0(\mathrm{mod}\ p)$, then we get $B_{p-n}\equiv 0(\mathrm{mod}\ p)$.

Case 2. $|A|=2$, $A=\{t_1, t_2\}=\{t\,|\,t^2+t+1\equiv 0(\mathrm{mod}\ p)\}$.

If $Q_n(t_1)\equiv Q_n(t_2)\equiv 0(\mathrm{mod}\ p)$, then $Q_n(x)$ must be divisible by $1+x+x^2(\mathrm{mod}\ p)$. When we cary out the calculation:

$$(8)\qquad Q_n(x)=(1+x+x^2)R_n(x)+S_n\cdot x^{(n-3)/2}\ ,\qquad (S_n\in \boldsymbol{Z})$$

$$(9)\qquad R_n(x)=c_{n,0}+c_{n,1}x+\cdots+c_{n,n-5}x^{n-5}$$

$$(10)\qquad c_{n,i}=c_{n,n-5-i}$$

then we get $S_n\neq 0$, because all roots of $P_n(x)=0$ are real. If $S_n\not\equiv 0(\mathrm{mod}\ p)$, then we get $B_{p-n}\equiv 0(\mathrm{mod}\ p)$.

Case 3. $|A|=6$.

From (1) we get $x+y+z\equiv 0(\mathrm{mod}\ p)$. Therefore if t is any one of A, then $A=\{t_1, t_2, \cdots, t_6\}=\{t, 1/t, -(t+1), -1/(t+1), -(t+1)/t, -t/(t+1)(\mathrm{mod}\ p)\}$. If $Q_n(t_1)\equiv\cdots\equiv Q_n(t_6)\equiv 0(\mathrm{mod}\ p)$, then $Q_n(x)$ must be divisible by $F(x)(\mathrm{mod}\ p)$ where $F(x)$ is given by

$$(11)\qquad \begin{aligned}F(x)&=(x-t)(x-1/t)\cdots(x+t/(t+1))\\&=1+3x+ax^2+(2a-5)x^3+ax^4+3x^5+x^6\end{aligned}$$

$$(12)\qquad a=(-t^6-3t^5+5t^3-3t-1)/(t^4+2t^3+t^2)\ .$$

We treat a as a variable and we carry out next calculation:

$$(13)\qquad \begin{aligned}Q_n(x)=F(x)\cdot T_n(x)+U_n\cdot(x^{(n-7)/2}+x^{(n+1)/2})+V_n\cdot(x^{(n-5)/2}+x^{(n-1)/2})\\+W_n\cdot x^{(n-3)/2},\ (U_n,\ V_n,\ W_n\in \boldsymbol{Z}[a])\end{aligned}$$

$$(14)\qquad T_n(x)=c_{n,0}+c_{n,1}x+\cdots+c_{n,n-9}x^{n-9}\ ,\qquad (c_{n,i}\in \boldsymbol{Z}[a])$$

$$(15)\qquad c_{n,i}=c_{n,n-9-i}\ .$$

If we use Krasner's method, we can prove easily that the greatest common divisor of U_n, V_n, W_n in $\boldsymbol{Q}[a]$ is one. Therefore multiplying suitable positive integer, we get

$$A_nU_n+B_nV_n+C_nW_n=D'_n\ , \qquad (D'_n\in \boldsymbol{Z},\ D'_n>0,\ A_n,\ B_n,\ C_n\in \boldsymbol{Z}[a])\ .$$

We define D_n as follows:

$$D_n=\min\{D'_n\in \boldsymbol{Z}\,|\,D'_n>0,\ D'_n=A_nU_n+B_nV_n+C_nW_n,\ A_n,\ B_n,\ C_n\in \boldsymbol{Z}[a]\}\ . \tag{16}$$

If $D_n\not\equiv 0(\mathrm{mod}\ p)$, then $U_n\not\equiv 0$ or $V_n\not\equiv 0$ or $W_n\not\equiv 0(\mathrm{mod}\ p)$. Therefore we get $B_{p-n}\equiv 0(\mathrm{mod}\ p)$.

§2. Result.

Using a computer, the author gets next results:

$Q_{11}(-2)=34082521=11\cdot 41\cdot 75571$
$Q_{13}(-2)=9363855865=5\cdot 7\cdot 13\cdot 20579903$
$Q_{15}(-2)=3547114323481=\mathrm{prime}$
$Q_{17}(-2)=1771884893993785=5\cdot 17\cdot 20845704635221$
$Q_{19}(-2)=1128511554418948441=7\cdot 19\cdot 916933\cdot 9253728769$
$S_{11}=1261501=683\cdot 1847$
$S_{13}=-151846331=-7\cdot 13\cdot 13\cdot 47\cdot 2731$
$S_{15}=25201039501=11\cdot 331\cdot 419\cdot 16519$
$S_{17}=-5515342166891=-23\cdot 401\cdot 13687\cdot 43691$
$S_{19}=1538993024478301=7\cdot 19\cdot 7691\cdot 8609\cdot 174763$
$D_{11}=11,\ D_{13}=13,\ D_{15}=1,\ D_{17}=17,\ D_{19}=19.$

All above prime factors p do not satisfy the criteria of Wieferich [2]:

$$2^{p-1}\equiv 1(\mathrm{mod}\ p^2)\ . \tag{17}$$

Therefore we get next theorem:

THEOREM. *Let p be an odd prime number. If $x^p+y^p+z^p=0$ has any integer solution such that $(xyz,\ p)=1$, then*

$$B_{p-n}\equiv 0(\mathrm{mod}\ p)\ , \qquad (n=3,\ 5,\ 7,\ 9,\ 11,\ 13,\ 15,\ 17,\ 19)\ .$$

From the values of D_n, we may conjecture that $D_n=n$ or one according as $n=$prime or not. If $n>19$, then $Q_n(-2)$ will become very large. Therefore it will be difficult to decompose $Q_n(-2)$ into prime factors.

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), 45-68.

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

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

Present Address:
DEPARTMENT OF MATHEMATICS
SOPHIA UNIVERSITY
KIOI-CHO, CHIYODA-KU, TOKYO 102