A NOTE ON BERNOULLI NUMBERS AND POLYNOMIALS OF HIGHER ORDER

L. CARLITZ

1. Introduction. Following the notation of Nörlund [5, Chap. 6], we defined \( B_m^{(k)} \), \( B_m^{(k)}(u) \) by means of

\[
\left( \frac{x}{e^x - 1} \right)^k e^{zu} = \sum_{m=0}^{\infty} B_m^{(k)}(u) \frac{x^m}{m!}, \quad B_m^{(k)} = B_m^{(k)}(0) \quad (k \geq 1).
\]

In the present paper we prove a number of theorems concerning \( B_m^{(k)}(u) \). It will be convenient to employ the abbreviations

\[
\begin{align*}
(m)_k &= m(m-1) \cdots (m-k+1), \quad (m)_0 = 1, \\
[m]_k &= (a^m-1)(a^{m-1}-1) \cdots (a^{m-k+1}-1), \quad [m]_0 = 1.
\end{align*}
\]

In the following theorems \( \rho \) denotes an odd prime; the rational numbers \( a, u \) are integral (mod \( \rho \)) and \( \rho \mid a \). We now state the following theorems.

Theorem 1. The number

\[
U_m^{(k)} = [m]_k B_m^{(k)}(u)/(m)_k \quad (m \geq k \geq 1)
\]

is integral (mod \( \rho \)).

Theorem 2. If \( k \leq \rho-1 \), \( m \not\equiv 0, 1, \cdots, k-1 \) (mod \( \rho-1 \)), \( m \geq k \geq 1 \), then \( B_m^{(k)}(u)/(m)_k \) is integral (mod \( \rho \)). In particular \( B_m^{(k)}(u) \) is integral (mod \( \rho \)).

Theorem 3. If \( k < \rho-1 \), \( m \not\equiv 0, 1, \cdots, k-1 \) (mod \( \rho-1 \)), \( m \geq k \geq 1 \), \( \rho' \mid (m)_k \), then the numerator of \( B_m^{(k)}(u) \) is divisible by \( \rho' \).

Theorem 4. Let \( U_m^{(k)} \) have the same meaning as in (1.3). If \((\rho-1)\rho^{-1} \mid b, m \geq rb+k, k \geq 1\), then

\[
\sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} U_{m+s}^{(k)} \equiv 0 \pmod{\rho^s}.
\]

Theorem 5. Put

\[
T_m^{(k)} = B_m^{(k)}(u)/(m)_k \quad (m \geq k \geq 1).
\]

If \( k < \rho-1, m \not\equiv 0, 1, \cdots, k-1 \) (mod \( \rho-1 \)), \( m \geq rb+k \), then

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

608
BERNOULLI NUMBERS AND POLYNOMIALS OF HIGHER ORDER 609

(1.6) \[ \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} T_{m+s}^{(k)} \equiv 0 \pmod{p^r}. \]

**Theorem 6.** If \( k < p - 1, m \equiv 0, 1, \cdots, k - 1 \pmod{p - 1}, m \equiv rb + k, r \geq k, \) then

(1.7) \[ \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} B_{m+s}^{(k)}(u) \equiv 0 \pmod{p^{(r-k)r}}. \]

**Theorem 7.** If \( k \leq p - 1, m \equiv 0 \pmod{p - 1}, 0 \leq s_0 \leq k - 1, \) then

(1.8) \[ pB_{m}^{(k)}(u) \equiv -\frac{(-1)^{k-s_0}}{(k - 1)!} \frac{(m)_k}{m - s_0} \binom{k - 1}{s_0} B_{s_0}^{(k)}(u) \pmod{p}. \]

**Theorem 8.** Let \( m \equiv 0 \pmod{p - 1}, 0 \leq s_0 < p - 1. \) If \( s_0 \neq 0, \) then

(1.9) \[ pB_{m}^{(p)}(u) \equiv \frac{(m)_p}{m - s_0} u^{s_0} \pmod{p}; \]

in particular if \( p \mid m - s_0, \) then

\[ pB_{m}^{(p)}(u) \equiv -u^{s_0}. \]

However, if \( s_0 = 0, \) then

(1.10) \[ pB_{m}^{(p)}(u) \equiv (m)_p \left( \frac{1}{m} + \frac{u^{p-1} - 1}{m - p + 1} \right) \pmod{p}; \]

in particular if \( p \mid m, \) then \( pB_{m}^{(p)}(u) \equiv -1, \) if \( p \mid m+1, \) then \( pB_{m}^{(p)}(u) \equiv 1 - u^{p-1}. \)

For references in the case \( k = 1, \) see [1, Chap. 1; 2; 3; 4, Chap. 14; 6]. Vandiver [6] has also discussed the case \( k = 2; \) indeed his numbers of the second order are somewhat more general.

2. **Proof of Theorem 1.** Let \( \eta(x) \) denote a (formal) power series of the type

(2.1) \[ 1 + \sum_{m=1}^{\infty} c_m (e^x - 1)^m, \]

where the \( c_m \) are integral (mod \( p \)). Put

(2.2) \[ g(x) = \left( \frac{x}{e^x - 1} \right)^k \eta(x). \]

If for brevity we define \( \delta^r g(x) \) recursively by means of

\[ \delta g(x) = g(ax) - g(x), \quad \delta^{r+1} g(x) = \delta^r g(ax) - a^r \delta^r g(x), \]
then in the first place, we have

\[ \delta g(x) = \left( \frac{ax}{e^{ax} - 1} \right)^k \eta(ax) - \left( \frac{x}{e^x - 1} \right)^k \eta(x) = \frac{x^k}{(e^x - 1)^{k-1}} \eta_1(x), \]

as is easily verified; here \( \eta_1(x) \) represents a series of the form (2.1). At the next step we find

\[ \delta^2 g(x) = \frac{a^k x^k}{(e^{ax} - 1)^{k-1}} \eta_1(ax) - \frac{ax^k}{(e^x - 1)^{k-1}} \eta_1(x) \]

\[ = \frac{x^k}{(e^x - 1)^{k-2}} \eta_2(x), \]

where \( \eta_2(x) \) is also of the form (2.1). Continuing in this way, we finally get

\[ (2.3) \quad \delta^k g(x) = x^k \eta_k(x), \]

where of course \( \eta_k(x) \) is of the form (2.1). Now let \( \eta(x) = e^{\alpha x} \) in (2.2); then it is clear from (1.1) that

\[ \delta^k g(x) = \sum_{m=k}^{\infty} \frac{[m]_k B_m^{(k)}(u)}{(m)_k} \frac{x^{m-k}}{(m-k)!} = \sum_{m=k}^{\infty} U_m^{(k)} \frac{x^m}{m!} \]

Now on the other hand it follows immediately from (2.1) that

\[ \eta(x) = \eta_k(x) = \sum_{n=0}^{\infty} b_n x^n / n!, \]

where the \( b_n \) are integral (mod \( p \)). Comparison with (2.3) and (2.4) yields the theorem.

3. **Proof of Theorems 2 and 3.** Suppose now that \( a \) is a primitive root (mod \( p \)); then it is clear from the hypothesis of Theorem 2 that none of the factors \( a^{k-i} - 1, \ i = 0, 1, \ldots, k-1 \), is divisible by \( p \). Consequently \( [m]_k \) is prime to \( p \) and thus Theorem 1 implies Theorem 2.

In the next place, let \( p \) \( | \) \( (m)_k \). Since, as we have just seen, \( p \) \( | \) \( [m]_k \), it follows from (1.3) that \( B_m^{(k)}(u) \equiv 0 \) (mod \( p^r \)). Hence Theorem 3 follows.

4. **Proof of Theorem 4.** We note first that for \( \eta(x) \) as defined by (2.1), we have

\[ \eta(x) = 1 + \sum_{i=1}^{\infty} c_i \sum_{s=0}^{t} (-1)^{t-s} \binom{t}{s} \sum_{m=0}^{\infty} \frac{x^m}{m!}. \]
Hence if we put

$$\eta(x) = 1 + \sum_{m=1}^{\infty} d_m x^m / m!,$$

it follows that

$$(4.1) \sum_{j=1}^{n} c_j \sum_{s=0}^{l} (-1)^{l-s} \binom{l}{s} s^m \quad (n \geq m),$$

since the inner sum in the right member of (4.1) vanishes for $n > m$. Then clearly

$$\begin{align*}
\sum_{j=0}^{r} (-1)^{-i} \binom{r}{j} d_{m+jb} &= \sum_{l=1}^{\infty} c_t \sum_{s=0}^{l} (-1)^{l-s} \binom{l}{s} (s-1)^r s^m, \\
\end{align*}$$

where of course the outer sum in the right member is finite. It follows at once that

$$(4.2) \sum_{j=0}^{r} (-1)^{-i} \binom{r}{j} d_{m+jb} \equiv 0 \pmod{p^r}$$

provided $m \geq rb$.

Turning now to $U_{m}^{(k)}$, we get from (2.3) and (2.4) that $\delta_k g(x)/x^k$ is of the form $\eta(x)$ and that the general term in the expansion is of the form $U_{m+k}^{(k)} x^m / m! \ (m \geq 0)$. Thus we may take $d_m = U_{m+k}^{(k)}$, and (4.1) and (4.2) apply. In particular (4.2) implies

$$(4.3) \sum_{j=0}^{r} (-1)^{-i} \binom{r}{j} U_{m+jb}^{(k)} \equiv 0 \pmod{p^r}$$

provided $m \geq rb$. If we replace $m+k$ by $m$, it is clear that Theorem 4 holds.

5. **Proof of Theorem 5.** If we substitute from (1.3) in (4.3), we get

$$(5.1) \sum_{i=0}^{r} (-1)^{r-i} \binom{r}{j} [m+jb]_k B_{m+jb}^{(k)} (u) \equiv 0 \pmod{p^r}$$

provided $m \geq rb+k$. Suppose now that $a$ is a primitive root (mod $p$) such that $a^{p-1} = 1 \pmod{p^r}$ for an arbitrarily assigned $w$. By Theorem 2 we know that $B_{m+jb}^{(k)} (u)/(m+jb)_k$ is integral. Hence it suffices to take $w = re$, so that

$$[m+jb]_k \equiv [m]_k \pmod{p^r} \quad (j = 0, 1, \cdot \cdot \cdot , r).$$

Thus the left member of (5.1) is congruent to
\[ [m]_k \sum_{i=0}^{r} (-1)^{r-i} \binom{r}{i} B_{m+i}^{(k)}(u)/(m + jb)_k \quad (\mod p^e). \]

Since \( p \mid [m]_k \), (1.6) follows immediately.

6. Proof of Theorem 6. We make use of a device employed by Nielsen [2, Chap. 14]. Let

\[ A_{r,q} = \sum_{s=0}^{r} (-1)^{r-s} \binom{r}{s} \binom{m + sb}{q} T_{m+sb}^{(k)} \]

so that \( A_{r,0} \) denotes the left member of (1.6) and \( A_{r,k} \) the left member of (1.7). We require the recursion

\[ (m + rb - q)A_{r,q} + rbA_{r-1,q} = (q + l)A_{r,q+1}, \]

which is easily verified by substituting from (6.1). Now by the last theorem \( A_{r,0} \equiv 0 \quad (\mod p^e) \); hence repeated application of (6.2) leads to

\[ A_{r,q} \equiv 0 \quad (\mod p^{(r-s)e}) \]

provided \( q \leq r \), \( q < p \). In particular if we take \( q = k \) in (6.3), Theorem 6 follows at once.

7. Proof of Theorems 7 and 8. We shall require the following formula [5, p. 148, (87)]:

\[ B_m^{(k)}(u) = k \left( \sum_{s=0}^{m} (-1)^{k-s} \binom{k-1-s}{s} \frac{B_{m-s}(u)}{m-s} B_s^{(k)}(u), \right. \]

where \( B_m(u) = B_m^{(1)}(u) \); we also need

\[ pB_m(u) \equiv \begin{cases} -1 \quad (\mod p) \\ 0 \quad (p - 1 \mid m), \end{cases} \]

\( p \mid (p - 1 \mid m) \).

Now let \( m = s_0 \quad (\mod p - 1) \), where \( 0 \leq s_0 \leq k - 1 \). Since for \( s < k \)

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

it is clear that \( B_s^{(k)}(u) \) is integral \( (\mod p) \). Thus if we apply (7.2) to the right member of (7.1), we get

\[ pB_m^{(k)} \equiv (-1)^{k-s_0} k \left( \binom{m}{k} \binom{k-1}{s_0} \frac{B_{s_0}(u)}{m-s_0} \right) \quad (\mod p), \]

which is the same as (1.8).
To prove Theorem 8, we again use (7.1). Then for \( k = p, s_0 \neq 0 \), it is clear that (7.1) and (7.2) imply

\[
pB_m^{(p)}(u) \equiv (-1)^{s_0+1} \frac{(m)_p}{(p - 1)!} \binom{p - 1}{s_0} \frac{B^{(p)}_{s_0}}{m - s_0} \pmod{p}.
\]

Now

\[
\binom{p - 1}{s} \equiv (-1)^s
\]

and by (7.3)

\[
B_s^{(p)}(u) \equiv \frac{s!}{(p - 1)!} \left( \frac{d}{du} \right)^{p-1-s} (u^{p-1} - 1) \equiv u^s \quad (s \leq p - 1).
\]

Thus

\[
pB_m^{(p)}(u) \equiv \frac{(m)_p}{m - s_0} u^s \pmod{p},
\]

which is identical with (1.9).

As for the case \( s_0 = 0 \), the only difference is that there are now two terms in (7.1) to consider, namely, those corresponding to \( s = 0, s = p - 1 \). Thus

\[
(7.4) \quad pB_m^{(p)}(u) \equiv -\frac{(m)_p}{(p - 1)!} \left( \frac{1}{m} + \frac{1}{m - p + 1} \right) B_{p-1}^{(p)}(u);
\]

but by (7.3)

\[
B_{p-1}^{(p)}(u) = (u - 1)(u - 2) \cdots (u - p + 1) \equiv u^{p-1} - 1.
\]

Substitution in (7.4) yields (1.10).

References

3. E. E. Kummer, *Über eine allgemeine Eigenschaft der rational Entwicklungss-

Duke University