# ON GENERAL METHODS FOR OBTAINING CONGRUENCES INVOLVING BERNOULLI NUMBERS

H. S. VANDIVER

In a previous article[1] the writer proved a theorem concerning congruences in rings. This was employed to obtain various congruences involving the Bernoulli numbers, in particular the relation[2]

$$h_1^{n_1}h_2^{n_2}\cdots h_s^{n_s}(\beta_1 h_1^{p-1}+\beta_2 h_2^{p-1}+\cdots+\beta_s h_s^{p-1})^i \equiv 0 \pmod{p^i, p^{n_1-1}, p^{n_2-1}, \cdots, p^{n_s-1}},$$

$n_i \not\equiv 0 \pmod{p-1}$; $p$ a prime; $i=1, 2, \cdots, s$; $\beta_1, \beta_2, \cdots, \beta_s$ are integers such that

$$\sum_{i=1}^{s}\beta_i \equiv 0 \pmod{p},$$

and the left-hand member is expanded in full employing the multinomial theorem, and $b_t/t$ is substituted for $h_i^t$ in the result, $i=1, 2, \cdots, s$, with the $b$'s defined by the following recursion formula:

$$(b+1)^n = b_n;\ n>1;\ b_0 = 1.$$

I shall now discuss other methods for obtaining congruences involving the $b$'s. The proofs will be indicated only. We have the following result.

THEOREM I. *If $a_1, a_2, \cdots, a_s$; $x_1, x_2, \cdots, x_s$ are integers with the $x$'s positive and the congruences*

$$a_1C_{x_1,i}+a_2C_{x_2,i}+\cdots+a_sC_{x_s,i} \equiv 0 \pmod{p^{k-i}},$$

*$i=0, 1, \cdots, k-1$; $C_{x,a}=0$ when $a>x$, are all satisfied, then*

$$\sum_{i=1}^{s}\frac{a_i b_{n+(p-1)x_i}}{n+(p-1)x_i} \equiv 0 \pmod{p^k, p^{n-1}}.$$

The proof of this depends on the formula

$$\frac{n^{2i}-1}{2i}b_{2i} \equiv \sum_{a=1}^{p^\alpha-1} y_a a^{2i-1} \pmod{p^\alpha}$$

for $p>3$, and noting that we can write

[1] This Bulletin, vol. 43 (1937), pp. 418–423.

[2] Here (mod $p^i, \cdots, p^{n_s-1}$) means (mod $(p^i, \cdots, p^{n_s-1})$).

$$a^{n+(p-1)t} = a^n(1 + pq(a))^t,$$

where $q(a) = (a^{p-1}-1)/p$, and expanding the right-hand member.

By means of this theorem we may set up numerous congruences such as the following, for $p>3$, $n \not\equiv 0 \pmod{p-1}$:

$$B'_{n+p\mu} - pB'_{n+\mu} + (p-1)B'_n \equiv 0 \pmod{p^3},$$
$$xB'_{n+py\mu} - yB'_{n+px\mu} + (y-x)B'_n \equiv 0 \pmod{p^4},$$

where $B_a = (-1)^{a-1}b_{2a}$; $B'_a = (-1)^a B_a/a$; and $x$ and $y$ are any positive or zero integers with $\mu = (p-1)/2$.

Beeger[3] proved the interesting congruence

$$(-1)^{i-1}\frac{B_{n+m\mu}}{2n+2m\mu} \equiv \sum_{s=1}^{i}(-1)^{s-1+(m-s+1)\mu} \cdot C_{m,s-1}C_{m-s,i-s}\frac{B_{n+(s-1)\mu}}{2n+2(s-1)\mu}$$

modulo $p^i$, where $m \geqq i$, $i<2n-1$, $2n \not\equiv 0 \pmod{p-1}$. Another proof of this, from Theorem I, follows if we can show that

$$\sum_{s=1}^{i}(-1)^{s-1}C_{m,s-1}C_{m-s,i-s}C_{s-1,k} + (-1)^i C_{m,k} \equiv 0 \pmod{p^{i-k}},$$

$k=0, 1, 2, \cdots, i-1$. This is possible, as is seen on expanding the expression

$$(y-z)^n = (x+y-(x+z))^n,$$

in which $x$, $y$ and $z$ are indeterminates, and equating the coefficients of each of the terms involving $x$ to zero, and then applying the known relation $C_{n+1,a} = C_{n,a} + C_{n,a-1}$. Let

$$n_1, n_2, \cdots, n_s, \qquad n_i < m, \tag{1}$$

form a repetitive set modulo $m$; that is, there exists an $n$ ($\not\equiv 1$) called a multiplier of the set, such that

$$nn_1, nn_2, \cdots, nn_s$$

are congruent modulo $m$ to the set (1) in some order.[4] Consider the set

$$(y_{ak}m - n_a k)/n \tag{2}$$

[3] This Bulletin, vol. 44 (1938), pp. 684–686.

[4] The writer employed the term conjugate set for this type of set in the Annals of Mathematics, (2), vol. 18 (1917), p. 106, but this does not agree with the terminology of group theory. Concerning the concept of repetitive sets in a semi-group see Proceedings of the National Academy of Sciences, vol. 23 (1937), pp. 554–555.

where $a=1, 2, \cdots, s$; $m$, $n$ and $k$ are prime each to each, $n$ and $k$ are multipliers of (1),

$$y_{ak} \equiv -n_a k/m \pmod{n},$$

and $y_{ak}$ is further selected so that it is the least integer satisfying the above congruence which also makes

$$y_{ak}m - n_a k > 0.$$

Then the set (2) may be shown to give the set (1) in some order. For $k=1$ this was obtained in a bit different form on page 110 of the article just cited, and proceeding as in that paper we obtain generalizations of most of the results therein. In particular by using the repetitive set $1, 2, \cdots, m-1$, modulo $m$, we find, if $i<p-1$,

$$b_i \frac{n^i - (-1)^i}{ik^{i-1}} \equiv \sum_{a=1}^{m-1} y_{ak}a^{i-1} \pmod{m}.$$

The set (2) having the multiplicative property of repetitive sets, it is a bit curious then that we may extend some of these ideas to integers in arithmetic progression. Consider the expressions $r<m$; $p$ prime;

$$\frac{y_t p + mt + r}{n}; \qquad t = 0, 1, \cdots, p-1; \tag{3}$$

where $y_t$ is selected so that each of these is an integer and also so that each is of the form $r \pmod{m}$. Suppose that $p \equiv s \pmod{m}$. Then if $(m, n)=1$; $n>m$; $(nr-r+s, m)=1$; then the maximum value for $y_t$ is $mn-n-1<m(n-1)$ so that each of these is less than $pm$; hence they are the integers $mt+r$; $t=0, 1, \cdots, p-1$, in some order. This property of the set (3) yields a number of results including the relation

$$\frac{n^i - 1}{i}(mb + r)^i \equiv \sum_{t=0}^{p-1} y_t(mt + r)^{i-1} \pmod{p},$$

with the restrictions on $m$, $n$ and $p$ mentioned above and also $i \not\equiv 1 \pmod{p-1}$.

UNIVERSITY OF TEXAS