CONGRUENCES MOD p^n FOR THE BERNOULLI NUMBERS

A. Simalarides
196 Kifissias Str., Kifissia 14562, Athens, Greece
(*Submitted September 1996*)

1. INTRODUCTION

Let p be a prime. In 1889 Voronoi proved the congruence

$$(a-a^{p-2k})\frac{B_{2k}}{2k}\equiv\sum_{s=1}^{p-1}\left[\frac{sa}{p}\right]s^{2k-1} \pmod{p}, \tag{1}$$

where k, a are positive integers such that p does not divide a and $p-1$ does not divide $2k$; B_{2k} is the $2k^{\text{th}}$ Bernoulli number. More general versions of this congruence can be found in [6] or [3]. Following Wagstaff, denote congruence (1) also by the symbol $\{a\}$. Adding together congruences $\{2\}$, $\{3\}$, and $-\{4\}$, we obtain the congruence

$$\{2\}+\{3\}-\{4\}$$

which, after some obvious cancellations in the right member, takes the form

$$(2^{p-2k}+3^{p-2k}-4^{p-2k}-1)\frac{B_{2k}}{4k}\equiv\sum_{p/4<s<p/3}s^{2k-1} \pmod{p}, \tag{2}$$

provided that $p>4$. Several such identities are also obtainable in a way analogous to that shown above by using suitable variations of parameter a. Several authors used formulas of this type to test regularity via computer. The best result in this direction is the following one, due to Tanner and Wagstaff [5], which is valid for all primes $p>10$,

$$\begin{aligned}(2^{p-2k}+9^{p-2k}-10^{p-2k}-1)\frac{B_{2k}}{4k}&\equiv(1+2^{2k-1}+3^{2k-1}+4^{2k-1})\sum_{\frac{p}{10}<s<\frac{13p}{120}}s^{2k-1}\\&+(1+2^{2k-1}+3^{2k-1}+4^{2k-1}+12^{2k-1})\sum_{\frac{13p}{120}<s<\frac{p}{9}}s^{2k-1}\\&-3^{2k-1}\sum_{\frac{2p}{9}<s<\frac{7p}{30}}s^{2k-1}-(2^{2k-1}+6^{2k-1})\sum_{\frac{5p}{18}<s<\frac{17p}{60}}s^{2k-1}\\&-2^{2k-1}\sum_{\frac{17p}{60}<s<\frac{3p}{10}}s^{2k-1}-(2^{2k-1}+4^{2k-1}+12^{2k-1})\sum_{\frac{7p}{18}<s<\frac{47p}{120}}s^{2k-1}\\&-(2^{2k-1}+4^{2k-1})\sum_{\frac{47p}{120}<s<\frac{2p}{5}}s^{2k-1} \pmod{p}.\end{aligned} \tag{3}$$

In formula (3), the sums in the right member contain a total of about $p/18$ terms [formula (2) contains about $p/12$ terms while formula (1) contains $(p-1)/2$ terms for $a=2$]. All the applications of these formulas concerning Fermat's Last Theorem are now mainly of historical interest after Wiles's proof [8] of FLT. There are congruences of various types for the Bernoulli numbers. Recent results on congruences for Bernoulli numbers of higher order can be found in [2].

We shall prove the following analog of formula (1).

Theorem 1: Let χ be a primitive Dirichlet character with modulus $m \ge 2$. If $a \ge 2$ is an integer such that m does not divide a, then

$$\sum_{s=1}^{m-1}\left[\frac{sa}{m}\right]\chi(s) = \begin{cases} 0 & \text{if } \chi \text{ is even,} \\ -\dfrac{\overline{\chi}(a)-a}{\overline{\chi}(2)-2}\displaystyle\sum_{s=1}^{[m/2]}\chi(s) & \text{if } \chi \text{ is odd,} \end{cases} \tag{4}$$

where the bar means complex conjugation.

The proof of Theorem 1 will be given in Section 2. Formula (4) can be written, equivalently, in the form

$$\sum_{s=1}^{m-1}\left[\frac{sa}{m}\right]\chi(s) = \begin{cases} 0 & \text{if } \chi \text{ is even,} \\ \dfrac{a-\overline{\chi}(a)}{m}\displaystyle\sum_{s=1}^{m-1}s\chi(s) & \text{if } \chi \text{ is odd,} \end{cases} \tag{5}$$

because of the formula

$$\sum_{s=1}^{m-1}s\chi(s) = \frac{m}{\overline{\chi}(2)-2}\sum_{s=1}^{[m/2]}\chi(s), \tag{6}$$

which is valid for an odd primitive character χ.

We use formula (5) to obtain p^n-divisibility criteria for Bernoulli numbers of the form

$$B_{(2k-1)p^n+1}, \quad k = 1, 2, \ldots, \frac{p-3}{2}.$$

Criteria of this type are still of interest because of their connection with the invariants of the irregular class group of a properly irregular cyclotomic field [7] (cf. also [4], p. 189). Assume now that $m = p$, an odd prime. Let ψ be the character defined as the p-adic limit

$$\psi(s) = \lim_{n\to\infty} s^{p^n}$$

for every s prime to p. All the values of ψ belong to $\mathbb{Z}_p$, the ring of p-adic integers. Moreover,

$$\psi(s) \equiv s^{p^{n-1}} \pmod{p^n}, \quad n \ge 1.$$

For an odd character, we have $\chi = \psi^{2k-1}$, for some $k \ge 1$, and

$$\chi(s) \equiv s^{(2k-1)p^{n-1}} \pmod{p^n},$$

$$\overline{\chi}(s) \equiv s^{-p^{n-1}(2k-1)} \equiv s^{p^{n-1}(p-1)-p^{n-1}(2k-1)} \equiv s^{p^{n-1}(p-2k)} \pmod{p^n}.$$

Theorem 2: Let p be a prime >3. If a is an integer such that p does not divide a, then

$$[a - a^{p^{n-1}(p-2k)}]B_{(2k-1)p^n+1} \equiv \sum_{s=1}^{p-1}\left[\frac{sa}{p}\right]s^{(2k-1)p^{n-1}} \pmod{p^n}, \tag{7}$$

for every $k \ge 1$ such that $p-1$ does not divide $2k$.

Proof: We consider the n^{th} Bernoulli polynomial

$$B_n(x)=\sum_{j=0}^{n}\binom{n}{j}B_jx^{n-j},\ \ n\geq 1.$$

Then, for the odd character $\chi=\psi^{2k-1}$, we have

$$\begin{aligned}\sum_{s=1}^{p-1}s\chi(s)&\equiv\sum_{s=1}^{p}s^{(2k-1)p^n+1}\equiv\frac{B_{(2k-1)p^n+2}(p)-B_{(2k-1)p^n+2}}{(2k-1)p^n+2}\\&\equiv pB_{(2k-1)p^n+1}+\frac{[(2k-1)p^n+1](2k-1)p^n}{3!}p^3B_{(2k-1)p^n-1}+\cdots\\&\equiv pB_{(2k-1)p^n+1}\ \ (\operatorname{mod} p^{n+1}).\end{aligned}$$

Since $p-1$ does not divide $2k$, we obtain the congruence

$$\frac{1}{p}\sum_{s=1}^{p-1}s\chi(s)\equiv B_{(2k-1)p^n+1}\ \ (\operatorname{mod} p^n),$$

which, together with Theorem 1 and relation (5), yields the sought result.

For $n=1$, congruence (7) reduces to congruence (1) since

$$B_{(2k-1)p+1}=[(2k-1)p+1]\frac{B_{(2k-1)p+1}}{(2k-1)p+1}\equiv\frac{B_{2k}}{2k}\ \ (\operatorname{mod} p)$$

because of Kummer's congruence.

We can prove, using exactly analogous techniques and starting from (7), a p^n-analog of congruence (3). Because of the obvious analogy between the proofs, the sought result follows simply by replacing expressions of the form

$$a^{p-2k},\ a^{2k-1},\ s^{2k-1},\ \frac{B_{2k}}{2k}$$

in congruence (3) with the respective expressions

$$a^{p^{n-1}(p-2k)},\ a^{(2k-1)p^{n-1}},\ s^{(2k-1)p^{n-1}},\ B_{(2k-1)p^n+1}.$$

The following theorem then follows.

Theorem 3: Let p be an odd prime >10, $k\geq 1$, $p-1$ does not divide $2k$ and $n\geq 1$. Then

$$\begin{aligned}&\frac{2^{(p-2k)p^{n-1}}+9^{(p-2k)p^{n-1}}-10^{(p-2k)p^{n-1}}-1}{2}B_{(2k-1)p^n+1}\\&\equiv[1+2^{(2k-1)p^{n-1}}+3^{(2k-1)p^{n-1}}+4^{(2k-1)p^{n-1}}]\sum_{\frac{p}{10}<s<\frac{13p}{120}}s^{(2k-1)p^{n-1}}\\&\quad+[1+2^{(2k-1)p^{n-1}}+3^{(2k-1)p^{n-1}}+4^{(2k-1)p^{n-1}}+12^{(2k-1)p^{n-1}}]\sum_{\frac{13p}{120}<s<\frac{p}{9}}s^{(2k-1)p^{n-1}}\\&\quad-3^{(2k-1)p^{n-1}}\sum_{\frac{2p}{9}<s<\frac{7p}{30}}s^{(2k-1)p^{n-1}}-[2^{(2k-1)p^{n-1}}+6^{(2k-1)p^{n-1}}]\sum_{\frac{5p}{18}<s<\frac{17p}{60}}s^{(2k-1)p^{n-1}}\end{aligned}$$

$$-2^{(2k-1)p^{n-1}}\sum_{\frac{17p}{60}<s<\frac{3p}{10}} s^{(2k-1)p^{n-1}} - [2^{(2k-1)p^{n-1}} + 4^{(2k-1)p^{n-1}} + 12^{(2k-1)p^{n-1}}]\sum_{\frac{7p}{18}<s<\frac{47p}{120}} s^{(2k-1)p^{n-1}}$$

$$-[2^{(2k-1)p^{n-1}} + 4^{(2k-1)p^{n-1}}]\sum_{\frac{47p}{120}<s<\frac{2p}{5}} s^{(2k-1)p^{n-1}} \pmod{p^n}.$$

The congruence contains in the right member $p/18$ terms only.

2. PROOF OF THEOREM 1

At first, we note that, obviously,

$$-\sum_{s=1}^{m-1}\left[\frac{sa}{m}\right]\chi(s) = \sum_{j=1}^{a}\sum_{s=0}^{[jm/a]}\chi(s). \tag{8}$$

For integer j, $0 < j \le a$, define

$$\Phi(x) = \begin{cases} \frac{1}{2} & \text{if } x = 0 \text{ or } 2\pi j/a, \\ 1 & \text{if } 0 < x < 2\pi j/a, \\ 0 & \text{if } 2\pi j/a < x < 2\pi, \end{cases}$$

and continue $\Phi(x)$ periodically with period 2π over the real numbers. The function $\Phi(x)$ has the Fourier expansion

$$\Phi(x) = \sum_{n=-\infty}^{\infty} c_n e^{inx} \quad (i = \sqrt{-1}),$$

where

$$c_n = \frac{1}{2\pi}\int_0^{2\pi}\Phi(x)e^{-inx}dx = \frac{i}{2\pi n}(e^{-\frac{2\pi ijn}{a}} - 1).$$

First, we assume that $a < m$. Then

$$\begin{aligned}\sum_{s=0}^{[jm/a]}\chi(s) &= \sum_{s=1}^{m-1}\chi(s)\,\Phi\left(\frac{2\pi s}{m}\right) \\ &= \frac{i}{2\pi}\sum_{s=1}^{m-1}\chi(s)\sum_{n=-\infty}^{\infty}\frac{(e^{-\frac{2\pi ijn}{a}} - 1)e^{\frac{2\pi is}{m}n}}{n} \\ &= \frac{i}{2\pi}\sum_{n=-\infty}^{\infty}\frac{e^{-\frac{2\pi ijn}{a}} - 1}{n}\sum_{s=1}^{m-1}\chi(s)e^{\frac{2\pi is}{m}n} \\ &= \frac{\tau(\chi)i}{2\pi}\sum_{n=-\infty}^{\infty}\frac{(e^{-\frac{2\pi ijn}{a}} - 1)\overline{\chi}(n)}{n},\end{aligned}$$

where

$$\tau(\chi) = \sum_{s=1}^{m-1}\chi(s)e^{\frac{2\pi is}{m}}.$$

As a consequence,

$$\sum_{j=1}^{a}\sum_{s=0}^{[jm/a]}\chi(s)=\frac{\tau(\chi)i}{2\pi}\sum_{n=-\infty}^{\infty}\frac{\overline{\chi}(n)}{n}\left(\sum_{j=1}^{a}e^{-\frac{2\pi ijn}{a}}-a\right)$$
$$=\frac{\tau(\chi)i}{2\pi}\sum_{n=-\infty}^{\infty}\frac{\overline{\chi}(n)}{n}\sum_{j=1}^{a}e^{-\frac{2\pi ijn}{a}}-\frac{\tau(\chi)ia}{2\pi}\sum_{n=-\infty}^{\infty}\frac{\overline{\chi}(n)}{n}.$$

Since

$$\sum_{j=1}^{a}e^{-\frac{2\pi ijn}{a}}=\begin{cases}a & \text{if } n\equiv 0 \pmod{a},\\ 0 & \text{if } n\not\equiv 0 \pmod{a},\end{cases}$$

it follows that

$$\sum_{j=1}^{a}\sum_{s=0}^{[jm/a]}\chi(s)=\frac{\tau(\chi)i}{2\pi}\sum_{n=-\infty}^{\infty}\frac{\overline{\chi}(na)}{na}a-\frac{\tau(\chi)i}{2\pi}\sum_{n=-\infty}^{\infty}\frac{\overline{\chi}(n)}{n}$$
$$=\frac{\tau(\chi)i}{2\pi}(\overline{\chi}(a)-a)\sum_{n=-\infty}^{\infty}\frac{\overline{\chi}(n)}{n}.$$

For even χ, the last infinite sum is equal to zero while, for odd χ, it is equal to $2L(1,\overline{\chi})$. In view of the formula (cf. [1], p. 336)

$$L(1,\overline{\chi})=\frac{\pi i}{(2-\overline{\chi}(2))\,\tau(x)}\sum_{s=1}^{[m/2]}\chi(s)$$

and relation (8), it follows that

$$\sum_{s=1}^{m-1}\left[\frac{sa}{m}\right]\chi(s)=-\frac{\overline{\chi}(a)-a}{\overline{\chi}(2)-2}\sum_{s=1}^{[m/2]}\chi(s) \tag{9}$$

for $a<m$. It remains to prove the theorem for $a>m$. Then $a=a_1+mt$, where a_1 and t are integers and $0<a_1<m$. Also m does not divide a_1. We have

$$\sum_{s=1}^{m-1}\left[\frac{sa}{m}\right]\chi(s)=\sum_{s=1}^{m-1}\left[\frac{sa_1}{m}+st\right]\chi(s)$$
$$=\sum_{s=1}^{m-1}\left[\frac{sa_1}{m}\right]\chi(s)+t\sum_{s=1}^{m-1}s\chi(s).$$

The last expression is zero for even χ. For odd χ we have, in view of (6) and (9),

$$\sum_{s=1}^{m-1}\left[\frac{sa}{m}\right]\chi(s)=-\frac{\overline{\chi}(a_1)-a_1}{\overline{\chi}(2)-2}\sum_{s=1}^{[m/2]}\chi(s)+\frac{tm}{\overline{\chi}(2)-2}\sum_{s=1}^{[m/2]}\chi(s)$$
$$=-\frac{\overline{\chi}(a)-(a_1+tm)}{\overline{\chi}(2)-2}\sum_{s=1}^{[m/2]}\chi(s)$$
$$=-\frac{\overline{\chi}(a)-a}{\overline{\chi}(2)-2}\sum_{s=1}^{[m/2]}\chi(s),$$

which proves the theorem for $a>m$.

REFERENCES

1. Z. I. Borevich & I. R. Shafarevich. *Number Theory.* New York: Academic Press, 1966.
2. F. T. Howard. "Congruences and Recurrences for Bernoulli Numbers of Higher Order." *The Fibonacci Quarterly* **32.4** (1994):316-28.
3. K. Ireland & M. Rosen. *A Classical Introduction to Modern Number Theory.* New York and Berlin: Springer-Verlag, 1982.
4. P. Ribenboim. *13 Lectures on Fermat's Last Theorem.* New York and Berlin: Springer-Verlag, 1979.
5. J. W. Tanner & S. S. Wagstaff. "New Congruences for the Bernoulli Numbers." *Math. of Comp.* **48** (1987):341-50.
6. J. V. Uspensky & M. A. Heaslet. *Elementary Number Theory.* New York: McGraw-Hill, 1939.
7. H. S. Vandiver. "On the Composition of the Group of Ideal Classes in a Properly Irregular Cyclotomic Field." *Monatsh. f. Math. u. Phys.* **48** (1939):369-80.
8. A. Wiles. "Modular Elliptic Curves and Fermat's Last Theorem." *Annals of Math.* **142** (1995):443-551.

AMS Classification Number: 11B68

❖❖❖