

Congruences for Bernoulli, Euler, and Stirling Numbers

PAUL THOMAS YOUNG

*Department of Mathematics, University of Charleston
Charleston, SC 29424*

We use properties of p -adic integrals and measures to obtain congruences for higher-order Bernoulli and Euler numbers and polynomials, as well as for certain generalizations, and for Stirling numbers of the second kind. These congruences are analogues and generalizations of the usual Kummer congruences for the ordinary Bernoulli numbers.

1. INTRODUCTION.

The Bernoulli polynomials of order w , denoted $B_n^{(w)}(x)$, are defined by

$$\left(\frac{t}{e^t - 1}\right)^w e^{xt} = \sum_{n=0}^{\infty} B_n^{(w)}(x) \frac{t^n}{n!}. \quad (1.1)$$

The Euler polynomials of order w , denoted $E_n^{(w)}(x)$, are defined by

$$\left(\frac{2}{1 + e^t}\right)^w e^{xt} = \sum_{n=0}^{\infty} E_n^{(w)}(x) \frac{t^n}{n!}. \quad (1.2)$$

The values at $x = 0$ are called Bernoulli and Euler numbers of order w ; when $w = 1$ the polynomials or numbers are called *ordinary*. When $x = 0$ or $w = 1$ we often suppress that part of the notation; e.g., $B_n^{(w)}$ denotes $B_n^{(w)}(0)$, $E_n(x)$ denotes $E_n^{(1)}(x)$, and B_n denotes $B_n^{(1)}(0)$.

These numbers have been extensively studied and many congruences for them are known. Among the most important results are the Kummer congruences for the ordinary Bernoulli numbers, which in their simplest form state that

$$\frac{B_m}{m} \equiv \frac{B_n}{n} \pmod{p\mathbb{Z}_p} \quad (1.3)$$

for positive even integers m, n such that $m \equiv n \not\equiv 0 \pmod{p-1}$, where p is an odd prime (cf. [10], Corollary 5.14). More general versions of these congruences are given in (4.9) and (4.16) below. In this paper we give extensions of these congruences for a variety of sequences, including the higher-order Bernoulli and Euler polynomials and the weighted Stirling numbers of the second kind, denoted $S(n, w, x)$, which are defined by

$$(e^t - 1)^w e^{xt} = w! \cdot \sum_{n=w}^{\infty} S(n, w, x) \frac{t^n}{n!}. \quad (1.4)$$

Setting $x = 0$ gives the usual Stirling numbers of the second kind $S(n, w) = S(n, w, 0)$. All these congruences are deduced from some basic properties of p -adic Γ -transforms which we record in Theorems 1.1 and 1.2 below.

A primary focus of this work is the application of these p -adic integration techniques to extend several known results on Bernoulli polynomials of higher order. A. Adelberg [2] has recently given congruences for $B_n^{(w)}$ which extend the Kummer congruences (1.3), and deduced information concerning the irreducibility of certain Bernoulli polynomials. Our congruences for the higher-order Bernoulli polynomials (§5) provide a different type of extension of a more general form of the Kummer congruences. Our method also provides a general lower bound of the p -adic ordinal of $B_n^{(w)}$ which, while not best possible in all cases, exceeds the previously known bounds in certain cases. Although the estimates of Adelberg ([1], [2]) and F. T. Howard [6] for the ordinal of $B_{m+w}^{(w)}$ are asymptotically superior to ours when m is fixed and $w \rightarrow \infty$, our bound is asymptotically superior when the order w is fixed and $m \rightarrow \infty$.

The binomial coefficient operator which appears in our Theorem 1.2 below is an extension of that employed by H. S. Gunaratne [5] in his generalization of the Kummer congruences, which he used to characterize the Iwasawa invariants of Dirichlet characters. Our theorem provides congruences of this type for a certain class of sequences. In §3 we apply this theorem to the Stirling numbers and Euler polynomials following the work of H. Tsumura [8], [9]. In §4 we treat the ordinary Bernoulli and generalized Bernoulli numbers using Theorem 1.2.

If c is a nonnegative integer, the difference operator Δ_c operates on the sequence $\{a_m\}$ by

$$\Delta_c a_m = a_{m+c} - a_m. \quad (1.5)$$

The powers Δ_c^k of Δ_c are defined by $\Delta_c^0 = \text{identity}$ and $\Delta_c^k = \Delta_c \circ \Delta_c^{k-1}$ for positive integers k , so that

$$\Delta_c^k a_m = \sum_{j=0}^k \binom{k}{j} (-1)^{k-j} a_{m+jc} \quad (1.6)$$

for all nonnegative integers k . To define binomial coefficient operators $\binom{D}{k}$ associated to an operator

D (cf. [5]), we write the binomial coefficient

$$\binom{X}{k} = \frac{X(X-1)\cdots(X-k+1)}{k!} \quad (1.7)$$

for $k \geq 0$ as a polynomial in X , and replace X by D . Since the particular sequences considered in this paper have multiple indices, we shall always use the index m to denote the index on which an operator operates.

Let p be a prime, and define q by

$$q = \begin{cases} p, & \text{if } p > 2, \\ 4, & \text{if } p = 2. \end{cases} \quad (1.8)$$

Let \mathfrak{D}_K denote the ring of integers in a finite extension of the field \mathbb{Q}_p of p -adic numbers. The following theorem is an extension of ([9], Lemma 1).

THEOREM 1.1. *Let $f \in \mathfrak{D}_K[[T-1]]$ and write $f(e^t) = \sum_{n=0}^{\infty} a_n \frac{t^n}{n!}$. Then $a_n \in \mathfrak{D}_K$ for all n . Furthermore, if $c \equiv 0 \pmod{\phi(q)p^a}$ with $a \geq 0$ then*

$$\Delta_c^k a_m \equiv 0 \pmod{p^A \mathfrak{D}_K}$$

for all $m, k \geq 0$, where $A = \min\{m, k(a+1)\}$ if $p > 2$ and $A = \min\{m, k(a+3)\}$ if $p = 2$.

Define the linear operator φ by

$$\varphi f(T) = f(T) - \frac{1}{p} \sum_{\zeta^p=1} f(\zeta T). \quad (1.9)$$

This operator is well-defined on rational functions, and also on $\mathfrak{D}_K[[T-1]]$ (cf. (2.14)). If $f(e^t) = \sum a_n t^n/n!$, write $(\varphi f)(e^t) = \sum \hat{a}_n t^n/n!$. A modification of Theorem 1.1 yields stronger congruences for the modified numbers \hat{a}_n .

THEOREM 1.2. *Let $f \in \mathfrak{D}_K[[T-1]]$ and write $\varphi f(e^t) = \sum_{n=0}^{\infty} \hat{a}_n \frac{t^n}{n!}$. Then $\hat{a}_n \in \mathfrak{D}_K$ for all n . Furthermore, if $c \equiv 0 \pmod{\phi(q)p^a}$ with $a \geq 0$ then*

$$\Delta_c^k \hat{a}_m \equiv 0 \pmod{p^{ka'} \mathfrak{D}_K}$$

for all $m, k \geq 0$, where $a' = a+1$ if $p > 2$ and $a' = a+3$ if $p = 2$, and also

$$\binom{p^{-r} \Delta_c}{k} \hat{a}_m \in \mathfrak{D}_K$$

for $0 \leq r \leq a'$ and all $m, k \geq 0$.

To compare the results of these theorems, one may observe by (2.10) and (2.15) below that $a_m \equiv \hat{a}_m \pmod{p^m \mathfrak{D}_K}$, so the first congruence of Theorem 1.2 is an extension of the congruence of Theorem 1.1. One may also observe that by the first statement of Theorem 1.2, the operator $(p^{-a'} \Delta_c)^k$ is a polynomial of order k in Δ_c with leading coefficient $p^{-ka'}$ which sends a_m into \mathfrak{D}_K , whereas by the second statement of Theorem 1.2, the binomial coefficient operator $\binom{p^{-a'} \Delta_c}{k}$ is a polynomial of order k in Δ_c with leading coefficient $p^{-ka'}/k!$ which sends a_m into \mathfrak{D}_K .

2. DEMONSTRATIONS OF THEOREMS.

Throughout this paper p will denote a prime number, \mathbb{Z}_p the ring of p -adic integers, and \mathbb{Q}_p the field of p -adic numbers. If K is a finite extension of \mathbb{Q}_p then \mathfrak{D}_K will denote its ring of integers and \mathfrak{D}_K^\times will denote the multiplicative group of units in \mathfrak{D}_K . Recall that q is defined by $q = p$ if $p > 2$ and $q = 4$ if $p = 2$. The Teichmüller character ω on \mathbb{Z}_p^\times is defined by setting $\omega(x)$ to be the unique $\phi(q)$ -th root of unity congruent to x modulo $q\mathbb{Z}_p$, and we define $\langle x \rangle$ by $x = \omega(x) \cdot \langle x \rangle$ for $x \in \mathbb{Z}_p^\times$. We use $\mathfrak{D}_K[T - 1]$, $\mathfrak{D}_K[[T - 1]]$, and $\mathfrak{D}_K((T - 1))$ to denote respectively the ring of polynomials, of formal power series, and of formal Laurent series in the indeterminate $(T - 1)$ over \mathfrak{D}_K . We use “ord” to denote the additive valuation on K normalized by $\text{ord } p = 1$. Finally, e^t denotes the exponential function defined by the power series $\sum_{n=0}^{\infty} t^n/n!$ for $\text{ord } t > 1/(p - 1)$.

Proof of Theorem 1.1. Write $f(T) = \sum_{m=0}^{\infty} b_m(T - 1)^m$ with each $b_m \in \mathfrak{D}_K$. Since

$$(e^t - 1)^m = m! \sum_{n=m}^{\infty} S(n, m) \frac{t^n}{n!}, \quad (2.1)$$

we have

$$a_n = \sum_{m=0}^n m! S(n, m) b_m, \quad (2.2)$$

and therefore $a_n \in \mathfrak{D}_K$, since $m! S(n, m) \in \mathbb{Z}$ for all m, n .

Let Λ denote the set of all \mathfrak{D}_K -valued measures on \mathbb{Z}_p . As is well-known, there is a one-to-one correspondence

$$\Lambda \leftrightarrow \mathfrak{D}_K[[T - 1]], \quad (2.3)$$

(cf. ([10], Ch. 12), ([9],§1)) under which each measure $\alpha \in \Lambda$ corresponds to the formal power series

$$f_\alpha(T) = \int_{\mathbb{Z}_p} T^x d\alpha(x) = \sum_{m=0}^{\infty} \left(\int_{\mathbb{Z}_p} \binom{x}{m} d\alpha(x) \right) (T-1)^m. \quad (2.4)$$

Let $\alpha = \alpha_f$ be the measure which corresponds to our power series $f(T)$ under this identification. Substituting $T = e^t$ in (2.4) with $\text{ord } t > 1/(p-1)$ and evaluating the n -th derivative (with respect to t) at $t = 0$ yields

$$a_n = \int_{\mathbb{Z}_p} x^n d\alpha_f(x). \quad (2.5)$$

For $i \in \mathbb{Z}$ we consider $\omega^i \alpha_f$ as a measure on \mathbb{Z}_p^\times . The function $g(s, i, f)$ defined for $s \in \mathbb{Z}_p$ by

$$g(s, i, f) = \int_{\mathbb{Z}_p^\times} \langle x \rangle^s \omega^i(x) d\alpha_f(x) \quad (2.6)$$

is the p -adic Γ -transform of the measure $\omega^i \alpha_f$, and as such is a p -adic analytic function of s on \mathbb{Z}_p ([10], Corollary 12.5). Furthermore, when n is a nonnegative integer with $n \equiv i \pmod{\phi(q)}$, we have $\langle x \rangle^n \omega^i(x) = x^n$ for all $x \in \mathbb{Z}_p^\times$, and therefore

$$g(n, i, f) = \int_{\mathbb{Z}_p^\times} x^n d\alpha_f(x). \quad (2.7)$$

It follows from (1.6) and (2.7) that for $c \equiv 0 \pmod{\phi(q)p^a}$, we have

$$\begin{aligned} \Delta_c^k g(m, i, f) &= \sum_{j=0}^k \binom{k}{j} (-1)^{k-j} g(m + jc, i, f) \\ &= \int_{\mathbb{Z}_p^\times} x^m (x^c - 1)^k d\alpha_f(x) \end{aligned} \quad (2.8)$$

when $m \equiv i \pmod{\phi(q)}$. Since $(x^c - 1)^k \equiv 0 \pmod{p^{ka'} \mathbb{Z}_p}$ for all $x \in \mathbb{Z}_p^\times$ (where $a' = a + 1$ if $p > 2$ and $a' = a + 3$ if $p = 2$), and α_f is an \mathfrak{D}_K -valued measure, this implies

$$\Delta_c^k g(m, i, f) \equiv 0 \pmod{p^{ka'} \mathfrak{D}_K}. \quad (2.9)$$

On the other hand, $x^n \equiv 0 \pmod{p^n \mathbb{Z}_p}$ for all $x \in p\mathbb{Z}_p$, so from (2.5), (2.7) we obtain

$$\begin{aligned} g(n, i, f) &= \int_{\mathbb{Z}_p^\times} x^n d\alpha_f(x) \\ &\equiv \int_{\mathbb{Z}_p} x^n d\alpha_f(x) = a_n \pmod{p^n \mathfrak{D}_K}. \end{aligned} \quad (2.10)$$

Therefore $\Delta_c^k g(m, i, f) \equiv \Delta_c^k a_m \pmod{p^m \mathfrak{D}_K}$, which yields the stated result.

Proof of Theorem 1.2. As in (2.4), we have

$$f(T) = \int_{\mathbb{Z}_p} T^x d\alpha_f(x), \quad (2.11)$$

which by (2.4) is valid as a power series identity which is convergent for $T \in \mathfrak{D}_K$ with $\text{ord}(T-1) > 0$.

We compute

$$\begin{aligned} \varphi f(T) &= f(T) - \frac{1}{p} \sum_{\zeta^p=1} f(\zeta T) \\ &= \int_{\mathbb{Z}_p} \left(1 - \frac{1}{p} \sum_{\zeta^p=1} \zeta^x \right) T^x d\alpha_f(x). \end{aligned} \quad (2.12)$$

Since

$$\frac{1}{p} \sum_{\zeta^p=1} \zeta^x = \begin{cases} 0, & \text{if } x \in \mathbb{Z}_p^\times, \\ 1, & \text{if } x \in p\mathbb{Z}_p, \end{cases} \quad (2.13)$$

we have

$$\varphi f(T) = \int_{\mathbb{Z}_p^\times} T^x d\alpha_f(x), \quad (2.14)$$

valid for $T \in \mathfrak{D}_K$ with $\text{ord}(T-1) > 0$, and therefore also valid as a power series identity in the ring $\mathfrak{D}_K[[T-1]]$. Note that this shows that $\varphi f \in \mathfrak{D}_K[[T-1]]$ via the correspondence (2.3), (2.4), with φf corresponding to the measure $g\alpha_f$ where g is the characteristic function of \mathbb{Z}_p^\times .

Setting $T = e^t$ and considering n -th derivatives as in (2.5) and comparing with (2.7) we have

$$\hat{a}_n = g(n, i, f) = \int_{\mathbb{Z}_p^\times} x^n d\alpha_f(x) \quad (2.15)$$

for all n, i such that $n \equiv i \pmod{\phi(q)}$. Since α_f is an \mathfrak{D}_K -valued measure, we have $\hat{a}_n \in \mathfrak{D}_K$, and we compute

$$\Delta_c^k \hat{a}_m = \int_{\mathbb{Z}_p^\times} x^m (x^c - 1)^k d\alpha_f(x) \quad (2.16)$$

for all $k, m \geq 0$, whence $\Delta_c^k \hat{a}_m \equiv 0 \pmod{p^{ka'} \mathfrak{D}_K}$, yielding the first statement.

For the second statement, we observe that

$$\binom{p^{-r} \Delta_c}{k} \hat{a}_m = \int_{\mathbb{Z}_p^\times} x^m \cdot \binom{p^{-r} (x^c - 1)}{k} d\alpha_f(x). \quad (2.17)$$

Since $p^{-r}(x^c - 1) \in \mathbb{Z}_p$ for all $x \in \mathbb{Z}_p^\times$ when $0 \leq r \leq a'$ and $c \equiv 0 \pmod{\phi(q)p^a}$, and $\binom{X}{k} \in \mathbb{Z}_p$ for all $X \in \mathbb{Z}_p$ and all $k \geq 0$, we conclude from the fact that α_f is an \mathfrak{D}_K -valued measure that

$$\binom{p^{-r}\Delta_c}{k} \hat{a}_m \in \mathfrak{D}_K \quad (2.18)$$

for $0 \leq r \leq a'$ and all $k, m \geq 0$.

3. CONGRUENCES FOR STIRLING NUMBERS AND EULER POLYNOMIALS.

The theorems of §1 are readily applied to $S(m, w, x)$, extending and strengthening [9, Theorem B]. (Note: The definition of $N(k)$ in that Theorem should read $N(k) = \min\{m, e+1\} - r(k)$, where $r(k) = \text{ord}(k!)$.)

THEOREM 3.1. *If $m \geq w \geq 0$ and $c \equiv 0 \pmod{\phi(q)p^a}$ with $a \geq 0$, then for all $k \geq 0$ and all $x \in \mathbb{Z}_p$ we have*

$$\Delta_c^k S(m, w, x) \equiv 0 \pmod{p^{A-r(w)} \mathbb{Z}_p},$$

where $A = \min\{m, ka'\}$ and $r(w) = \text{ord}(w!)$. If in addition we have $w < p$ then

$$\Delta_c^k S(m, w) \equiv 0 \pmod{p^{ka'} \mathbb{Z}_p}$$

and

$$\binom{p^{-r}\Delta_c}{k} S(m, w) \in \mathbb{Z}_p.$$

for $0 \leq r \leq a'$.

Proof. Let $f(T) = (p^{r(w)}/w!) \cdot (T-1)^w T^x \in \mathbb{Z}_p[[T-1]]$. The first statement follows directly by applying Theorem 1.1 to f . For the second statement, observe that $\varphi T^n = T^n$ whenever $(n, p) = 1$; therefore $\varphi f = f - 1$ when $w < p$ and $x = 0$. In this case we also have $r(w) = 0$, so the second statement then follows directly from Theorem 1.2.

We now give congruences for the generalized Euler polynomials $H_n^{(w)}(u, x)$ of order w attached to an algebraic number $u \neq 1$, which are defined by

$$\left(\frac{1-u}{e^t-u}\right)^w e^{xt} = \sum_{n=0}^{\infty} H_n^{(w)}(u, x) \frac{t^n}{n!}. \quad (3.1)$$

Here the order w may be any p -adic integer. Note that $E_n^{(w)}(x) = H_n^{(w)}(-1, x)$. Again, we often suppress w in the notation when $w = 1$ and we often suppress mention of x when $x = 0$.

THEOREM 3.2. *Let u be algebraic over \mathbb{Q}_p , and suppose that $1 - u \in \mathfrak{D}_K^\times$, where $K = \mathbb{Q}_p(u)$. Then for all $m \geq 0$ and all $w, x \in \mathbb{Z}_p$, we have $H_m^{(w)}(u, x) \in \mathfrak{D}_K$, and for $c \equiv 0 \pmod{\phi(q)p^a}$ we have*

$$\Delta_c^k H_m^{(w)}(u, x) \equiv 0 \pmod{p^A \mathfrak{D}_K}$$

for all $k \geq 0$, where $A = \min\{m, ka'\}$. Furthermore, if w is a positive integer then the congruences of Theorem 1.2 hold for the numbers

$$\hat{a}_n = H_n^{(w)}(u) - \sum_{j=1}^w A_{w,j} \frac{(u^{-1} - 1)^w}{(u^{-p} - 1)^j} p^n H_n^{(j)}(u^p)$$

where $A_{w,j}$ equals (w/pj) times the coefficient of z^w in $((1+z)^p - 1)^j$.

Proof. If $1 - u \in \mathfrak{D}_K^\times$ then $f(T) = ((1-u)/(T-u))^w \cdot T^x \in \mathfrak{D}_K[[T-1]]$ for all $x, w \in \mathbb{Z}_p$, and therefore the first statement follows immediately from Theorem 1.1. For the second part, we make use of the identity

$$\psi \left(\frac{1}{(X-1)^s} \right) = \sum_{j=1}^s \frac{A_{s,j}}{(X-1)^j}, \quad (3.2)$$

given in ([4], Lemma 5.3.1), where

$$\psi f(X) = \frac{1}{p} \sum_{Z^p=X} f(Z). \quad (3.3)$$

Noting that $\varphi f(T) = f(T) - (\psi f)(T^p)$ for any function f and setting $X = u^{-1}T$ in (3.2) yields

$$\varphi \left(\frac{1-u}{T-u} \right)^w = \left(\frac{1-u}{T-u} \right)^w - \sum_{j=1}^w A_{w,j} \frac{(u^{-1} - 1)^w}{(u^{-p} - 1)^j} \left(\frac{1-u^p}{T^p - u^p} \right)^j. \quad (3.4)$$

Therefore corresponding to the function $f(T) = ((1-u)/(T-u))^w$ we have $(\varphi f)(e^t) = \sum_n \hat{a}_n t^n / n!$ with \hat{a}_n as in the statement of the theorem. The second part then follows from Theorem 1.2.

In many applications of Euler numbers the parameter u is taken to be a nontrivial $(p-1)$ -st root of unity. We observe that in this case the numbers \hat{a}_n simplify to

$$\hat{a}_n = (1 - p^{w+n-1}) H_n^{(w)}(u) - \sum_{j=1}^{w-1} A_{w,j} (u^{-1} - 1)^{w-j} p^n H_n^{(j)}(u). \quad (3.5)$$

In particular when $w = 1$ and u is a nontrivial $(p - 1)$ -st root of unity, the numbers $a_n = H_n(u)$ and \hat{a}_n are related by the simple Euler factor $(1 - p^n)$.

For a primitive Dirichlet character χ of conductor f , the generalized Euler numbers $H_{n,\chi}(u)$ are defined by

$$\sum_{a=0}^{f-1} \frac{(1 - u^f)\chi(a)e^{at}u^{f-1-a}}{e^{ft} - u^f} = \sum_{n=0}^{\infty} H_{n,\chi}(u) \frac{t^n}{n!} \quad (3.6)$$

(cf. [8]). If $\chi = 1$, we observe that $H_{n,\chi}(u) = H_n(u)$. For nontrivial characters χ , we note that the associated function $f(T)$ is

$$f(T) = f(u, \chi, T) = \sum_{a=0}^{f-1} \frac{(1 - u^f)\chi(a)T^a u^{f-1-a}}{T^f - u^f} = u^{-1}(1 - u^f)f_\chi(u^{-1}T) \quad (3.7)$$

with f_χ as defined in (4.11). As a corollary to the proof of Theorem 4.2 below we deduce congruences for these generalized Euler numbers.

THEOREM 3.3. *Suppose that χ is a primitive Dirichlet character of conductor f , and that u is algebraic over \mathbb{Q}_p with $1 - u^f \in \mathfrak{D}_K^\times$, where $K = \mathbb{Q}_p(u, \chi)$. If $c \equiv 0 \pmod{\phi(q)p^a}$ with $a \geq 0$, then the congruences of Theorem 1.2 hold for the numbers*

$$\hat{a}_n = H_{n,\chi}(u) - u^{p-1} \frac{1 - u^f}{1 - u^{pf}} \chi(p) p^n H_{n,\chi}(u^p).$$

Proof. If $\chi = 1$, then $f = 1$, $H_{n,\chi}(u) = H_n(u)$, and the result follows from the second statement of Theorem 3.2 by taking $w = 1$ and observing $A_{1,1} = 1$, so suppose $\chi \neq 1$. Since $1 - u^f \in \mathfrak{D}_K^\times$, the polynomial $T^f - u^f$ is invertible in $\mathfrak{D}_K[[T - 1]]$, so $f(u, \chi, T) \in \mathfrak{D}_K[[T - 1]]$. From (3.7), (4.12), and (4.13) we compute

$$\varphi f(u, \chi, T) = f(u, \chi, T) - u^{p-1} \frac{1 - u^f}{1 - u^{pf}} \chi(p) f(u^p, \chi, T^p), \quad (3.8)$$

from which the theorem follows.

The reader will also observe that if u is a nontrivial $(p - 1)$ -st root of unity then the numbers \hat{a}_n simplify to

$$\hat{a}_n = (1 - \chi(p)p^n)H_{n,\chi}(u). \quad (3.9)$$

4. ORDINARY AND GENERALIZED BERNOULLI NUMBERS.

In this section we give congruences for the action of binomial coefficient operators on the ordinary Bernoulli numbers, which extend ([5], Remark 5.1 and Theorem 3.1), in the case $c \equiv 0 \pmod{\phi(q)p^a}$ with $a > 0$.

THEOREM 4.1 *Suppose that $\phi(q)$ does not divide m . If $c \equiv 0 \pmod{\phi(q)p^a}$ with $a \geq 0$, then*

$$\binom{p^{-r}\Delta_c}{k} \left\{ (1 - p^{m-1}) \frac{B_m}{m} \right\} \in \mathbb{Z}_p$$

for $0 \leq r \leq a'$ and all $k > 0$.

Proof. For $p = 2$, the quantity $(1 - 2^{m-1})B_m/m$ is zero for all odd m , and the theorem is therefore trivially true. Now suppose p is odd and let $b \in \mathbb{Z}$ with $b > 1$ and $(b, p) = 1$. The polynomial

$$F_b(T) = \frac{T^b - 1}{T - 1} = \frac{((T - 1) + 1)^b - 1}{T - 1} = b + \binom{b}{2}(T - 1) + \cdots + (T - 1)^{b-1} \quad (4.1)$$

lies in $\mathbb{Z}[T - 1]$ and has constant term $b \in \mathbb{Z}_p^\times$ when viewed as an element of $\mathbb{Z}[T - 1]$. Therefore

$$\frac{b}{F_b(T)} \in 1 + (T - 1)\mathbb{Z}_p[[T - 1]], \quad (4.2)$$

so that

$$\frac{b}{T^b - 1} = \frac{1}{T - 1} + f(T), \quad (4.3)$$

where $f(T)$ is a rational function which also lies in $\mathbb{Z}_p[[T - 1]]$.

Now we substitute $T = e^t$ and expand as formal power series,

$$t^{-1} \sum_{n=0}^{\infty} (b^n - 1) B_n \frac{t^n}{n!} = \sum_{n=0}^{\infty} a_n \frac{t^n}{n!}, \quad (4.4)$$

where each $a_n \in \mathbb{Z}_p$. For each $n \geq 0$, equating coefficients of $t^n/n!$ yields

$$(b^{n+1} - 1) \frac{B_{n+1}}{n + 1} = a_n. \quad (4.5)$$

Since

$$\varphi \left(\frac{1}{T^a - 1} \right) = \frac{1}{T^a - 1} - \frac{1}{T^{pa} - 1} \quad (4.6)$$

whenever $(a, p) = 1$, we see that for this function $f(T)$ we have

$$(1 - p^n)(b^{n+1} - 1) \frac{B_{n+1}}{n + 1} = \hat{a}_n. \quad (4.7)$$

Supposing that $n + 1$ is not divisible by $p - 1$, choose b so that $b^{n+1} \not\equiv 1 \pmod{p}$. Since the congruences of Theorem 1.2 hold for the numbers \hat{a}_n as in (4.7) associated to b^{p^i} for $i = 1, 2, 3, \dots$, they hold for the numbers

$$(1 - p^n)(\omega(b)^{n+1} - 1) \frac{B_{n+1}}{n+1} \quad (4.8)$$

obtained upon passing to the p -adic limit. We then take $m = n + 1$ and observe that $(\omega(b)^m - 1)$ is a p -adic unit and that $(\omega(b)^j - 1) = (\omega(b)^m - 1)$ if $j \equiv m \pmod{c}$, allowing us to divide the congruences by $(\omega(b)^m - 1)$, giving the result.

Remark. The reader will observe that this proof also implies the more classical Kummer congruences

$$\Delta_c^k \left\{ (1 - p^{m-1}) \frac{B_m}{m} \right\} \equiv 0 \pmod{p^{k(a+1)} \mathbb{Z}_p} \quad (4.9)$$

for odd primes p when $c \equiv 0 \pmod{(p-1)p^a}$ and $p-1$ does not divide m .

For a primitive Dirichlet character χ of conductor f the generalized Bernoulli numbers $B_{n,\chi}$ are defined by

$$\sum_{a=1}^f \frac{\chi(a) t e^{at}}{e^{ft} - 1} = \sum_{n=0}^{\infty} B_{n,\chi} \frac{t^n}{n!} \quad (4.10)$$

(cf. [10], Ch. 4). We give congruences for the action of binomial coefficient operators on these numbers.

THEOREM 4.2. *Suppose that χ is a nontrivial primitive Dirichlet character of conductor f , with $(f, p) = 1$, and put $K = \mathbb{Q}_p(\chi)$. If $c \equiv 0 \pmod{\phi(q)p^a}$ with $a \geq 0$, then*

$$\binom{p^{-r} \Delta_c}{k} \left\{ (1 - \chi(p) p^{m-1}) \frac{B_{m,\chi}}{m} \right\} \in \mathfrak{D}_K$$

for $0 \leq r \leq a'$ and all $m, k > 0$.

Proof. Define

$$f_\chi(T) = \sum_{a=1}^f \frac{\chi(a) T^a}{T^f - 1}. \quad (4.11)$$

Since $(f, p) = 1$ we see from (4.3), (4.11) that $f_\chi(T)$ lies in $\mathfrak{D}_K((T-1))$. At $T = 1$ the numerator of $f_\chi(T)$ equals $\sum_{a=1}^f \chi(a) = 0$ since $\chi \neq 1$. Therefore we see that $f_\chi(T) \in \mathfrak{D}_K[[T-1]]$. It is easily

verified that $f_\chi(T)$ has the partial fraction decomposition

$$f_\chi(T) = \frac{1}{f} \sum_{i=1}^{f-1} \frac{g(u_i)}{u_i T - 1}, \quad (4.12)$$

where the u_i are the nontrivial f -th roots of unity and $g(u_i) = \sum_{a=1}^{f-1} \chi(a) u_i^{-a}$. Since

$$\varphi\left(\frac{1}{u_i T - 1}\right) = \frac{1}{u_i T - 1} - \frac{1}{u_i^p T^p - 1} \quad (4.13)$$

and $g(u_i) = \chi(p)g(u_i^p)$ for $1 \leq i < f$, we conclude that

$$\varphi f_\chi(T) = f_\chi(T) - \chi(p) f_\chi(T^p). \quad (4.14)$$

From (4.10) we see that

$$f_\chi(e^t) = \sum_{n=0}^{\infty} \frac{B_{n+1, \chi}}{n+1} \frac{t^n}{n!}, \quad (4.15)$$

so if $f(T) = f_\chi(T)$ then $a_n = B_{n+1, \chi}/(n+1)$, and from (4.14) it readily follows that $\hat{a}_n = (1 - \chi(p)p^m) a_n$. Taking $m = n+1$ and applying Theorem 1.2 gives the result.

Remark. Under the hypotheses of this theorem the more classical Kummer congruences

$$\Delta_c^k \left\{ (1 - \chi(p)p^{m-1}) \frac{B_{m, \chi}}{m} \right\} \equiv 0 \pmod{p^{ka'} \mathfrak{D}_K} \quad (4.16)$$

also follow from this proof.

5. HIGHER ORDER BERNOULLI NUMBERS.

In this section we generalize the Kummer congruences to the higher order Bernoulli numbers $B_n^{(w)}$ in the case where $0 \leq w \leq n$. This is the most interesting case, since the Bernoulli numbers may be expressed in terms of Stirling numbers when $w < 0$ or when $n < w$ (cf. [6], §2). In this section p will denote an odd prime.

Let a nonnegative integer m and a positive integer w be given, and define

$$J = J(m, w) = \{j \in \{1, 2, \dots, w\} : p-1 \mid m+j\}; \quad (5.1)$$

$$M = M(m, w) = \max_{j \in J} \{1 + \text{ord}(m+j)\}; \quad (5.2)$$

$$E = E(m, w) = \sum_{j \in J \cup \{w\}} k(j, m, w), \quad (5.3)$$

$$\text{where } k(j, m, w) = \begin{cases} \max\{1 + \text{ord}(m+j) - \text{ord } j, 0\}, & \text{if } j \in J \text{ and } j \neq w, \\ 1 + \text{ord}(m+j) - \text{ord } j, & \text{if } j = w \in J, \\ -\text{ord } j, & \text{if } j = w \notin J. \end{cases} \quad (5.4)$$

By definition we set $M = 0$ if J is empty.

Suppose that $0 \leq m \leq n$ and $m \equiv n \pmod{(p-1)p^a}$ for some nonnegative integer a . Observe that $E(m, w) = E(n, w)$ if $a \geq M$.

THEOREM 5.1. *For all $m \geq 0$,*

$$\frac{B_{m+w}^{(w)}}{(m+1)_w} \in p^{-E} \mathbb{Z}_p,$$

where $(m+1)_w = (m+w)!/m!$ is the Pochhammer symbol. Furthermore, if $0 \leq m \leq n$ and $m \equiv n \pmod{(p-1)p^a}$ with $a \geq M$, then

$$\frac{B_{m+w}^{(w)}}{(m+1)_w} \equiv \frac{B_{n+w}^{(w)}}{(n+1)_w} \pmod{p^C \mathbb{Z}_p},$$

where $C = \min\{m - E, a + 1 - M - E\}$.

Proof. Let a, m, n, w be given as described above. Let b denote a primitive root modulo p^{a+1} , and note that this implies $\text{ord}(b^{(p-1)p^e} - 1) = e + 1$ for $0 \leq e \leq a$. As in (4.3), we have

$$\frac{b}{T^b - 1} \in \frac{1}{T - 1} + \mathbb{Z}_p[[T - 1]]. \quad (5.5)$$

Therefore for any positive integer w , we may use the binomial expansion to write

$$\left(\frac{b}{T^b - 1}\right)^w = \frac{1}{(T - 1)^w} + \frac{c_{w-1}}{(T - 1)^{w-1}} + \cdots + \frac{c_1}{(T - 1)} + f(T), \quad (5.6)$$

where $c_1, \dots, c_{w-1} \in \mathbb{Z}_p$ and $f(T)$ is a rational function which also lies in $\mathbb{Z}_p[[T - 1]]$. From the binomial expansion we observe that if $\text{ord } w = r > 0$ then $\text{ord } c_{w-i} \geq r + 1 - s$ for $1 \leq i < p^s$ if $s \leq r$.

Now we substitute $T = e^t$ and expand as formal power series, giving

$$\begin{aligned} t^{-w} \sum_{n=0}^{\infty} (b^n - 1) B_n^{(w)} \frac{t^n}{n!} &= c_{w-1} t^{1-w} \sum_{n=0}^{\infty} B_n^{(w-1)} \frac{t^n}{n!} + \cdots \\ &+ c_1 t^{-1} \sum_{n=0}^{\infty} B_n^{(1)} \frac{t^n}{n!} + \sum_{n=0}^{\infty} a_n \frac{t^n}{n!}, \end{aligned} \quad (5.7)$$

where each $a_n \in \mathbb{Z}_p$. For each $m \geq 0$, equating coefficients of $t^m/m!$ yields

$$(b^{m+w} - 1) \frac{B_{m+w}^{(w)}}{(m+1)_w} = c_{w-1} \frac{B_{m+w-1}^{(w-1)}}{(m+1)_{w-1}} + \cdots + c_1 \frac{B_{m+1}^{(1)}}{m+1} + a_m. \quad (5.8)$$

Since $f(T)$ is a rational function in $\mathbb{Z}_p[[T-1]]$ and $f(e^t) = \sum_n a_n \frac{t^n}{n!}$, from Theorem 1.1 with $k = 1$ we deduce a congruence $a_m \equiv a_n \pmod{p^A \mathbb{Z}_p}$ when $m \equiv n \pmod{(p-1)p^a}$, where $A = \min\{m, a+1\}$. When $w = 1$ the equality (5.8) is

$$(b^{m+1} - 1) \frac{B_{m+1}^{(1)}}{m+1} = a_m, \quad (5.9)$$

and therefore

$$(b^{m+1} - 1) \frac{B_{m+1}^{(1)}}{m+1} \equiv (b^{n+1} - 1) \frac{B_{n+1}^{(1)}}{n+1} \pmod{p^A \mathbb{Z}_p}, \quad (5.10)$$

or equivalently,

$$(b^{m+1} - 1) \frac{B_{m+1}^{(1)}}{m+1} \equiv (b^{m+1} - 1) \frac{B_{n+1}^{(1)}}{n+1} + (b^{n+1} - b^{m+1}) \frac{B_{n+1}^{(1)}}{n+1} \pmod{p^A \mathbb{Z}_p}. \quad (5.11)$$

If $m, n \not\equiv -1 \pmod{p-1}$, then $E = M = 0$ and $\text{ord}(b^{m+1} - 1) = \text{ord}(b^{n+1} - 1) = 0$, so $B_{m+1}^{(1)}/(m+1)$ and $B_{n+1}^{(1)}/(n+1)$ lie in \mathbb{Z}_p . Since $m \equiv n \pmod{(p-1)p^a}$, we have $\text{ord}(b^{n+1} - b^{m+1}) = a+1$, so

$$\frac{B_{m+1}^{(1)}}{m+1} \equiv \frac{B_{n+1}^{(1)}}{n+1} \pmod{p^A \mathbb{Z}_p}, \quad (5.12)$$

and the theorem holds for $w = 1$ in this case, since $C = A$.

Suppose that $m \equiv n \equiv -1 \pmod{(p-1)p^e}$ with $0 \leq e \leq a$; then $\text{ord}(b^{m+1} - 1) = e+1$. In this situation $E = M = e+1$, and from (5.9) we see that $B_{m+1}^{(1)}/(m+1)$ and $B_{n+1}^{(1)}/(n+1)$ lie in $p^{-E} \mathbb{Z}_p$. Since $m \equiv n \pmod{(p-1)p^a}$, we have $\text{ord}(b^{n+1} - b^{m+1}) = a+1$, so from (5.11) we have

$$(b^{m+1} - 1) \frac{B_{m+1}^{(1)}}{m+1} \equiv (b^{m+1} - 1) \frac{B_{n+1}^{(1)}}{n+1} \pmod{p^{\min\{m, a+1-E\}} \mathbb{Z}_p}, \quad (5.13)$$

and therefore

$$\frac{B_{m+1}^{(1)}}{m+1} \equiv \frac{B_{n+1}^{(1)}}{n+1} \pmod{p^C \mathbb{Z}_p}, \quad (5.14)$$

completing the proof of the theorem for $w = 1$.

Now suppose that $w > 1$. For $1 \leq t \leq w - 1$ define

$$E' = E'(m, t) = \sum_{j \in J(m, t)} k(j, m, w), \quad (5.15)$$

and observe that we always have $E'(m, t) \geq E(m, t)$; also note that $E'(m, t) = E(m, t)$ if p does not divide t , or if $p - 1$ divides $m + t$ and $\text{ord } t \leq 1 + \text{ord } (m + t)$, and $E'(m, t) > E(m, t)$ in all other cases. Since each $k(j, m, w)$ appearing in (5.15) is nonnegative, it is also clear that for m and w fixed, $E'(m, t)$ is a nondecreasing function of t for $1 \leq t \leq w - 1$ (whereas $E(m, t)$ is not), so that $E'(m, w - 1) = \max_{1 \leq t < w} \{E'(m, t)\}$. Furthermore, we note that $E'(m, t) > E'(m, t - 1)$ only if $p - 1$ divides $m + t$ and $1 + \text{ord } (m + j) > \text{ord } j$.

If $\text{ord } w = r > 0$, we have noted that $\text{ord } c_{w-i} \geq r + 1 - s$ when $1 \leq i < p^s$ with $s \leq r$. We now claim that if $\text{ord } w = r > 0$, then the function $F(m, t)$ defined for $1 \leq t \leq w - 1$ by

$$F(m, t) = \begin{cases} E(m, t) - r - 1 + s, & \text{if } p^{s-1} \leq w - t < p^s \text{ with } s \leq r, \\ E(m, t) & \text{if } w - t \geq p^r, \end{cases} \quad (5.16)$$

attains its maximum value at $t = w - 1$. For $1 \leq j \leq p - 1$, we have

$$\begin{aligned} F(m, w - 1) &= E(m, w - 1) - r = E'(m, w - 1) - r \\ &\geq E'(w - j) - r = E(m, w - j) - r = F(m, w - j). \end{aligned} \quad (5.17)$$

If $p - 1$ does not divide $m + w - p$ then

$$E(m, w - 1) = E'(m, w - 1) \geq E'(m, w - p) > E(m, w - p). \quad (5.18)$$

If $p - 1$ divides $m + w - p$, then $p - 1$ divides $m + w - 1$ as well, and since p cannot divide $w - 1$ we have

$$E(m, w - 1) = E'(m, w - 1) > E'(m, w - 2) \geq E'(m, w - p) \geq E(m, w - p). \quad (5.19)$$

Thus in either case we have $E(m, w - 1) > E(m, w - p)$, so that

$$F(m, w - 1) = E(m, w - 1) - r \geq E(m, w - p) + 1 - r = F(m, w - p). \quad (5.20)$$

If $F(m, w - 1) < F(m, w - p - 1)$ then we must have $E'(m, w - p - 1) = E'(m, w - 1)$. Since at least one of $\{w - 1, w - 2, \dots, w - p - 1\}$ must lie in $J(m, w - 1)$, we will have $E'(m, w - p - 1) < E'(m, w - 1)$

unless all such elements j are divisible by p and satisfy $\text{ord } j > \text{ord } (m+j)$. This requires $w-p \in J$, but then $w-1 \in J$ as well; however, p cannot divide $w-1$. This contradiction shows that $F(m, w-1) \geq F(m, w-p-1)$.

Clearly $F(m, w-p^{s-1}-1) \geq F(m, w-j)$ for $p^{s-1}+1 \leq j \leq p^s-1$. For $1 < s \leq r$, the set $\{w-p^{s-1}-1, w-p^{s-1}-2, \dots, w-p^s+1\}$ contains at most p^{s-2} numbers t such that p divides t and $p-1$ divides $m+t$, and therefore at least $p^{s-2}(p-1)-1$ numbers t such that $p-1$ divides $m+t$ and p does not divide t . Since E' is nondecreasing and $E'(m, t) > E'(m, t-1)$ for all such t , and $p^{s-2}(p-1)-1 \geq 1$ for $s > 1, p > 2$, we have

$$\begin{aligned} E(m, w-p^{s-1}-1) &= E'(m, w-p^{s-1}-1) \geq E'(m, w-p^s+1) + 1 \\ &= E(m, w-p^s+1) + 1, \end{aligned} \tag{5.21}$$

so that

$$F(m, w-p^{s-1}-1) = E(m, w-p^{s-1}-1) - 1 - r + s \geq E'(m, w-p^s+1) - r + s. \tag{5.22}$$

Since $E'(m, w-p^s+1) \geq E'(m, w-p^s) \geq E'(m, w-p^s)$ and $E'(m, w-p^s+1) \geq E'(m, w-p^s-1) = E'(m, w-p^s-1)$, we obtain $F(m, w-p^{s-1}-1) \geq F(m, w-p^s)$ and $F(m, w-p^{s-1}-1) \geq F(m, w-p^s-1)$ for $1 < s \leq r$. But since $F(m, w-p^r-1) = E'(m, w-p^r-1)$ if $w > p^r$ and $E'(m, w-p^r-1) \geq E'(m, w-j) \geq E(m, w-j)$ for all $j \geq p^r+1$, we see that $F(m, w-1) \geq F(m, w-j)$ for all $j, 1 \leq j \leq w-1$.

Assume now that the theorem has been proven for all positive integer orders less than w . Denoting the right member of (5.8) by $R(m)$, the facts that $F(m, w-1) = \max_{1 \leq t < w} \{F(m, t)\}$ and $E'(m, w-1) = \max_{1 \leq t < w} \{E'(m, t)\}$ imply that $R(m) \in p^{-F'} \mathbb{Z}_p$ and $R(m) \equiv R(n) \pmod{p^{C'} \mathbb{Z}_p}$, where

$$F' = \begin{cases} E(m, w-1), & \text{if } \text{ord } w = 0, \\ F(m, w-1), & \text{if } \text{ord } w > 0, \end{cases} \tag{5.23}$$

$M' = M(m, w-1)$, and $C' = \min\{m-F', a+1-M'-F'\}$. If $m, n \not\equiv -w \pmod{p-1}$, then $\text{ord}(b^{m+w}-1) = 0$, $E = F'$, and $M = M'$. If $m \equiv n \equiv -w \pmod{(p-1)p^e}$ with $0 \leq e \leq a$, then $\text{ord}(b^{m+w}-1) = e+1$, $E = F' + e + 1$, and $M = \max\{M', e+1\}$. In either case, from (5.8) we

see that $B_{m+w}^{(w)}/(m+1)_w$ lies in $p^{-E}\mathbb{Z}_p$. From (5.8) and the induction hypothesis we also have

$$(b^{m+w} - 1) \frac{B_{m+w}^{(w)}}{(m+1)_w} \equiv (b^{m+w} - 1) \frac{B_{n+w}^{(w)}}{(n+1)_w} + (b^{n+w} - b^{m+w}) \frac{B_{n+w}^{(w)}}{(n+1)_w} \pmod{p^{C'}\mathbb{Z}_p}. \quad (5.24)$$

Since $m \equiv n \pmod{(p-1)p^a}$, we have $\text{ord}(b^{n+w} - b^{m+w}) = a+1$, so

$$(b^{m+w} - 1) \frac{B_{m+w}^{(w)}}{(m+1)_w} \equiv (b^{m+w} - 1) \frac{B_{n+w}^{(w)}}{(n+1)_w} \pmod{p^{\min\{C', a+1-E\}}\mathbb{Z}_p}. \quad (5.25)$$

Then since $\min\{C', a+1-E\} - \text{ord}(b^{m+w} - 1) = \min\{m-F', a+1-M'-F', a+1-E\} - (E-F') = \min\{m-E, a+1-M-E\} = C$, we have

$$\frac{B_{m+w}^{(w)}}{(m+1)_w} \equiv \frac{B_{n+w}^{(w)}}{(n+1)_w} \pmod{p^C\mathbb{Z}_p}, \quad (5.26)$$

so the theorem holds for order w . Thus the theorem holds for all positive integer orders.

Remarks. The divisibility statement of this theorem also may be modified to include $B_r^{(w)}$ when $0 \leq r \leq w$ via (5.7). Specifically, for $0 \leq r \leq w$ write $r = m+w$ where $-w \leq m \leq 0$, and replace the set $J(m, w)$ with

$$J^+(m, w) = \{j \in \{1, 2, \dots, w\} : m+j > 0 \text{ and } p-1 \mid m+j\}, \quad (5.27)$$

and define $E = E(m, w)$ as in (5.3) with J replaced by J^+ . Then equating coefficients of t^{r-w} in (5.7) yields

$$(b^r - 1) \frac{B_r^{(w)}}{r!} = c_{w-1} \frac{B_{r-1}^{(w-1)}}{(r-1)!} + \dots + c_1 \frac{B_{r+1-w}^{(1)}}{(r+1-w)!} + a_{r-w}, \quad (5.28)$$

where we interpret all terms $B_k^{(s)}$ and a_k to be zero if $k < 0$. Since $B_0^{(w)} = 1$, it is easily proven by induction on r that

$$\frac{B_r^{(w)}}{r!} \in p^{-E}\mathbb{Z}_p. \quad (5.29)$$

The divisibility statement of this theorem is not best possible in all cases, but is presented as a reference point against which to measure the strength of the congruences. Specifically, if one views the terms $B_{m+w}^{(w)}/(m+1)_w$ and $B_{n+w}^{(w)}/(n+1)_w$ as elements of $p^{-E}\mathbb{Z}_p$, then the congruences are specifying p -adic agreement of these terms to d digits, where $d = \min\{m, a+1-M\}$. However, despite its crudity, it does complement the known bounds in an interesting manner.

A. Adelberg has shown that

$$\text{ord } B_{m+w}^{(w)} \geq - \left\lfloor \left\lfloor \frac{S(m+w)}{p-1} \right\rfloor \right\rfloor \quad (5.30)$$

([1], Remark 2, p. 337), and this result has also been obtained independently by F. T. Howard ([6], Theorem 3.5); here $S(m+w)$ denotes the sum of the base p digits of the integer $m+w$ and $\lfloor \cdot \rfloor$ denotes the greatest integer function. Howard's result also showed that if p^j divides w but p does not divide m , then

$$\text{ord } B_{m+w}^{(w)} \geq j - \left\lfloor \left\lfloor \frac{S(m+w)}{p-1} \right\rfloor \right\rfloor, \quad (5.31)$$

and Adelberg ([2], Theorem 2.1(i)) showed that (5.31) holds when p^j divides w and $(p-1)p$ does not divide $m+w$. For fixed $m > 0$, these results provide a better asymptotic bound as $w \rightarrow \infty$ than does the bound

$$\text{ord } B_{m+w}^{(w)} \leq \text{ord } (m+1)_w - E \quad (5.32)$$

obtained from the divisibility statement of Theorem 5.1; indeed (5.30) and (5.31) show that $\text{ord } B_{m+w}^{(w)} \geq -\log_p(m+w+1)$, which is not apparent from (5.32). By means of the well-known result $\text{ord } (n!) = (n - S(n))/(p-1)$, (5.32) may be rewritten as

$$\text{ord } B_{m+w}^{(w)} \geq \left\lfloor \left\lfloor \frac{S(m)}{p-1} \right\rfloor \right\rfloor - \left\lfloor \left\lfloor \frac{S(m+w)}{p-1} \right\rfloor \right\rfloor - \sum_{j \in J} (k(j, m, w) - 1) \quad (5.33)$$

if $w \in J$, and if $w \notin J$ then

$$\text{ord } B_{m+w}^{(w)} \geq \text{ord } w + \left\lfloor \left\lfloor \frac{S(m)}{p-1} \right\rfloor \right\rfloor - \left\lfloor \left\lfloor \frac{S(m+w)}{p-1} \right\rfloor \right\rfloor - \sum_{j \in J} (k(j, m, w) - 1). \quad (5.34)$$

So in the case $m = 0$, for example, we observe that (5.33), (5.34) agree precisely with the bound (5.30), (5.31) for all w , since $k(j, 0, w) = 1$ for all $j \in J(0, w)$. For fixed $m \neq 0$, (5.33), (5.34) are sometimes better than (5.30), (5.31) due to the beneficial term $\lfloor \lfloor S(m)/(p-1) \rfloor \rfloor$, but (5.33), (5.34) are often worse than (5.30), (5.31) due to the "detrimental" term $\sum_{j \in J} (k(j, m, w) - 1)$. If m is fixed with $\text{ord } m = s$, then this term is asymptotic to $w/p^{s+1}(p-1)^2$, as will be shown in Proposition 5.2 below.

On the other hand, if w is fixed and $m \rightarrow \infty$, the right side of (5.31) is bounded above by $j = \text{ord } w$; that is, (5.31) does not produce arbitrarily large positive ordinals for $B_{m+w}^{(w)}$ if w is fixed, and indeed does not predict any positive ordinal for $B_{m+w}^{(w)}$ unless p divides w . But if $w > 0$ is given, choose (for example) $m = p^N - 1$, where N is large enough so that $m > w$. Then $\llbracket S(m+w)/(p-1) \rrbracket \leq \log_p(w+1)$ for any such N and $\sum_{j \in J} (k(j, m, w) - 1)$ is likewise independent of N (since $p^N \equiv 1 \pmod{p-1}$ for all N and $\text{ord}(p^N + k) = \text{ord } k$ for $0 < k < p^N$), whereas $\llbracket S(m)/(p-1) \rrbracket = N$. Therefore, for any fixed w , (5.33) explicitly produces values of m for which $B_{m+w}^{(w)}$ has positive ordinal, and also for which $\text{ord } B_{m+w}^{(w)}$ is arbitrarily large. We do not know of any other general bound for $\text{ord } B_n^{(w)}$ with this property.

For any fixed w one may find values of m for which the term $\sum_{j \in J} (k(j, m, w) - 1)$ in (5.33), (5.34) is actually negative (and therefore beneficial to the bound); however in general this term will be positive. Below we describe the asymptotic behavior of this term for fixed m .

PROPOSITION 5.2. *If $m > 0$ is fixed with $\text{ord } m = s$, then the term $\sum_{j \in J} (k(j, m, w) - 1)$ in (5.33), (5.34) is asymptotic to $w/p^{s+1}(p-1)^2$ as $w \rightarrow \infty$.*

Proof. With the possible exception of the term $j = w$, the sum is

$$\sum_{j \in J} \max\{\text{ord}(m+j) - \text{ord } j, -1\}. \quad (5.35)$$

If $\text{ord } j < \text{ord } m$, then $\text{ord}(m+j) = \text{ord } j$ and the contribution to the sum is zero. If $\text{ord } j = \text{ord } m$, then $\text{ord}(m+j) \geq \text{ord } j$ and the contribution to the sum is $\text{ord}(m+j) - \text{ord } j$. If $\text{ord } j > \text{ord } m$, then $\text{ord}(m+j) < \text{ord } j$ and the contribution to the sum is -1 . Therefore for $\text{ord } m = s$ the sum (5.35) becomes

$$\sum_{\substack{(p-1)|(m+j) \\ \text{ord } j = s \\ 1 \leq j \leq w}} (\text{ord}(m+j) - \text{ord } j) - \sum_{\substack{(p-1)|(m+j) \\ \text{ord } j \geq s+1 \\ 1 \leq j \leq w}} 1. \quad (5.36)$$

The second sum in (5.36) is clearly asymptotic to $w/p^{s+1}(p-1)$. In the first sum of (5.36), write $m = ap^s$, $j = bp^s$ with $(a, p) = (b, p) = 1$. Then $m+j \equiv a+b \pmod{p-1}$ and $\text{ord}(m+j) - \text{ord } j =$

$\text{ord}(a+b)$, so

$$\sum_{\substack{(p-1)|(m+j) \\ \text{ord } j=s \\ 1 \leq j \leq w}} (\text{ord}(m+j) - \text{ord } j) = \sum_{\substack{(p-1)|(a+b) \\ \text{ord } b=0 \\ 1 \leq b \leq \lceil w/p^s \rceil}} \text{ord}(a+b) = \sum_{\substack{(p-1)|(a+b) \\ 1 \leq b \leq \lceil w/p^s \rceil}} \text{ord}(a+b), \quad (5.37)$$

the second equality holding because if $\text{ord } b > 0$ then $\text{ord}(a+b) = 0$. This last sum in (5.37) equals $\text{ord}(\lceil (a + \lceil w/p^s \rceil)/(p-1) \rceil!) - \text{ord}(\lceil a/(p-1) \rceil!)$. Using the fact that $\text{ord}(n!) = (n - S(n))/(p-1)$, we see that this sum is asymptotic to $w/p^s(p-1)^2$. So the difference of sums in (5.36) is asymptotic to $w/p^{s+1}(p-1)^2$. Since the term $j = w$ changes the sum by at most $\text{ord } w$, the result follows.

As a further corollary to the divisibility result of Theorem 5.1, we observe that its $w = p$ case implies a result of L. Carlitz ([3], §6), giving sufficient conditions for $B_n^{(p)}$ to lie in \mathbb{Z}_p . (Carlitz also proved that these conditions are necessary for $B_n^{(p)} \in \mathbb{Z}_p$ when $n > p$).

COROLLARY 5.3. (Carlitz). *For all $n \geq 0$, $B_n^{(p)} \in \mathbb{Z}_p$ unless $n \equiv 0 \pmod{p-1}$ and $n \equiv 0, -1 \pmod{p}$, in which case $B_n^{(p)} \in p^{-1}\mathbb{Z}_p$.*

Proof. First assume $n \geq p$ and write $n = m + p$. If $n \not\equiv 0 \pmod{p-1}$, then $J = J(m, p)$ consists of a single term, so $E = 1 + \text{ord}(m + j_0) - 1$ for some j_0 , $1 \leq j_0 \leq p$. But $\text{ord}(m+1)_p \geq \text{ord}(m + j_0)$, so by the divisibility statement of Theorem 5.1 we have $B_n^{(p)} \in \mathbb{Z}_p$.

Suppose $n \equiv 0 \pmod{p-1}$; then $E = E(m, p) = 1 + \text{ord}(m+1) + \text{ord}(m+p)$. If $m \not\equiv 0, -1 \pmod{p}$ then $E = 1$, and since $\text{ord}(m+1)_p \geq 1$ we have $B_n^{(p)} \in \mathbb{Z}_p$ by the divisibility statement of Theorem 5.1. In the case $m \equiv 0$ (resp. -1) \pmod{p} we have $E = 1 + \text{ord}(m+p)$ (resp. $E = 1 + \text{ord}(m+1)$), whereas $\text{ord}(m+1)_p = \text{ord}(m+p)$ (resp. $\text{ord}(m+1)_p = \text{ord}(m+1)$), showing that $B_n^{(p)} \in p^{-1}\mathbb{Z}_p$.

In the case $0 \leq n < p$, we have $B_n^{(p)}/n! \in p^{-E}\mathbb{Z}_p$ as in (5.29) by the remark following Theorem 5.1, where $E = E(n-p, p)$. Since $E(n-p, p) = 0$ when $0 \leq n < p$, the result follows in this case.

We now extend the result of Theorem 5.1 to treat the action of powers of Δ_c on the higher-order Bernoulli numbers.

THEOREM 5.4. *If $m \geq 0$, $w > 0$, and $c \equiv 0 \pmod{(p-1)p^a}$ with $a \geq M$, then for all $k \geq 0$ we have*

$$\Delta_c^k \left\{ \frac{B_{m+w}^{(w)}}{(m+1)_w} \right\} \equiv 0 \pmod{p^C \mathbb{Z}_p},$$

where $C = \min\{m - E, k(a + 1 - M) - E\}$.

Proof. This has been proven for $k = 0, 1$ in Theorem 5.1. Assume now that $k > 1$ and the theorem has been proven for all positive integers less than k . We require the identity

$$\Delta_c^k\{X_m Y_m\} = \sum_{i=0}^k \binom{k}{i} \Delta_c^i\{X_m\} \Delta_c^{k-i}\{Y_{m+ic}\}, \quad (5.38)$$

which follows from the definition (1.6) of Δ_c^k . Specifically, using (1.6) to expand the right side of (5.38), one finds the coefficient of $X_{m+jc} Y_{m+hc}$ to be

$$(-1)^{k-h} \binom{k}{j, k-h, h-j} \sum_{s=0}^{h-j} \binom{h-j}{s} (-1)^s, \quad (5.39)$$

which is zero if $j \neq h$ and equals $(-1)^{k-j} \binom{k}{j}$ if $j = h$. Applying this identity in (5.9) with $X_m = b^{m+1} - 1$ and $Y_m = B_{m+1}^{(1)}/(m+1)$ yields

$$(b^{m+1} - 1) \Delta_c^k \left\{ \frac{B_{m+1}^{(1)}}{m+1} \right\} = \Delta_c^k a_m - \sum_{i=1}^k \binom{k}{i} \Delta_c^i \{b^{m+1}\} \Delta_c^{k-i} \left\{ \frac{B_{m+ic+1}^{(1)}}{m+ic+1} \right\}. \quad (5.40)$$

Observe that $\Delta_c^i \{b^{m+1}\} \equiv 0 \pmod{p^{i(a+1)}\mathbb{Z}}$, and by Theorem 1.1 we have $\Delta_c^k a_m \equiv 0 \pmod{p^A \mathbb{Z}_p}$, where $A = \min\{m, k(a+1)\}$. By the induction hypothesis $\text{ord} \Delta_c^{k-i} \{B_{m+ic+1}^{(1)}/(m+ic+1)\}$ is at least $\min\{m - E, (k-i)(a+1 - M) - E\}$ for $i > 0$, so the p -adic ordinal of the sum in (5.40) is at least $\min\{a+1 + m - E, a+1 + (k-1)(a+1 - M) - E\}$, and therefore

$$\text{ord} (b^{m+1} - 1) \Delta_c^k \left\{ \frac{B_{m+1}^{(1)}}{m+1} \right\} \geq \min\{m, (a+1) + (k-1)(a+1 - M) - E\}, \quad (5.41)$$

since $M = E \leq a$. Since $M = E = \text{ord} (b^{m+1} - 1)$ it follows that

$$\text{ord} \Delta_c^k \left\{ \frac{B_{m+1}^{(1)}}{m+1} \right\} \geq \min\{m - E, k(a+1 - M) - E\}, \quad (5.42)$$

so the theorem is true for the k -th power in the case $w = 1$. Now assume that $w > 1$ and the theorem has also been proved for the k -th power for all positive integer orders less than w . Applying the identity (5.38) in equation (5.8) yields

$$(b^{m+w} - 1) \Delta_c^k \left\{ \frac{B_{m+w}^{(w)}}{(m+1)_w} \right\} = \Delta_c^k \{R(m)\} - \sum_{i=1}^k \binom{k}{i} \Delta_c^i \{b^{m+w}\} \Delta_c^{k-i} \left\{ \frac{B_{m+ic+w}^{(w)}}{(m+ic+1)_w} \right\}, \quad (5.43)$$

where $R(m)$ denotes the right member of (5.8) as in the proof of Theorem 5.1. By the induction hypotheses $\Delta_c^k \{R(m)\} \equiv 0 \pmod{p^{C'} \mathbb{Z}_p}$ where $C' = \min\{m - F', k(a + 1 - M') - F'\}$ with $F' = F'(m, w - 1)$, $M' = M(m, w - 1)$ as in the proof of Theorem 5.1, and the p -adic ordinal of the sum in (5.43) is at least $\min\{a + 1 + m - E, a + 1 + (k - 1)(a + 1 - M) - E\}$. Therefore we have

$$\text{ord}(b^{m+w} - 1) \Delta_c^k \left\{ \frac{B_{m+w}^{(w)}}{(m+1)_w} \right\} \geq \min\{m - F', k(a + 1 - M') - F', (a + 1) + (k - 1)(a + 1 - M) - E\}. \quad (5.44)$$

Noting that either $M = M'$ or $M = \text{ord}(b^{m+w} - 1)$, and that $\text{ord}(b^{m+w} - 1) = E - F'$, we finally obtain

$$\text{ord} \Delta_c^k \left\{ \frac{B_{m+w}^{(w)}}{(m+1)_w} \right\} \geq \min\{m - E, k(a + 1 - M) - E\}, \quad (5.45)$$

demonstrating the theorem for k -th power and order w . By induction the theorem for k -th power is proven for all w , which completes the proof for all k .

We conclude by extending these results to $B_n^{(w)}(x)$ for $x \in \mathbb{Z}_p$.

THEOREM 5.5. *For all $m \geq 0$ and all $x \in \mathbb{Z}_p$,*

$$\frac{B_{m+w}^{(w)}(x)}{(m+1)_w} \in p^{-E^*} \mathbb{Z}_p,$$

and if $c \equiv 0 \pmod{(p-1)p^a}$ with $a \geq M$, then for all $k \geq 0$ we have

$$\Delta_c^k \left\{ \frac{B_{m+w}^{(w)}(x)}{(m+1)_w} \right\} \equiv 0 \pmod{p^{C^*} \mathbb{Z}_p},$$

where $C^* = \min\{m - E^*, k(a + 1 - M) - E^*\}$, and

$$E^* = E^*(m, w) = \sum_{j \in J} \max\{1 + \text{ord}(m + j) - \text{ord} j, 0\}.$$

Proof. Since the set of nonnegative integers is dense in \mathbb{Z}_p , it suffices to prove the statements for nonnegative integers x . The theorem is certainly true for $x = 0$ by Theorems 5.1 and 5.4. Assume that the statement is true for all $m \geq 0$ and all $w > 0$ for some nonnegative integer x . From the well-known identity

$$B_n^{(w)}(x + 1) = B_n^{(w)}(x) + n B_{n-1}^{(w-1)}(x) \quad (5.46)$$

([6], eq. 2.3), we deduce

$$\frac{B_{m+w}^{(w)}(x+1)}{(m+1)_w} = \frac{B_{m+w}^{(w)}(x)}{(m+1)_w} + \frac{B_{m+w-1}^{(w-1)}(x)}{(m+1)_{w-1}}. \quad (5.47)$$

Since $E^*(m, w) = \max\{E(m, w), E(m, w-1)\}$, the two statements for $x+1$ follow from the induction hypothesis and (5.47). By induction the theorem holds for all nonnegative integers x , and then by continuity it holds for all $x \in \mathbb{Z}_p$.

REFERENCES

1. A. ADELBERG, On the degrees of irreducible factors of higher order Bernoulli polynomials, *Acta Arith.*, **62** (1992), 329-342.
2. A. ADELBERG, Congruences of p -adic integer order Bernoulli numbers, *J. Number Theory*, **59** (1996), 374-388.
3. L. CARLITZ, Some theorems on Bernoulli numbers of higher order, *Pacific J. Math.*, **2** (1952), 127-139.
4. B. DWORK, "Lectures on p -adic Differential Equations", Springer-Verlag, New York, 1982.
5. H. S. GUNARATNE, A new generalisation of the Kummer congruence, in "Computational Algebra and Number Theory", pp. 255-265, Math. Appl. **325**, Kluwer Academic Publishers, Dordrecht, 1995.
6. F. T. HOWARD, Congruences and recurrences for Bernoulli numbers of higher order, *Fib. Q.*, **32** (1994), 316-328.
7. N. E. NÖRLUND, "Differenzenrechnung", Springer, Berlin, 1924.
8. H. TSUMURA, On a p -adic interpolation of the generalized Euler numbers and its applications, *Tokyo J. Math.*, **10** (1987), 281-293.
9. H. TSUMURA, On some congruences for the Bell numbers and for the Stirling numbers, *J. Number Theory*, **38** (1991), 206-211.
10. L. WASHINGTON, "Introduction to Cyclotomic Fields", Springer-Verlag, New York, 1982.