Degenerate and n-adic versions of Kummer's congruences for values of Bernoulli polynomials

Paul Thomas Young

Department of Mathematics, College of Charleston
Charleston, SC 29424

Abstract

We first prove an analogue of Kummer's congruences for expressions involving the degenerate Bernoulli polynomials which were introduced by L. Carlitz, by relating them to the general theory of "degenerate number sequences" developed in a recent article. These congruences extend, for example, known congruences for the Genocchi numbers. We also give versions of Kummer's congruences modulo powers of a general positive integer n for Bernoulli polynomials with n-adic integer argument, and similar congruences for generalized Bernoulli polynomials, which extend recent results of Z.-W. Sun and of the author.

Keywords: Bernoulli polynomials; Degenerate Bernoulli polynomials; Kummer congruences; n-adic numbers

1. Introduction

The Bernoulli polynomials $B_m(x)$ may be defined by the generating function

$$\left(\frac{t}{e^t-1}\right)e^{xt}=\sum_{m=0}^{\infty}B_m(x)\frac{t^m}{m!} \tag{1.1}$$

and their values at $x=0$ are called the Bernoulli numbers and denoted B_m. These polynomials arise in formulas for sums of powers of consecutive integers; specifically we have

$$\sum_{a=0}^{N}a^m=\frac{1}{m+1}\left[B_{m+1}(N+1)-B_{m+1}\right] \tag{1.2}$$

for any nonnegative integers m and N. For an odd prime p a general version (cf. [19]) of Kummer's congruences states that if $m\equiv m' \pmod{(p-1)p^a}$ and $p-1$ does not divide $m+1$ then

$$\frac{B_{m+1}}{m+1}\equiv\frac{B_{m'+1}}{m'+1}\pmod{p^A\mathbb{Z}_p} \tag{1.3}$$

where $A=\min\{m,m',a+1\}$. In [4] Carlitz defined the *degenerate Bernoulli polynomials* $\beta_m(\lambda,x)$ for $\lambda\neq 0$ by means of the generating function

$$\left(\frac{t}{(1+\lambda t)^{\mu}-1}\right)(1+\lambda t)^{\mu x}=\sum_{m=0}^{\infty}\beta_m(\lambda,x)\frac{t^m}{m!} \tag{1.4}$$

where $\lambda\mu = 1$. Since $(1+\lambda t)^\mu \to e^t$ as $\lambda \to 0$ it is evident that $\beta_m(0,x) = B_m(x)$. The degenerate Bernoulli polynomials are related to sums of generalized falling factorials $(a|\lambda)_m$ by

$$\sum_{a=0}^{N}(a|\lambda)_m = \frac{1}{m+1}\left[\beta_{m+1}(\lambda, N+1) - \beta_{m+1}(\lambda, 0)\right] \tag{1.5}$$

(cf. ([4], eq. (5.4))). Adelberg [1] interpreted these polynomials as divided differences of binomial coefficients, and Howard [13] gave explicit formulas and recurrences for them. In [23] we developed a general notion of "degenerate number sequences" and used a p-adic integral representation for such sequences to deduce congruences for them similar to Kummer's. In the first part of this paper we apply these techniques to deduce analogues of Kummer's congruences (1.3) for the polynomials $\beta_m(\lambda, x)$. While the congruences (1.3) are trivial for even m (since $B_{2k+1} = 0$ for all $k > 0$), our generalization (Theorem 3.1 below) provides a nontrivial extension of (1.3) for any m, even or odd.

The second part of this paper is devoted to stronger versions of Kummer's congruences which connect the Bernoulli polynomials to values of p-adic L-functions at negative integers. When the Riemann zeta function defined for $\Re(s) > 1$ by $\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ is meromorphically continued to the complex plane we have $\zeta(1-m) = -B_m/m$ for every positive integer m. The strong form

$$\Delta_c^k\left\{(1-p^{m-1})\frac{B_m}{m}\right\} \equiv 0 \pmod{p^{k(a+1)}\mathbb{Z}_p} \tag{1.6}$$

of the Kummer congruences [2],[3], where Δ_c is the forward difference operator with increment $c \equiv 0 \pmod{(p-1)p^a}$ and Δ_c^k is the k-th compositional iterate of this operator, was interpreted by Kubota and Leopoldt [14] to imply the existence of p-adic analytic analogues of Riemann ζ- and Dirichlet L-functions. The congruences (1.6) were recently generalized to the Bernoulli polynomials $B_m(x)$ with p-adic integer argument x by Eie and Ong [8]; then Fox [10] derived similar congruences for generalized Bernoulli polynomials from his construction of a two-variable p-adic L-function. In [21], [22] we extended the congruences of [8] and [10] by means of p-adic integral representations of those L-functions. Z.-W. Sun [18] recently gave n-adic congruences modulo powers of a general integer $n > 1$ which contain special cases of the congruences of Eie and Ong for odd n and of the Fox congruences for Dirichlet characters whose conductor is relatively prime to n. In section 4 we show how these hypotheses may be removed and the congruences significantly strengthened. We also give binomial coefficient operator versions of all these congruences.

2. Preliminaries

Throughout this paper n will denote an integer greater than 1 and p will denote a prime number. If a, b are nonzero integers then there exists a unique integer k such that $a/b = n^k(a'/b')$ with $(a', b') = (n, b') = 1$ and a' not divisible by n. The integer k is called the n-adic ordinal of the rational number a/b and denoted $k = \mathrm{ord}_n(a/b)$, and the n-adic absolute value of a/b is then defined by $|a/b|_n = n^{-k}$, with $|0|_n = 0$ by definition. The function $|\cdot|_n$ is a non-archimedean pseudo-valuation on $\mathbb{Z}$ or on $\mathbb{Q}$, and is a valuation on $\mathbb{Z}$ or on $\mathbb{Q}$ if n is prime. The completion of $\mathbb{Z}$ (resp. $\mathbb{Q}$) with respect to $|\cdot|_n$ is called the ring of n-adic integers (resp. n-adic numbers) and denoted $\mathbb{Z}_n$ (resp. $\mathbb{Q}_n$). For $x \in \mathbb{Q}_n$ we have $x \in \mathbb{Z}_n$ if and only if $\mathrm{ord}_n x \geq 0$. If A is a ring with identity, $A^\times$ will denote its multiplicative group of units.

Writing $n = p_1^{a_1} \cdots p_r^{a_r}$ as a product of powers of distinct primes $p_1, ..., p_r$, we define $s(n) = p_1 \cdots p_r$, the largest squarefree divisor of n. For any n we define the subring $\mathbb{Z}_{(n)} = \{a/b : a, b \in \mathbb{Z}, (b, n) = 1\}$ of $\mathbb{Q}$. We have $\mathbb{Z}_{(n)} = \mathbb{Z}_n \cap \mathbb{Q}$ for any n; furthermore $\mathbb{Z}_{(n)} = \mathbb{Z}_{(n')}$ if and only if $s(n) = s(n')$, and $\mathbb{Z}_n = \mathbb{Z}_{n'}$ if and only if $s(n) = s(n')$. All of the congruences in this paper will be stated in terms of either $\mathbb{Z}_{(n)}$ or its n-adic completion $\mathbb{Z}_n$. If A_n denotes either $\mathbb{Z}_{(n)}$ or $\mathbb{Z}_n$, then a congruence $x \equiv y \pmod{n^k A_n}$ is equivalent to $\mathrm{ord}_n(x - y) \geq k$. One advantage of the rings $\mathbb{Z}_{(n)}$ over $\mathbb{Z}_n$ is that they may be considered subrings of $\mathbb{Q}$ and we have for example $\mathbb{Z}_{(n)} = \bigcap_{p|n} \mathbb{Z}_{(p)}$. If n is not a prime power then $\mathbb{Z}_n$ has zero divisors and thus is not a subring of any field. An excellent reference for properties of n-adic numbers is [15].

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

$$\Delta_c a_m = a_{m+c} - a_m. \tag{2.1}$$

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

$$\Delta_c^k a_m = \sum_{j=0}^{k} \binom{k}{j} (-1)^{k-j} a_{m+jc} \tag{2.2}$$

for all nonnegative integers k. To define binomial coefficient operators $\binom{D}{k}$ associated to an operator D (cf. [12]), we write the binomial coefficient

$$\binom{X}{k} = \frac{X(X-1)\cdots(X-k+1)}{k!} \tag{2.3}$$

for $k \geq 0$ as a polynomial in X, and replace X by D; therefore

$$\binom{D}{k} = \frac{1}{k!} \sum_{j=0}^{k} s(k,j) D^j \tag{2.4}$$

for any operator D, where $s(j,k)$ denotes the Stirling number of the first kind. In this paper we shall always use the index m to denote the index on which an operator operates. The generalized falling factorial $(x|\lambda)_m$ with increment λ is defined by

$$(x|\lambda)_m = \prod_{i=0}^{m-1} (x - i\lambda) \tag{2.5}$$

for positive integers m, with the convention $(x|\lambda)_0 = 1$.

If p is a prime number we define the quantity q_p by

$$q_p = \begin{cases} p, & \text{if } p > 2, \\ 4, & \text{if } p = 2, \end{cases} \tag{2.6}$$

so that $\phi(q_p) = p - 1$ if p is odd and $\phi(q_p) = 2$ if $p = 2$, where ϕ denotes Euler's totient. The Möbius function $\mu(k)$ is defined for positive integers k by

$$\mu(k) = \begin{cases} 1, & \text{if } k = 1, \\ (-1)^r, & \text{if } k \text{ is the product of } r \text{ distinct primes}, \\ 0, & \text{if } k \text{ is divisible by the square of a prime.} \end{cases} \tag{2.7}$$

Let A_n denote either $\mathbb{Z}_{(n)}$ or $\mathbb{Z}_n$. For any divisor d of n we define a function $x \mapsto [x]_d$ on A_n by requiring that $[x]_d$ is the unique element of A_n satisfying $d[x]_d - x \in \{0, 1, 2, ..., d-1\}$. If n is a prime and $d = n$ then the map $x \mapsto [x]_n$ is Dwork's shift map (cf. [21]). The following lemma will be needed in section 4.

Lemma 2.1. *If cd divides n then $[[x]_c]_d = [x]_{cd}$.*

Proof. Define $r_d(x) = d[x]_d - x \in \{0, 1, ..., d-1\}$. Then

$$\begin{aligned} [[x]_c]_d &= \left[\frac{x + r_c(x)}{c}\right]_d \\ &= \frac{x + r_c(x) + c r_d\left(\frac{x + r_c(x)}{c}\right)}{cd}, \end{aligned} \tag{2.8}$$

so that

$$cd\,[[x]_c]_d - x = r_c(x) + c r_d\left(\frac{x + r_c(x)}{c}\right). \tag{2.9}$$

Since

$$r_c(x) + cr_d\left(\frac{x + r_c(x)}{c}\right) \in \{0, 1, ..., cd - 1\} \tag{2.10}$$

it follows from the uniqueness of $r_{cd}(x)$ that

$$r_c(x) + cr_d\left(\frac{x + r_c(x)}{c}\right) = r_{cd}(x) \tag{2.11}$$

and therefore $[[x]_c]_d = [x]_{cd}$.

3. Degenerate versions of Kummer congruences

For any element $h(T)$ of the formal power series ring $\mathbb{Z}_p[[T-1]]$ we defined [23] the *degenerate number sequence* $\alpha_m(\lambda)$ *arising from* h by the generating function

$$h((1+\lambda t)^\mu) = \sum_{m=0}^{\infty} \alpha_m(\lambda)\frac{t^m}{m!} \tag{3.1}$$

where $\lambda\mu = 1$. The $\alpha_m(\lambda)$ are actually polynomials in λ and may therefore be defined for $\lambda = 0$ as well, where they satisfy

$$h(e^t) = \sum_{m=0}^{\infty} \alpha_m(0)\frac{t^m}{m!}. \tag{3.2}$$

We showed ([23], Theorem 1.1) that for any such h there is a p-adic measure γ_h on $\mathbb{Z}_p$ such that

$$\alpha_m(\lambda) = \int_{\mathbb{Z}_p} (x|\lambda)_m \, d\gamma_h(x) \tag{3.3}$$

for all $\lambda \in \mathbb{Z}_p$ and all $m \geq 0$. From this integral representation we deduced ([23], Theorem 1.2) that $\alpha_m(\lambda) \in \mathbb{Z}_p$ for all λ and all m; that $\alpha_m(\lambda) \in m!\mathbb{Z}_p$ for all $\lambda \in \mathbb{Z}_p^\times$ and all m; and that if $\lambda \in p\mathbb{Z}_p$ and $m \equiv m' \pmod{\phi(q_p)p^a}$ with $a \geq 0$ then $\alpha_m(\lambda) \equiv \alpha_{m'}(\lambda) \pmod{p^A\mathbb{Z}_p}$ where $A = \min\{m, m', a+1\}$. We now use these results to deduce congruences for expressions involving the degenerate Bernoulli polynomials.

Theorem 3.1. *Let A_p denote either $\mathbb{Z}_{(p)}$ or $\mathbb{Z}_p$. If $c \in A_p^\times$ and $\lambda, x \in A_p$ then for all positive integers m we have*

$$\beta_m(c\lambda, x) - c^m\beta_m(\lambda, x) \in \begin{cases} mA_p, & \text{if } \lambda \in pA_p, \\ m!A_p, & \text{if } \lambda \in A_p^\times. \end{cases}$$

Furthermore if $c \in A_p^\times$, $\lambda \in pA_p$, and $m \equiv m' \pmod{\phi(q_p)p^a}$ then for $x \in A_p$ we have

$$\frac{\beta_{m+1}(c\lambda, x) - c^{m+1}\beta_{m+1}(\lambda, x)}{m+1} \equiv \frac{\beta_{m'+1}(c\lambda, x) - c^{m'+1}\beta_{m'+1}(\lambda, x)}{m'+1} \pmod{p^A A_p}$$

where $A = \min\{m, m', a+1\}$.

Proof. Let $A_p = \mathbb{Z}_p$ and let b be a positive integer with $(b,p) = 1$, and consider the formal power series

$$h(T) = \frac{bT^{bx}}{T^b - 1} - \frac{T^x}{T-1}. \tag{3.4}$$

In ([21], Theorem 3.2) we showed that $h(T) \in \mathbb{Z}_p[[T-1]]$ for any $x \in \mathbb{Z}_p$. If we then write $h((1+\lambda t)^\mu) = \sum_{m=0}^{\infty} \alpha_m(\lambda) t^m/m!$ then $\{\alpha_m(\lambda)\}_{m=0}^{\infty}$ is the degenerate number sequence arising from h. Comparison with (1.4) shows that

$$\alpha_m(\lambda) = b^{m+1} \frac{\beta_{m+1}(c\lambda, x) - c^{m+1}\beta_{m+1}(\lambda, x)}{m+1} \tag{3.5}$$

where $bc = 1$. By ([23], Theorem 1.1) we have $\alpha_m(\lambda) \in \mathbb{Z}_p$ for all m. By ([23], Theorem 1.2) we have $\alpha_m(\lambda) \in m!\mathbb{Z}_p$ when $\lambda \in \mathbb{Z}_p^\times$ and $\alpha_m(\lambda) \equiv \alpha_{m'}(\lambda) \pmod{p^A \mathbb{Z}_p}$ when $\lambda \in p\mathbb{Z}_p$ and $m \equiv m'$ $(\mathrm{mod}\ \phi(q_p)p^a)$. Since b^{m+1} is a p-adic unit and $b^{m+1} \equiv b^{m'+1} \pmod{p^{a+1}}$ when $m \equiv m'$ $(\mathrm{mod}\ \phi(q_p)p^a)$, the assertions of the theorem follow for $c = b^{-1}$ with $(b,p) = 1$. Since the set of positive integers b with $(b,p) = 1$ is dense in $\mathbb{Z}_p^\times$, the result follows for general $c \in \mathbb{Z}_p^\times$ by p-adic continuity. Since the β_m are polynomials in λ, x with rational coefficients and $\mathbb{Z}_{(n)} = \mathbb{Z}_n \cap \mathbb{Q}$ the theorem remains valid for $A_p = \mathbb{Z}_{(p)}$.

Remarks. When $\lambda = x = 0$ and $c = 2$ the expression $\beta_m(c\lambda, x) - c^m\beta_m(\lambda, x)$ in the theorem reduces to $(1-2^m)B_m = G_m/2$, where the integers G_m are the Genocchi numbers, which have several combinatorial interpretations in terms of certain surjective maps on finite sets (cf. [5], [6], [7]). The system of congruences of the theorem implies

$$\frac{G_{m+1}}{m+1} \equiv \frac{G_{m'+1}}{m'+1} \pmod{p^A A_p} \tag{3.6}$$

when p is odd and $m \equiv m'$ $(\mathrm{mod}\ (p-1)p^a)$, where $A = \min\{m, m', a+1\}$, and the theorem may be viewed as a generalization of this result on Genocchi numbers. (Stronger versions of (3.6) involving the Δ_c^k operator and binomial coefficient operators may be obtained by applying Theorems 1.1 and 1.2 of [20] to the power series $h(T)$ in (3.4); see ([20], eqs. (4.5), (4.7)) and also [11].) When $p-1$ does not divide $m+1$ one may choose a positive integer c such that $c^{m+1} \not\equiv 1 \pmod{p}$; then the congruences (1.3) are obtained by taking $\lambda = x = 0$ in the theorem, dividing by $1 - c^{m+1}$, and noting that $1 - c^{m+1} \equiv 1 - c^{m'+1} \pmod{p^{a+1}}$ when $m \equiv m'$ $(\mathrm{mod}\ (p-1)p^a)$.

When c is an integer greater than 1 and $x = 0$ the expression $\beta_m(c\lambda, x) - c^m\beta_m(\lambda, x)$ of the theorem also appears in Howard's recurrence formula

$$c\beta_m(c\lambda) - c^{m+1}\beta_m(\lambda) = \sum_{k=0}^{m-1} c^k \binom{m}{k} \beta_k(\lambda) \sum_{j=1}^{c-1} (j|c\lambda)_{m-k} \tag{3.7}$$

([13], Theorem 4.1) for the degenerate Bernoulli numbers $\beta_m(\lambda) = \beta(\lambda, 0)$. It follows from Theorem 3.1 that for integers $c > 1$ with $(c, p) = 1$ we have

$$\sum_{k=0}^{m-1} c^k \binom{m}{k} \beta_k(\lambda) \sum_{j=1}^{c-1} (j|c\lambda)_{m-k} \in \begin{cases} mA_p, & \text{if } \lambda \in pA_p, \\ m!A_p, & \text{if } \lambda \in A_p^\times \end{cases} \tag{3.8}$$

for any positive integer m.

Setting $\lambda = 1$ gives another application of the first congruence, since it may be seen from (1.4) that $\beta_m(1, x) = (x|1)_m$. In this case the first congruence reads

$$\beta_m(c, x) - c^m(x|1)_m \in m!A_p \tag{3.9}$$

for any $c \in A_p^\times$ and any $x \in A_p$. However $(x|1)_m = m!\binom{x}{m} \in m!A_p$ for any $x \in A_p$, so it follows that $\beta_m(c, x) \in m!A_p$ for any $c \in A_p^\times$ and any $x \in A_p$.

4. n-adic versions of Kummer congruences

In this section we give strong versions of Kummer's congruences for the Bernoulli polynomials modulo powers of a general integer $n > 1$. We define $\phi^*(n) = \text{l.c.m.}\{\phi(q_p), p^{a-1} : p^a|n, a > 0\}$ and observe that $\phi^*(2) = 2$; that $\phi^*(n) = \phi(n)$ if n is any prime power other than 2; and that $\phi^*(n)$ divides $\phi(n)$ for all $n > 2$.

Theorem 4.1. *Let $n > 1$ be an integer and let A_n denote either $\mathbb{Z}_{(n)}$ or $\mathbb{Z}_n$. Let m be a positive integer such that $\phi(q_p)$ does not divide m for any prime p dividing n, and let c be a positive integer divisible by $\phi^*(n)$. Then for all $x \in A_n$ and all $k > 0$ we have*

$$\Delta_c^k \left\{ \sum_{d|n} \frac{\mu(d)d^{m-1}B_m([x]_d)}{m} \right\} \equiv 0 \pmod{n^k A_n}$$

and

$$2\binom{\rho\Delta_c}{k} \left\{ \sum_{d|n} \frac{\mu(d)d^{m-1}B_m([x]_d)}{m} \right\} \in A_n$$

for all $\rho \in (2n)^{-1} A_n$.

Proof. First assume $A_n = \mathbb{Z}_{(n)}$ and let $\rho \in (2n)^{-1} A_n$. Write $n = p_1^{a_1} \cdots p_r^{a_r}$ as a product of powers of distinct primes $p_1, ..., p_r$; then $\mu(d)$ is nonzero only for the 2^r distinct squarefree divisors d of n. Let $S_1 = \{p_2^{e_2} \cdots p_r^{e_r} : e_i \in \{0,1\}\}$ be the set of all 2^{r-1} squarefree divisors of d not divisible by p_1. Then by Lemma 2.1

$$\begin{aligned}\sum_{d|n} \frac{\mu(d) d^{m-1} B_m([x]_d)}{m} &= \sum_{s \in S_1} \frac{\mu(s) s^{m-1} B_m([x]_s) + \mu(sp_1)(sp_1)^{m-1} B_m([x]_{sp_1})}{m} \\ &= \sum_{s \in S_1} \mu(s) s^{m-1} \frac{B_m([x]_s) - p_1^{m-1} B_m([[x]_s]_{p_1})}{m}.\end{aligned} \tag{4.1}$$

Since $[x]_s$ lies in the subring $\mathbb{Z}_{(n)}$ of $\mathbb{Z}_{p_1}$, $\phi(q_{p_1})$ does not divide m, and l.c.m. $\{\phi(q_{p_1}), p_1^{a_1 - 1}\}$ divides c we know from ([21], Theorem 3.2) that

$$\Delta_c^k \left\{ \frac{B_m([x]_s) - p_1^{m-1} B_m([[x]_s]_{p_1})}{m} \right\} \equiv 0 \pmod{p_1^{k a_1} \mathbb{Z}_{(p_1)}} \tag{4.2}$$

and

$$2 \binom{\rho \Delta_c}{k} \left\{ \frac{B_m([x]_s) - p_1^{m-1} B_m([[x]_s]_{p_1})}{m} \right\} \in \mathbb{Z}_{(p_1)} \tag{4.3}$$

for any $s \in S_1$ and any $\rho \in (2p_1^{a_1})^{-1} \mathbb{Z}_{(p_1)}$. (The result in [21] is stated only for ρ of the form $\rho = p_1^{-r} \in (2p_1^{a_1})^{-1} \mathbb{Z}_{(p_1)}$, but this restriction is not necessary; in the proof (cf. [20], eq. (2.17), (2.18)) the essential point is that $\rho(x^c - 1) \in \mathbb{Z}_p$ for all $x \in \mathbb{Z}_p^{\times}$). Since p_1 is an arbitrary prime factor of n, we have

$$\Delta_c^k \left\{ \sum_{d|n} \frac{\mu(d) d^{m-1} B_m([x]_d)}{m} \right\} \equiv 0 \pmod{p_i^{k a_i} \mathbb{Z}_{(p_i)}} \tag{4.4}$$

and for any $\rho \in (2n)^{-1} \mathbb{Z}_{(n)}$ we have

$$2 \binom{\rho \Delta_c}{k} \left\{ \sum_{d|n} \frac{\mu(d) d^{m-1} B_m([x]_d)}{m} \right\} \in \mathbb{Z}_{(p_i)} \tag{4.5}$$

for $i = 1, ..., r$. Therefore (4.4) holds modulo $n^k \mathbb{Z}_{(n)}$ and (4.5) lies in $\mathbb{Z}_{(n)}$, proving the theorem for $A_n = \mathbb{Z}_{(n)}$. Finally by n-adic continuity if $x \in \mathbb{Z}_n$ then (4.4) holds modulo $n^k \mathbb{Z}_n$ and if $\rho \in (2n)^{-1} \mathbb{Z}_n$ then (4.5) lies in $\mathbb{Z}_n$, proving the theorem for $A_n = \mathbb{Z}_n$.

Remark. Several special cases of these results have recently appeared. The second result was first obtained by Gunaratne [12] in the case $n = p$ and $x = 0$. Eie and Ong [8] then proved the first result in the case $n = p^a$ and $k = 1$ for primes $p \geq 5$. In [20] we gave a different proof of the second result for $n = p^a$ and $x = 0$, and Z.-H. Sun [17] then gave a different proof of the first result in the special case where $n = p$ and $c = p - 1$. At this time Fox [10] proved both results for $n = p^a$ in the case where $x \in pq_p\mathbb{Z}_p$, and in [21] we proved them for general $x \in \mathbb{Z}_p$ for $n = p^a$. Then Z.-W. Sun [18] gave a version of the first result which applies when n is any odd integer and $c = \phi(n)$. The above theorem removes the restrictions that n is odd and $c = \phi(n)$ from [18] and the restriction that $n = p^a$ from [21].

Let $\chi : (\mathbb{Z}/d\mathbb{Z})^\times \to R^\times$ be a multiplicative homomorphism, where R is a commutative ring with identity of characteristic zero. Then χ induces a homomorphism from $(\mathbb{Z}/c\mathbb{Z})^\times$ to $R^\times$ for any multiple c of d. If $\chi : (\mathbb{Z}/d\mathbb{Z})^\times \to R^\times$ cannot be induced by a homomorphism from $(\mathbb{Z}/c\mathbb{Z})^\times$ to $R^\times$ for any proper divisor c of d, then χ is called *primitive* and d is called the *conductor of* χ. If χ is primitive of conductor f we extend χ to a map from $\mathbb{Z}$ to $R^\times$ by defining $\chi(a) = 0$ if $(a, f) \neq 1$; then χ is called a *primitive Dirichlet character* of conductor f. Since the non-zero values of χ are roots of unity of order dividing $\phi(f)$, the ring $\mathbb{Z}_{(n)}(\zeta_d)$, where ζ_d is a d-th root of unity for some divisor d of $\phi(f)$, is a subring of $\mathbb{C}$ containing $\mathbb{Z}_{(n)}$ and the values of χ. The quotient ring $\mathbb{Z}_n[T]/(T^d - 1)$ for suitable d may likewise be viewed as a ring which contains $\mathbb{Z}_n$ and the values of χ. For any primitive Dirichlet character χ of conductor f we define the generalized Bernoulli polynomials $B_{m,\chi}(x)$ by

$$\left(\sum_{a=1}^{f} \frac{\chi(a) t e^{at}}{e^{ft} - 1} \right) e^{xt} = \sum_{m=0}^{\infty} B_{m,\chi}(x) \frac{t^m}{m!}. \tag{4.6}$$

The following theorem gives congruences for these polynomials modulo powers of a general integer $n > 1$.

Theorem 4.2. *Let $n > 1$ be an integer and let c be a positive integer divisible by $\phi^*(n)$. Let χ be a nontrivial primitive Dirichlet character of conductor f. Let A_n be either $\mathbb{Z}_{(n)}$ or $\mathbb{Z}_n$, and $A_n[\chi]$ a ring containing A_n and the values of χ. If f is not a power of a prime factor of n, then for all*

$x \in A_n$ and all $k > 0$ we have

$$\Delta_c^k \left\{ \sum_{d|n} \frac{\mu(d)\chi(d)d^{m-1}B_{m,\chi}\left(\frac{s(n)x}{d}\right)}{m} \right\} \equiv 0 \pmod{n^k A_n[\chi]}$$

and

$$\binom{\rho\Delta_c}{k} \left\{ \sum_{d|n} \frac{\mu(d)\chi(d)d^{m-1}B_{m,\chi}\left(\frac{s(n)x}{d}\right)}{m} \right\} \in A_n[\chi]$$

for all $\rho \in (2n)^{-1}A_n$, where $s(n)$ denotes the largest squarefree divisor of n. If $f = q_p p^e$ $(e \geq 0)$ is a power of a prime p which divides n, then for all $x \in p^e A_n$ and all $k > 0$ we have

$$\Delta_c^k \left\{ \sum_{d|n} \frac{\mu(d)\chi(d)d^{m-1}B_{m,\chi}\left(\frac{s(n)x}{d}\right)}{m} \right\} \equiv 0 \pmod{n^k A_n[\chi]}$$

and

$$p^{-1}q_p\binom{\rho\Delta_c}{k} \left\{ \sum_{d|n} \frac{\mu(d)\chi(d)d^{m-1}B_{m,\chi}\left(\frac{s(n)x}{d}\right)}{m} \right\} \in A_n[\chi]$$

for all $\rho \in (2n)^{-1}A_n$.

Proof. First assume $A_n = \mathbb{Z}_{(n)}$. Write $n = p_1^{a_1} \cdots p_r^{a_r}$ as a product of powers of distinct primes $p_1, ..., p_r$, and let $S_1 = \{p_2^{e_2} \cdots p_r^{e_r} : e_i \in \{0,1\}\}$. Then

$$\begin{aligned} &\sum_{d|n} \frac{\mu(d)\chi(d)d^{m-1}B_{m,\chi}\left(\frac{s(n)x}{d}\right)}{m} \\ &= \sum_{s\in S_1} \frac{\mu(s)\chi(s)s^{m-1}B_{m,\chi}\left(\frac{s(n)x}{s}\right) + \mu(sp_1)\chi(sp_1)(sp_1)^{m-1}B_{m,\chi}\left(\frac{s(n)x}{p_1 s}\right)}{m} \qquad (4.7) \\ &= \sum_{s\in S_1} \mu(s)\chi(s)s^{m-1}\frac{B_{m,\chi}\left(\frac{s(n)x}{s}\right) - \chi(p_1)p_1^{m-1}B_{m,\chi}\left(\frac{s(n)x}{p_1 s}\right)}{m}. \end{aligned}$$

Observe that $s(n)x/p_1 s \in \mathbb{Z}_{(p_1)}$ for all $x \in \mathbb{Z}_{(p_1)}$ and all $s \in S_1$, and that l.c.m. $\{\phi(q_{p_1}), p_1^{a_1-1}\}$ divides c. If f is not a power of p_1 then by ([21], Theorem 4.1) we have

$$\Delta_c^k \left\{ \frac{B_{m,\chi}\left(\frac{s(n)x}{s}\right) - \chi(p_1)p_1^{m-1}B_{m,\chi}\left(\frac{s(n)x}{p_1 s}\right)}{m} \right\} \equiv 0 \pmod{p_1^{ka_1}\mathbb{Z}_{(p_1)}[\chi]} \qquad (4.8)$$

and

$$\binom{\rho\Delta_c}{k}\left\{\frac{B_{m,\chi}\left(\frac{s(n)x}{s}\right)-\chi(p_1)p_1^{m-1}B_{m,\chi}\left(\frac{s(n)x}{p_1 s}\right)}{m}\right\}\in\mathbb{Z}_{(p_1)}[\chi] \tag{4.9}$$

for all $s\in S_1$ and all $\rho\in(2p_1^{a_1})^{-1}\mathbb{Z}_{(p_1)}$. (Again the restriction that $\rho=p^{-r}$ in ([21], Theorem 4.1) is not essential). Therefore if f is not a power of any p_i, $i=1,...,r$ then we have

$$\Delta_c^k\left\{\sum_{d|n}\frac{\mu(d)\chi(d)d^{m-1}B_{m,\chi}\left(\frac{s(n)x}{d}\right)}{m}\right\}\equiv 0 \pmod{p_i^{ka_i}\mathbb{Z}_{(p_i)}[\chi]} \tag{4.10}$$

and for all $\rho\in(2n)^{-1}\mathbb{Z}_{(n)}$ we have

$$\binom{\rho\Delta_c}{k}\left\{\sum_{d|n}\frac{\mu(d)\chi(d)d^{m-1}B_m\left(\frac{s(n)x}{d}\right)}{m}\right\}\in\mathbb{Z}_{(p_i)}[\chi] \tag{4.11}$$

for $i=1,...,r$, and therefore the first statement of the theorem follows for $A_n=\mathbb{Z}_{(n)}$.

If $f=q_p p^e$ is a power of $p=p_1$ then for $s\in S_1$, $x\in p^e\mathbb{Z}_{(p)}$ and $\rho\in(2p_1^{a_1})^{-1}\mathbb{Z}_{(p)}$ the congruences

$$\Delta_c^k\left\{\frac{B_{m,\chi}\left(\frac{s(n)x}{s}\right)-\chi(p_1)p_1^{m-1}B_{m,\chi}\left(\frac{s(n)x}{p_1 s}\right)}{m}\right\}\equiv 0 \pmod{p_1^{ka_1}\mathbb{Z}_{(p_1)}[\chi]} \tag{4.12}$$

and

$$p^{-1}q_p\binom{\rho\Delta_c}{k}\left\{\frac{B_{m,\chi}\left(\frac{s(n)x}{s}\right)-\chi(p_1)p_1^{m-1}B_{m,\chi}\left(\frac{s(n)x}{p_1 s}\right)}{m}\right\}\in\mathbb{Z}_{(p_1)}[\chi] \tag{4.13}$$

follow from ([22], Corollary 3.2) except in the case where $p=2$, $e=0$, and $x\in\mathbb{Z}_{(2)}^{\times}$, when they follow from ([22], Corollary 5.2). Since (4.12), (4.13) hold for $p=p_1$ and (4.10), (4.11) hold for all other primes p_i where $p_i^{a_i}$ divides n, the second statement of the theorem then follows for $A_n=\mathbb{Z}_{(n)}$. By continuity the statements of the theorem hold for $A_n=\mathbb{Z}_n$ as well, completing the proof.

Remark. In the case $n=p^a$ and $x=0$ the Δ_c^k form of the above result was proved by Carlitz [3], Shiratani [16], and Ernvall [9]. The binomial coefficient operator form of this result was obtained by Gunaratne [12] in the case $x=0$ and $f=q_p$ and in [20], [21] we proved both results in the case where $n = p^a$ and f is not a power of p. Fox [10] gave the first proof of these results for general χ in the case $n = p^a$ under the assumption that $x \in F_0\mathbb{Z}_p$, where $F_0 = \text{l.c.m.}\{f, q_p\}$. In [22] we relaxed this restriction on x, and in [18] Z.-W. Sun proved the Δ_c^k form of this result for general $n > 1$ in the special case where $(f, n) = 1$ and $c = \phi(n)$. The above theorem removes the restrictions that $(f, n) = 1$ and $c = \phi(n)$ from [18] and the restriction that $n = p^a$ from [22]. In the congruences of Gunaratne [12], Fox [10], and the author [22] for $n = p^a$ the condition that $\phi^*(n)$ divides c may be waived by "twisting" the character χ by powers of the Teichmüller character; however if n is not a prime power there seems to be no natural way of doing this.

References

[1] A. Adelberg, A finite difference approach to degenerate Bernoulli and Stirling polynomials, Discrete Math. 140 (1995), 1-21.

[2] L. Carlitz, Some congruences for the Bernoulli numbers, Amer. J. Math. 75 (1953), 163-172.

[3] L. Carlitz, Arithmetic properties of generalized Bernoulli numbers, J. Reine Angew. Math. 202 (1959), 174-182.

[4] L. Carlitz, Degenerate Stirling, Bernoulli, and Eulerian numbers, Utilitas Math. 15 (1979), 51-88.

[5] D. Dumont, Interprétations combinatoires des nombres de Genocchi, Duke Math. J. 41 (1974), 305-318.

[6] D. Dumont and G. Viennot, A combinatorial interpretation of the Seidel generation of Genocchi numbers, Ann. Discrete Math. 6 (1980), 77-87.

[7] D. Dumont and A. Randrianarivony, Dérangements et nombres de Genocchi, Discrete Math. 132 (1994), 37-49.

[8] M. Eie and Y. L. Ong, A generalization of Kummer's congruence, Abh. Math. Sem. Univ. Hamburg 67 (1997), 149-157.

[9] R. Ernvall, Generalized Bernoulli numbers, generalized irregular primes, and class number, Ann. Univ. Turku. Ser. A I 178 (1979), 72 pp.

[10] G. Fox, A p-adic L-function of two variables, L'Enseign. Math. 46 (2000), 225-278.

[11] J. M. Gandhi, Congruences for Genocchi numbers, Duke Math. J. 31 (1964), 519-527.

[12] 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.

[13] F. T. Howard, Explicit formulas for degenerate Bernoulli numbers, Discrete Math. 162 (1996), 175-185.

[14] T. Kubota and H. W. Leopoldt, Eine p-adische Theorie der Zetawerte I, J. Reine Angew. Math. 214/215 (1964), 328-339.

[15] K. Mahler, Introduction to p-adic numbers and their functions, Cambridge University Press, Cambridge, 1973.

[16] K. Shiratani, Kummer's congruence for generalized Bernoulli numbers and its application, Mem. Fac. Sci. Kyushu Univ. Ser. A 26 (1971), 119-138.

[17] Z.-H. Sun, Congruences concerning Bernoulli numbers and Bernoulli polynomials, Discrete Appl. Math. 105 (2000), 193-223.

[18] Z.-W. Sun, General congruences for Bernoulli polynomials, Discrete Math. 262 (2003), 253-276.

[19] L. Washington, Introduction to Cyclotomic Fields, Springer-Verlag, New York, 1982.

[20] P. T. Young, Congruences for Bernoulli, Euler, and Stirling numbers, J. Number Theory 78 (1999), 204-227.

[21] P. T. Young, Kummer congruences for values of Bernoulli and Euler polynomials, Acta Arith. 99 (2001), 277-288.

[22] P. T. Young, On the behavior of some two-variable p-adic L-functions, J. Number Theory 98 (2003), 67-88.

[23] P. T. Young, Congruences for degenerate number sequences, Discrete Math. 270 (2003), 279-289.