TOKYO J. MATH.
VOL. 1, No. 1, 1978

Some Criteria for the First Case of Fermat's Last Theorem

Dedicated to the memory of my friend Professor Masao NARITA

Paulo RIBENBOIM

Queen's University

(Communicated by Y. Kawada)

Introduction.

Let p be a prime. We say that the first case of Fermat's last theorem (FLT) fails for the exponent p when there exist integers x, y, z, such that $p \nmid xyz$ and $x^p+y^p+z^p=0$. We shall indicate some congruences which follow from the assumption that the FLT fails for p. These will involve the Bernoulli polynomials

$$B_n(X)=\sum_{j=0}^{n}\binom{n}{j}B_jX^{n-j} \quad (\text{for } n\geqq 0)\,.$$

We require also some values of the Bernoulli polynomials and its functional equation:

$$B_n(1-X)=(-1)^nB_n(X), \text{ and for } n \text{ even:}$$

$$B_n\left(\frac{1}{3}\right)=B_n\left(\frac{2}{3}\right)=\frac{(1-3^{n-1})B_n}{2\times 3^{n-1}}\,,$$

$$B_n\left(\frac{1}{6}\right)=B_n\left(\frac{5}{6}\right)=\frac{(1-2^{n-1})(1-3^{n-1})B_n}{2^n\times 3^{n-1}}\,.$$

E. Lehmer proved in [1] (1938), the following congruences (for $2\leqq n<p$):

$$\sum_{j=1}^{[p/n]}(p-jn)^{2k}\equiv\frac{n^{2k}}{2k+1}\left\{\frac{2k+1}{n}pB_{2k}-B_{2k+1}\left(\frac{s}{n}\right)\right\} \pmod{p^3}\,,$$

$$\sum_{j=1}^{[p/n]}j^{2k-1}\equiv\frac{1}{2k}\left\{B_{2k}\left(\frac{s}{n}\right)-B_{2k}\right\}-\frac{P}{n}B_{2k-1}\left(\frac{s}{n}\right) \pmod{p^2}\,,$$

where $p\equiv s \pmod{n}$, $1\leqq s\leqq n-1$. Schwindt proved in [4] (1933):

Received January 14, 1978

$$5\sum_{j=1}^{[p/3]}\frac{1}{j^2}\equiv\sum_{j=1}^{[p/6]}\frac{1}{j^2} \pmod p .$$

Vandiver proved in [6] (1925) that if the first case fails for p then $\sum_{j=1}^{[p/3]}(1/j^2)\equiv 0 \pmod p$. Genocchi showed in 1852 that if the first case fails for p then $B_{p-3}\equiv 0 \pmod p$. Similarly, Kummer showed that $B_{p-5}\equiv 0 \pmod p$ and Mirimanoff proved that $B_{p-7}\equiv B_{p-9}\equiv 0 \pmod p$. Mirimanoff has also proved that if the first case fails for p then the Fermat quotient $q_p(3)=(3^{p-1}-1)/p$ is congruent to 0 modulo p.

§ 1. Three lemmas.

It is notorious that very little is known about the values of Bernoulli polynomials $B_n(X)$ with odd index n. In this respect we prove:

LEMMA 1. *Let p be a prime, $p>3$. Then*

$$5B_{p-2}\left(\frac{1}{3}\right)\equiv B_{p-2}\left(\frac{1}{6}\right) \pmod p .$$

PROOF. Let $p\equiv s \pmod 3$, $p\equiv t \pmod 6$, with $s=1$ or 2 and $t=1$ or 5. Moreover if $t=1$ then $s=1$, and if $t=5$ then $s=2$. E. Lehmer proved in [1] (1938):

$$\sum_{j=1}^{[p/3]}(p-3j)^{p-3}\equiv\frac{3^{p-3}}{p-2}\left\{\frac{p-2}{3}pB_{p-3}-B_{p-2}\left(\frac{s}{3}\right)\right\} \pmod{p^2}$$

and

$$\sum_{j=1}^{[p/6]}(p-6j)^{p-3}\equiv\frac{6^{p-3}}{p-2}\left\{\frac{p-2}{6}pB_{p-3}-B_{p-2}\left(\frac{t}{6}\right)\right\} \pmod{p^2} .$$

But

$$(p-3j)^{p-3}\equiv\frac{1}{(p-3j)^2}\equiv\frac{1}{(3j)^2} \pmod p .$$

Since p does not divide the denominator of B_{p-3} then

$$\frac{1}{3^2}\sum_{j=1}^{[p/3]}\frac{1}{j^2}\equiv\frac{1}{2\times 3^2}B_{p-2}\left(\frac{s}{3}\right) \pmod p .$$

Similarly

$$\frac{1}{6^2}\sum_{j=1}^{[p/6]}\frac{1}{j^2}\equiv\frac{1}{2\times 6^2}B_{p-2}\left(\frac{t}{6}\right) \pmod p .$$

By Schwindt's lemma [4] (1933)

$$5\sum_{j=1}^{[p/3]}\frac{1}{j^2}\equiv\sum_{j=1}^{[p/6]}\frac{1}{j^2}\pmod{p},$$

then

$$5B_{p-2}\left(\frac{s}{3}\right)\equiv B_{p-2}\left(\frac{t}{6}\right)\pmod{p}.$$

If $t=1$ then $s=1$ and the lemma is proved. If $t=5$ then $s=2$. By the functional equation for the Bernoulli polynomials:

$$5B_{p-2}\left(\frac{1}{3}\right)=-5B_{p-2}\left(\frac{2}{3}\right)\equiv-5B_{p-2}\left(\frac{5}{6}\right)=B_{p-2}\left(\frac{1}{6}\right)\pmod{p}.$$

Q.E.D.

With the above congruence, we are able to obtain a new congruence for Bernoulli numbers:

LEMMA 2. *If* $p>3$ *then*

$$\sum_{j=0}^{p-2}(-1)^j(j+1)3^j(2^{j+1}-5)B_j\equiv 0\pmod{p}.$$

PROOF. We have

$$B_{p-2}\left(\frac{1}{3}\right)=\sum_{j=0}^{p-2}\binom{p-2}{j}\left(\frac{1}{3}\right)^{p-2-j}B_j\equiv\sum_{j=0}^{p-2}(-1)^j(j+1)3^{j+1}B_j\pmod{p},$$

because

$$\binom{p-2}{j}=\frac{(p-2)(p-3)\cdots(p-j-1)}{1\times 2\times\cdots\times j}\equiv(-1)^j(j+1)\pmod{p}$$

and

$$\frac{1}{3^{p-2-j}}\equiv 3^{j+1}\pmod{p}.$$

Similarly

$$B_{p-2}\left(\frac{1}{6}\right)=\sum_{j=0}^{p-2}\binom{p-2}{j}\left(\frac{1}{6}\right)^{p-2-j}B_j\equiv\sum_{j=0}^{p-2}(-1)^j(j+1)6^{j+1}B_j\pmod{p}.$$

By Lemma 1,

$$5\sum_{j=0}^{p-2}(-1)^j(j+1)3^{j+1}B_j\equiv\sum_{j=0}^{p-2}(-1)^j(j+1)6^{j+1}B_j\pmod{p},$$

hence

$$\sum_{j=0}^{p-2}(-1)^j(j+1)3^j(2^{j+1}-5)B_j\equiv 0 \pmod{p}.$$

Q.E.D.

We shall also require:

LEMMA 3. *If* $B_{p-(2n+1)}\equiv 0 \pmod{p}$ *where* $1\leqq n\leqq(p-3)/2$, *then*

$$\sum_{j=1}^{[p/3]}\frac{1}{j^{2n+1}}\equiv 0 \pmod{p}$$

and

$$\sum_{j=1}^{[p/6]}\frac{1}{j^{2n+1}}\equiv 0 \pmod{p}.$$

PROOF. According to E. Lehmer's congruence, we have

$$\sum_{j=1}^{[p/3]}\frac{1}{j^{2n+1}}\equiv\sum_{j=1}^{[p/3]}j^{p-2n-2}\equiv\frac{1}{p-2n-1}\left\{B_{p-2n-1}\left(\frac{s}{3}\right)-B_{p-2n-1}\right\} \pmod{p},$$

since

$$B_{p-2n-2}\left(\frac{s}{3}\right)=\sum_{i=0}^{p-2n-2}\binom{p-2n-2}{i}\left(\frac{s}{3}\right)^{p-2n-2-i}B_i$$

is p-integral, by the Von Staudt and Clausen's theorem. By hypothesis $B_{p-(2n+1)}\equiv 0 \pmod{p}$, hence

$$\sum_{j=1}^{[p/3]}\frac{1}{j^{2n+1}}\equiv\frac{1}{(p-2n-1)}B_{p-2n-1}\left(\frac{s}{3}\right)\equiv\frac{(1-3^{p-2n-2})B_{p-2n-1}}{(p-2n-1)\times 2\times 3^{p-2n-2}}\equiv 0 \pmod{p}.$$

Similarly, we prove the other congruence. Q.E.D.

§ 2. The Criteria.

We prove:

PROPOSITION 1. *If the first case of* FLT *fails for the exponent* p, *then*:

(1) $$B_{p-2}\left(\frac{1}{3}\right)\equiv 0 \pmod{p},\quad B_{p-2}\left(\frac{1}{6}\right)\equiv 0 \pmod{p}$$

(2) $$2\sum_{j=1}^{[p/3]}j^{p-3}\equiv B_{p-2}\left(\frac{s}{3}\right) \pmod{p^2}$$

and

$$2\sum_{j=1}^{[p/6]} j^{p-3} \equiv B_{p-2}\left(\frac{t}{6}\right) \pmod{p^2},$$

where $s=1$ *or* 2, $t=1$ *or* 5 *and* $p\equiv s \pmod 3$, $p\equiv t \pmod 6$.

PROOF.

(1) We have

$$(p-3j)^{p-3}=(3j-p)^{p-3}\equiv(3j)^{p-3}-(p-3)p(3j)^{p-4}$$
$$\equiv(3j)^{p-3}+3p(3j)^{p-4} \pmod{p^2}.$$

Also

$$\frac{1}{2-p}\equiv\frac{1}{2}+\frac{p}{4} \pmod{p^2}.$$

By Lehmer's congruence, we have

$$\sum_{j=1}^{[p/3]}(p-3j)^{p-3}\equiv\frac{3^{p-3}}{p-2}\left\{\frac{p-2}{3}pB_{p-3}-B_{p-2}\left(\frac{s}{3}\right)\right\}\equiv\frac{3^{p-3}}{2-p}B_{p-2}\left(\frac{s}{3}\right) \pmod{p^2},$$

because, by Gennocchi's theorem $B_{p-3}\equiv 0 \pmod p$ since the first case fails for p. Hence

$$3^{p-3}\sum_{j=1}^{[p/3]} j^{p-3}+3^{p-3}p\sum_{j=1}^{[p/3]} j^{p-4}\equiv\frac{3^{p-3}}{2}B_{p-2}\left(\frac{s}{3}\right)+\frac{3^{p-3}}{4}pB_{p-2}\left(\frac{s}{3}\right) \pmod{p^2}.$$

By Vandiver's criterion (1925), we have:

$$\sum_{j=1}^{[p/3]} j^{p-3}\equiv\sum_{j=1}^{[p/3]}\frac{1}{j^2}\equiv 0 \pmod p.$$

Hence

$$B_{p-2}\left(\frac{s}{3}\right)\equiv 0 \pmod p.$$

Since $s=1$ or 2, by the functional equation for the Bernoulli polynomial, we have $B_{p-2}(1/3)\equiv 0 \pmod p$ in all cases. By Lemma 1

$$B_{p-2}\left(\frac{1}{6}\right)\equiv 0 \pmod p.$$

(2) We use again Lehmer's formula. Noting that

$$B_{p-4}\left(\frac{s}{3}\right)=\sum_{j=0}^{p-4}\binom{p-4}{j}\left(\frac{s}{3}\right)^{p-4-j}B_j$$

is p-integral then

$$\sum_{j=1}^{[p/3]} j^{p-4} \equiv \frac{1}{p-3}\left\{B_{p-3}\left(\frac{s}{3}\right)-B_{p-3}\right\} \pmod{p}.$$

Since $B_{p-3}\equiv 0 \pmod{p}$ then

$$\sum_{j=1}^{[p/3]} j^{p-4} \equiv -\frac{1}{3}B_{p-3}\left(\frac{s}{3}\right) = -\frac{(1-3^{p-4})B_{p-3}}{2\times 3^{p-3}} \equiv 0 \pmod{p}.$$

Therefore, from part 1 and a previous congruence, we have:

$$2\sum_{j=1}^{[p/3]} j^{p-3} \equiv B_{p-2}\left(\frac{s}{3}\right) \pmod{p^2}.$$

In the same way, we show that

$$2\sum_{j=1}^{[p/6]} j^{p-3} \equiv B_{p-2}\left(\frac{t}{6}\right) \pmod{p^2}.$$

Finally, we prove:

PROPOSITION 2. *If the first case of* FLT *fails for the exponent p, then*:

$$\sum_{j=1}^{[p/3]} \frac{1}{j^r} \equiv 0 \pmod{p}$$

and

$$\sum_{j=1}^{[p/6]} \frac{1}{j^r} \equiv 0 \pmod{p}$$

for $r=1, 3, 5, 7, 9$.

PROOF. In 1905 Lerch [2] proved that if $p>3$ then

$$-\frac{2}{3}\sum_{j=1}^{[p/3]} \frac{1}{j} \equiv q_p(3) \pmod{p}$$

where

$$q_p(3)=\frac{3^{p-1}-1}{p}.$$

By Mirimanoff's theorem (1910) if the first case fails for p then $q_p(3)\equiv 0 \pmod{p}$. Hence $\sum_{j=1}^{[p/3]}(1/j)\equiv 0 \pmod{p}$. In 1938, E. Lehmer proved that necessarily $\sum_{j=1}^{[p/6]}(1/j)\equiv 0 \pmod{p}$.

Kummer and Mirimanoff proved that if the first case fails for p then

$B_{p-3}\equiv 0 \pmod p$, $B_{p-5}\equiv 0 \pmod p$, $B_{p-7}\equiv 0 \pmod p$ and $B_{p-9}\equiv 0 \pmod p$.

By Lemma 3, we deduce that $\sum_{j=1}^{[p/3]}(1/j^r)\equiv 0 \pmod p$ and $\sum_{j=1}^{[p/6]}(1/j^r)\equiv 0 \pmod p$, for $j=3, 5, 7, 9$. Q.E.D.

References

[1] E. LEHMER, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, Annals of Math., **39** (1938), 350-359.

[2] M. LERCH, Zur Theorie des Fermatschen Quotienten $(a^{p-1}-1)/p=q(a)$, Math. Annalen, **60** (1905), 471-490.

[3] H. RADEMACHER, Topics in Analytic Number Theory, Springer Verlag, Berlin, 1973.

[4] H. SCHWINDT, Eine Bemerkung zu einem Kriterium von H. S. Vandiver, Jahresber. Deutscher Math. Verein., **43** (1933/4), 229-232.

[5] H. S. VANDIVER and G. E. WAHLIN, Algebraic Numbers II, Report n° 62, 1928, National Research Council, U.S.A., Reprinted in Algebraic Numbers, by L. E. Dickson et al., Chelsea Publ. Co., Bronx, N.Y., 1967.

[6] H. S. VANDIVER, A new type of criteria for the first case of Fermat's last the theorem, Annals of Math., **26** (1925), 88-94.

Present Address;
QUEEN'S UNIVERSITY
KINGSTON, ONTARIO
CANADA