A DIVISIBILITY PROPERTY OF THE BERNOULLI POLYNOMIALS

L. CARLITZ

1. Put

$$(1.1)\qquad \frac{xe^{xu}}{e^x-1}=\sum_{m=0}^{\infty}B_m(u)\frac{x^m}{m!},\qquad B_m=B_m(0).$$

The writer has shown [1, §4] that if $(p-1)p^r \mid m$, $m>0$, then

$$(1.2)\qquad B_m+\frac{1}{p}-1\equiv 0 \pmod{p^r}\qquad (p\geqq 3);$$

indeed if $m=t(p-1)p^r$, then

$$(1.3)\qquad \sigma_m=\frac{1}{p^r}\left(B_m+\frac{1}{p}-1\right)\equiv tw_p \pmod{p},$$

where $w_p=((p-1)!+1)/p$. (For the case $r=0$, see [2, p. 354].) It was stated that

$$(1.4)\qquad \sigma_m\equiv p^{1-h}\sum_{a=1,\,p\nmid a}^{ph}q(a) \pmod{p^{2h}}\qquad (p>3),$$

where $h=[(r+2)/3]$ and $q(a)=(a^{(p-1)p^r}-1)/p^{r+1}$.

In the present note we first extend these results to $B_m(u)$, where the rational number u is integral (mod p). Secondly we derive the corresponding divisibility property for $B_m^{(k)}(u)$ defined by [3, chap. 6]

$$(1.5)\qquad \left(\frac{x}{e^x-1}\right)^k e^{xu}=\sum_{m=0}^{\infty}B_m^{(k)}(u),\qquad B_m^{(k)}=B_m^{(k)}(0),$$

where k is restricted to the range $1\leqq k\leqq p-1$.

2. We recall that

$$(2.1)\qquad \frac{1}{m+1}\left(B_{m+1}(u+t)-B_{m+1}(u)\right)=\sum_{s=0}^{t-1}(u+s)^m,$$

also

$$(2.2)\qquad B_m(u+t)=\sum_{s=0}^{m}\binom{m}{s}t^sB_{m-s}(u).$$

Presented to the Society, February 23, 1952; received by the editors November 21, 1951.

Now for $p\nmid u+s$, put

$$(u+s)^{(p-1)p^r} = 1 + p^{r+1}q(u+s),$$

from which it follows that

$$(2.3)\qquad (u+s)^m \equiv 1 + tp^{r+1}q(u+s) \pmod{p^{2r+2}} \qquad (m = t(p-1)p^r).$$

If we put

$$S_m(p^h) = \sum_{s=0}^{p^h-1} (u+s)^m, \qquad S'_m(p^h) = \sum_{s=0,\, p\nmid u+s}^{p^h-1} (u+s)^m,$$

where $h \geqq 1$, it is evident that

$$(2.4)\qquad S_m(p^h) \equiv S'_m(p^h) \pmod{p^{2r+2}},$$

since $m \geqq (p-1)p^r \geqq 2(r+1)$. In the next place it follows from (2.3) that

$$(2.5)\qquad S'_m(p^h) \equiv p^h - p^{h-1} + tp^{r+1}R(p^h) \pmod{p^{2r+2}},$$

where

$$R(p^h) = \sum_{s=0,\, p\nmid u+s}^{p^h-1} q(u+s).$$

By (2.1) and (2.2) we see that

$$(2.6)\qquad \begin{aligned} S_m(p^h) &= \frac{1}{m+1}\sum_{s=1}^{m+1}\binom{m+1}{s} p^{hs}B_{m+1-s}(u) \\ &= \sum_{s=0}^{m} \frac{1}{s+1}\binom{m}{s} p^{h(s+1)}B_{m-s}(u). \end{aligned}$$

Now let $p \geqq 3$; then it is easily verified that for $s \geqq 1$ each term in the extreme right member of (2.6) is divisible by at least p^{r+2h}. Hence by (2.4), (2.5), (2.6) we have

$$(2.7)\qquad p^hB_m(u) + p^{h-1} - p^h \equiv tp^{r+1}R(p^h) \pmod{p^{2r+2},\, p^{r+2h}}.$$

In particular for $h=1$, (2.7) becomes

$$pB_m(u) + 1 - p \equiv tp^{r+1}R(p) \pmod{p^{r+2}}$$

which shows that

$$(2.8)\qquad \sigma_m(u) = \frac{1}{p^r}\left(B_m(u) + \frac{1}{p} - 1\right)$$

is integral (mod p) and indeed

$$\sigma_m(u) \equiv tR(p) \pmod{p}. \tag{2.9}$$

It is easily seen that, for $u=0$, (2.9) reduces to (1.3).

To get a stronger congruence we take $2h \leqq r+2$. Clearly (2.7) implies

$$\sigma_m(u) \equiv tp^{1-h}R(p^h) \pmod{p^h} \qquad (1 \leqq h \leqq r/2+1). \tag{2.10}$$

In particular when $h=[r/2+1]$, we have the largest modulus.

We now state:

THEOREM 1. *Let $p \geqq 3$, $m=t(p-1)p^r$, then $\sigma_m(u)$ as defined by* (2.8) *is integral* (mod p). *Moreover $\sigma_m(u)$ satisfies the congruences* (2.9) *and* (2.10).

For $u=0$, (2.10) is not quite as sharp as (1.4). Indeed to prove (1.4) we take $u=0$ in (2.6) and assume $p>3$. Then since $B_{m-1}=0$ we can show that (2.6) implies

$$S_m(p^h) \equiv p^h B_m \pmod{p^{r+3h}} \qquad (u=0);$$

the rest of the argument is as before except that we take $3h \leqq r+2$. Thus (1.4) is proved.

We remark that if in place of (2.3) we use

$$(u+s)^m = 1 + p^{r+1}Q(u+s)$$

so that Q is integral (mod p), and replace (2.4) by the stronger congruence

$$S_m(p^h) \equiv S'_m(p^h) \pmod{p^m},$$

then (2.7) becomes

$$p^h B_m(u) + p^{h-1} - p^h \equiv p^{r+1}R^*(p^h) \pmod{p^m,\ p^{r+2h}},$$

where now

$$R^*(p^h) = \sum_{s=0,\, p \nmid u+s}^{p^h-1} Q(u+s).$$

Hence

$$\sigma_m(u) \equiv p^{1-h}R^*(p^h) \pmod{p^h}, \tag{2.10$'$}$$

provided $r+2h \leqq m$.

Similarly in the case $u=0$, we find that

$$\sigma_m \equiv p^{1-h}R^*(p^h) \pmod{p^h} \qquad (p>3),$$

provided $r+3h \leqq m$.

3. We shall require the following formula [3, p. 148, (87)]:

$$B^{(k)}(u) = k\binom{m}{k}\sum_{s=0}^{k-1}(-1)^{k-1-s}\binom{k-1}{s}\frac{B_{m-s}(u)}{m-s}B_s^{(k)}(u), \tag{3.1}$$

where $B_m^{(k)}(u)$ is defined by (1.5). We suppose $m \equiv s_0 \pmod{p-1}$, $0 \leqq s_0 \leqq k-1$, $k \leqq p-1$; also $p^r | m-s_0$. Now for $s \neq s_0$, both $B_{m-s}(u)$ and $B_s^{(k)}(u)$ are integral (mod p). Hence (3.1) implies

$$B_m^{(k)}(u) \equiv (-1)^{k-1-s_0}\binom{m}{s_0}\binom{m-s_0-1}{k-s_0-1}B_{m-s_0}(u)B_{s_0}^{(k)}(u) \pmod{p^r},$$

so that by Theorem 1,

$$\begin{aligned}\sigma_m^{(k)}(u) = \frac{1}{p^r}\Big\{&B_m^{(k)}(u) \\ &+ (-1)^{k-s_0}\left(1-\frac{1}{p}\right)\binom{m}{s_0}\binom{m-s_0-1}{k-s_0-1}B_{s_0}^{(k)}(u)\Big\}\end{aligned} \tag{3.2}$$

is integral (mod p). We state:

THEOREM 2. *Let $p \geqq 3$, $1 \leqq k \leqq p-1$; $m \equiv s_0$* (mod $p-1$), *$0 \leqq s_0 \leqq k-1$; $p^r | m-s_0$; then $\sigma_m^{(k)}(u)$ as defined by* (3.2) *is integral* (mod p). *In particular if $(p-1)p^r | m$ then*

$$\frac{1}{p^r}\left\{B_m^{(k)}(u) + (-1)^k\left(1-\frac{1}{p}\right)\binom{m-1}{k-1}\right\}$$

is integral (mod p).

Theorem 2 can be extended to larger values of k but the results are complicated. We remark that

$$B_s^{(k)}(u) = \frac{s!}{(k-1)!}\left(\frac{d}{du}\right)^{k-1-s}(u-1)(u-2)\cdots(u-k+1)$$

for $k > s$.

REFERENCES

1. L. Carlitz, *Some congruences for the Bernoulli numbers*, Amer. J. Math.

2. Emma Lehmer, *On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson*, Ann. of Math. (2) vol. 39 (1938) pp. 350–360.

3. N. E. Nörlund, *Vorlesungen über Differenzenrechnung*, Berlin, 1924.

DUKE UNIVERSITY