Journal of Number Theory **84**, 119–135 (2000)
doi:10.1006/jnth.2000.2526, available online at http://www.idealibrary.com on IDEAL®

Universal Higher Order Bernoulli Numbers and Kummer and Related Congruences

Arnold Adelberg

Department of Mathematics, Grinnell College, Grinnell, Iowa 50112
E-mail: adelbe@math.grin.edu

Communicated by A. Hildebrand

Received August 23, 1999

We define higher or arbitrary order universal Bernoulli numbers and higher order universal Bernoulli–Hurwitz numbers. We deduce a universal first-order Kummer congruence and a congruence for the higher order universal Bernoulli–Hurwitz numbers from Clarke's universal von Staudt theorem. We also establish other Kummer-type congruences for the higher order universal Bernoulli numbers and for the universal Nörlund polynomials, generalizing the author's previous work.

Key Words: universal Bernoulli numbers; Kummer congruences; universal higher order Bernoulli numbers; Nörlund polynomials.

1. INTRODUCTION

Let the power series $F(t)$ over the polynomial ring $\mathbf{Q}[c_1, c_2, \ldots]$ be defined by

$$F(t) = \sum_{i=0}^{\infty} c_i \frac{t^{i+1}}{i+1}$$

where $c_0 = 1$.

Let $G(t) = F^{-1}(t)$ be the compositional inverse, so

$$G(t) = \sum_{i=0}^{\infty} d_i \frac{t^{i+1}}{i+1}$$

where $d_0 = 1$, $d_1 = -c_1$, $d_2 = \frac{3}{2}c_1^2 - c_2, \ldots$. Observe that $d_1, d_2, \ldots$ are also indeterminates over $\mathbf{Q}$.

Clarke [9] defined the *universal Bernoulli numbers* $\hat{B}_n$ in $\mathbf{Q}[c_1, c_2, \ldots]$ by $\hat{B}_n/n! = [t^n]\, t/G(t)$, i.e.,

$$\frac{t}{G(t)} = \sum_{n=0}^{\infty} \hat{B}_n \frac{t^n}{n!}.$$

0022-314X/00 $35.00

We generalize to define *arbitrary* or *higher order* universal Bernoulli numbers $\hat{B}_n^{(l)}$ by

$$\left(\frac{t}{G(t)}\right)^l = \sum_{n=0}^{\infty} \hat{B}_n^{(l)} \frac{t^n}{n!}.$$

If $l=1$ we get $\hat{B}_n$, which we call *ordinary* or *first-order*. In most of our applications the order l of $\hat{B}_n^{(l)}$ is a rational integer, usually in the range of 1 to n for higher order; a p-adic integer; or a variable x, in which case $\hat{B}_n^{(x)}$ is called a *universal Nörlund polynomial*.

The specialization $c_i=(-1)^i$ gives $F(t)=\log(1+t)$ and $G(t)=e^t-1$. This yields the classical higher order Bernoulli numbers $B_n^{(l)}$ and Nörlund polynomials $B_n^{(x)}$. Other specializations have been studied in the ordinary case [9, 10].

Ray defined higher order universal Bernoulli numbers in the context of coalgebras and Hopf algebras. He used this machinery to show that the universal Bernoulli numbers play a privileged role in the theory [18, Proposition 10.1]. Much of the impetus for this study has come from algebraic topology, since the universal Bernoulli numbers are relevant to universal formal groups and to the homotopy of certain classifying spaces.

We believe that simple, direct definitions of arbitrary order Bernoulli numbers are useful. The explicit formulas that come out of Lagrange inversion [Corollary 2.3] are invaluable in studying the arithmetic of these numbers. The arbitrary order context seems appropriate since the Lagrange inversion works the same way for arbitrary order as for first order. Indeed, the Lagrange inversion formulas express duality relations between order l and order $n-l$ universal Bernoulli numbers, as well as between order l and order $n-l+1$ [Proposition 2.1]. Finally, the explicit general order formulas appear more natural in some ways than the special first order formula [9, Proposition 4] given by Clarke.

The first part of this paper relies heavily on Clarke's universal von Staudt theorem [9, Theorem 5]. We deduce a universal first-order Kummer congruence that fully generalizes the basic classical Kummer result that if n is even and $p-1 \nmid n$ then (cf. [7, 13])

$$\frac{B_{n+p-1}}{n+p-1} \equiv \frac{B_n}{n} \pmod{p}.$$

The following theorem is proved in Section 3.

THEOREM 3.2. *Suppose that* $n \not\equiv 0, 1 \pmod{p-1}$. *Then*

$$\frac{\hat{B}_{n+p-1}}{n+p-1} \equiv \frac{\hat{B}_n}{n} c_{p-1} \pmod{p\mathbf{Z}_p[c_1, c_2, \ldots]}.$$

Note that $n \not\equiv 0, 1 \pmod{p-1}$ implies that $p \geqslant 5$. The hypotheses of our theorem are satisfied if n is even and $p-1 \nmid n$, since n and $n \bmod p-1$ have the same parity for $p \neq 2$. Our theorem also includes nontrivial congruences for n odd. It is easy to see that the hypotheses are necessary for the conclusion of our theorem.

Clarke defined [9] *universal Bernoulli–Hurwitz* numbers $\widehat{BH}_n$, following the terminology of Katz [14], essentially by an ad hoc definition as

$$\widehat{BH}_n = \hat{B}_n^{(2)}/(n-1) \qquad \text{for} \quad n \geqslant 2.$$

Clarke then proved [9, Theorem 12] the congruence

$$\frac{\widehat{BH}_n}{n} \equiv -\frac{\hat{B}_n}{n} + c_1 \frac{\hat{B}_{n-1}}{n-1} \qquad \bmod \mathbf{Z}[c_1, c_2, \ldots].$$

This theorem generalizes a result of Carlitz [6, Theorem 3]. Clarke's proof, which uses only the generating function definition, is just a slight modification of the one given by Carlitz.

We define *higher order universal Bernoulli–Hurwitz* numbers $\widehat{BH}_n^{(l)}$ by

$$\widehat{BH}_n^{(l)} = \frac{\hat{B}_n^{(l+1)}}{n-l} \qquad \text{for} \quad l = 0, 1, 2, \ldots, n-1.$$

Clarke's theorem is the special case for $l = 1$ of the following general result, which is deduced from Clarke's universal von Staudt theorem.

THEOREM 3.4.

$$\frac{\widehat{BH}_n^{(l)}}{(n)_l} \equiv -\sum_{i=0}^{l-1} c_i \frac{\hat{B}_{n-i}^{(l-i)}}{(l-i)(n-i)_{l-i}} + c_l \frac{\hat{B}_{n-l}}{n-l} \qquad \bmod (c_l, c_{l+1}, \ldots)\, \mathbf{Z}[c_1, c_2, \ldots].$$

The proofs of these theorems in Section 3 follow from the universal von Staudt theorem. On the other hand, Section 4 does not depend on the first-order theory. Since our approach to the classical higher order theory relies on the same Lagrange inversion that is the cornerstone of the universal theory, it is not surprising that many of our results [2, 3] carry over. In most cases, only minor modifications are required in the statements and proofs. The primary exception is where the proofs involve the higher order Bernoulli polynomials $B_n^{(l)}(x)$, since the universal analogues do not have similar symmetry properties. As an example, if $v = v_p$ is the p-adic

exponential valuation and $[x]$ is the greatest integer function, we proved in [1, Theorem 3.3] that if l is a (p-adic) integer then

$$v(B_n^{(l)}/n!) \geqslant -\left[\frac{n}{p-1}\right].$$

That proof used the Bernoulli polynomials and cannot be adapted, but we gave an alternate proof [2, Lemma 2], which shows immediately that if v is extended to polynomials as the minimum valuation of the coefficients, then we have

THEOREM 4.2. $v(\hat{B}_n^{(l)}/n!) \geqslant -[\frac{n}{p-1}]$.

We have included a list of our congruences that carry over to the universal context with some discussion. Proofs are given to the extent that they differ substantially from our classical proofs. Included in the list is the strong mod mp version of a congruence for universal Nörlund polynomials [Theorem 4.10] that was noted but not proved in [3] for the classical Nörlund polynomials. The congruences and denominator estimates are all best possible, i.e., the congruences don't hold modulo higher powers of p and the bounds for the denominators are achieved.

2. PRELIMINARIES

Notations. p is always a (rational) prime and $\mathbf{Z}_p$ is the ring of p-adic integers. We denote the exponential valuation by $v = v_p$, so $e = v(n)$ means $p^e \parallel n$, and $v(n/m) = v(n) - v(m)$.

We extend v to multivariable polynomials by $v(f(\mathbf{x})) = \min\{v(c_I)\}$ over all coefficients c_I of $f(\mathbf{x})$. Divisibility and congruence are understood p-adically, e.g., $f(\mathbf{x}) \equiv g(\mathbf{x}) \pmod{n}$ if $n \mid f(\mathbf{x}) - g(\mathbf{x})$ in $\mathbf{Z}_p[\mathbf{x}]$, i.e., if $v(f(\mathbf{x}) - g(\mathbf{x})) \geqslant v(n)$.

We make heavy use of the following fundamental facts about factorials and binomial coefficients (cf. [16, Chap. 4]).

If $n = kp + \alpha$ where $0 \leqslant \alpha < p$, then

$$v(n!) = v((kp)!) = v(k!) + k. \tag{1}$$

If $n = kp + \alpha$ where $\alpha \geqslant 0$, then

$$n! \equiv (-1)^k \alpha!\, k!\, p^k \pmod{p^{v(n!)+1}}. \tag{2}$$

If $S(n)$ is the base p digit sum, then

$$v(n!) = \frac{n - S(n)}{p-1}. \tag{3}$$

Since the binomial coefficient

$$\binom{n}{m} = \frac{(n)_m}{m!} = \frac{n!}{m!\,(n-m)!} \in \mathbf{Z},$$

$$v(n!) \geqslant v(m!) + v((n-m)!). \tag{4}$$

$$p \nmid \binom{n}{m} \quad \text{if and only if} \quad S(n) = S(m) + S(n-m). \tag{5}$$

Lagrange inversion gives the following fundamental proposition, where $[t^n]$ denotes the coefficient of t^n in the indicated formal power series.

PROPOSITION 2.1. *Let $F(t)$ be a power series with zero constant term and first degree coefficient one, and let $G(t) = F^{-1}(t)$. Then*

(i) $$[t^n]\left(\frac{t}{G(t)}\right)^l = \frac{l}{l-n}[t^n]\left(\frac{F(t)}{t}\right)^{l-n}.$$

(ii) $$[t^n]\left(\frac{t}{G(t)}\right)^l = [t^n]\left(\frac{F(t)}{t}\right)^{l-n-1} F'(t).$$

Proof. Part (i) follows immediately from [11, Theorem 1.2.4], using essentially the same proof as for [9, Proposition 4], which is the special case $l = 1$.

For part (ii), differentiate the series on the right in (i). ∎

Remark 2.2. (a) The case $l = n$ is not a major problem in (i), since we can first use polynomial division to divide by $l-n$ and then take $l = n$. Specifically,

$$[t^n]\left(\frac{t}{G(t)}\right)^n = n[t^n]\log\left(\frac{F(t)}{t}\right) \qquad \text{if} \quad n > 0. \tag{6}$$

(b) If $F(t)$ is as in the Introduction, then Proposition 2.1(i) expresses a kind of duality between order l and order $n-l$ universal Bernoulli numbers. Similarly, Proposition 2.1(ii) is a duality between order l and order $n-l+1$ universal numbers. In particular, order 0 and order $n+1$ are both trivial, and order 1 (ordinary) and order n (Nörlund numbers) are

dual. The range $1 \leqslant l \leqslant n$ is stable for this duality, which appears to be the more significant of the two dualities.

Henceforth consider the case of the Introduction when

$$F(t) = \sum_{i=0}^{\infty} c_i t^{i+1}/(i+1) \qquad \text{and} \qquad F'(t) = \sum_{i=0}^{\infty} c_i t^i. \tag{7}$$

Let $(u) = (u_1, u_2, \ldots)$ be a finite sequence of nonnegative integers, $w = w(u) = \sum i u_i$ the *weight* of (u), and $d = d(u) = \sum u_i$ the *degree* of (u). Observe that (u) is a partition of w into d parts, where u_i is the number of occurrences of i.

Let

$$u! = u_1!\, u_2! \ldots, \qquad \binom{d}{u} = \frac{d!}{u!} \tag{8}$$

the multinomial coefficient, $\Lambda^u = 2^{u_1} 3^{u_2} \cdots$, $c^u = c_1^{u_1} c_2^{u_2} \cdots$, and $t_u(s) = \binom{s}{d}\binom{d}{u}/\Lambda^u = (s)_d/(u!\, \Lambda^u)$.

COROLLARY 2.3.

(i) $$\frac{\hat{B}_n^{(l)}}{n!} = \frac{l}{l-n} \sum_{w=n} t_u(l-n)\, c^u.$$

(ii) $$\frac{\hat{B}_n^{(l)}}{n!} = \sum_{w \leqslant n} t_u(l-n-1)\, c^u c_{n-w}.$$

Proof. Part (i) follows from Proposition 2.1(i) by the binomial and multinomial expansions, namely, let $H = (F(t)/t) - 1$. Then $(F(t)/t)^s = (1+H)^s = \sum \binom{s}{d} H^d$, and $H^d = \sum_{d(u)=d} \binom{d}{u} (c^u/\Lambda^u)\, t^{w(u)}$.

Part (ii) follows similarly from Proposition 2.1(ii). ∎

See [2, (10), (14)] for the classical versions of these formulas. Note that the number of terms in (i) is the partition function $p(n)$. The monomials c^u flag the partitions.

Remark 2.4. Corollary 2.3(i) can be explicitly rewritten as

$$\hat{B}_n^{(l)}/n! = l \sum_{w=n} \binom{l-n-1}{d-1}\binom{d}{u} c^u \Big/ d\Lambda^u.$$

The following corollary is the special case $l=1$ of the previous one.

COROLLARY 2.5. (i) $\hat{B}_n = n\sum_{w=n}(-1)^{d-1}(n+d-2)!\,c^u/(u!\,\Lambda^u)$.
(ii) $\hat{B}_n = n\sum_{w\leqslant n}(-1)^d(n+d-1)!\,c^u c_{n-w}/(u!\,\Lambda^u)$.

Remark 2.6. Corollary 2.5(i) is the same as [9, Proposition 4]. Clarke doesn't use (ii), which has more terms than (i), so monomials in $c_1, c_2, \ldots$ occur multiple times. However, (ii) is particularly useful for certain inductions, and the terms have somewhat better integrality properties.

PROPOSITION 2.7. *If* $w(u)=n$ *and* $d(u)=d$ *then* $(n+d)(n+d-2)!/u!\,\Lambda^u \in \mathbf{Z}$.

Proof. This is what we need from Clarke's universal von Staudt theorem [9, Theorem 5]:

$$\text{If } p-1 \nmid n \qquad \text{then} \quad \frac{(n+d-2)!}{u!\,\Lambda^u} \in \mathbf{Z}_p. \tag{9}$$

$$\text{If } p-1 \mid n \quad \text{and } p \text{ is odd then} \quad \frac{(n+d-2)!}{u!\,\Lambda^u} \in \mathbf{Z}_p, \tag{10}$$

except if $u_{p-1}=d=n/(p-1)$, in which case $n+d=dp$ and $(n+d)(n+d-2)!/u!\,\Lambda^u$ is a p-adic unit.

$$\text{If } p=2, \text{ the term where } u_1=d=n \text{ is handled as above.} \tag{11}$$

In addition, if $p=2$ there are other nonintegral terms with $v=-1$, if $n\equiv 2 \pmod 4$ or n is odd, but in both cases $n+d$ is even, so the result follows. ∎

3. CONSEQUENCES OF THE VON STAUDT THEOREM

Throughout this section $w=w(u)\leqslant n$ and $d=d(u)$. Also,

$$m=\left\lfloor \frac{n}{p-1} \right\rfloor,\ \sigma=n-m(p-1),\ \gamma_u=\frac{1}{u!\,\Lambda^u},\ \text{and } \tau_u=(n+d-1)!\,\gamma_u. \tag{12}$$

LEMMA 3.1. *Suppose that* $\sigma>1$. *If* $w(u)\leqslant n$ *then*

(i) $\tau_u \in \mathbf{Z}_p$, *and*
(ii) $\tau_u \in p\mathbf{Z}_p$ *if* $u_{p-1}\neq m$.

Proof. We will prove that if $w(u) \leqslant n$ then $v(\tau_u) \geqslant 0$, and $v(\tau_u) > 0$ if $u_{p-1} \neq m$. To prove (i), write $n+d-1 = n-w+1+d+w-2$. Then since $(d+w-2)!\ \gamma_u \in \mathbf{Z}_p$ by (9) and (10) unless $u_{p-1} = d$, it suffices to assume that $w = (p-1)\,d$. But then since $\sigma \neq 0$, we have $n-w+1 \geqslant 2$, so $n+d-1 \geqslant d+w$, whence $v(\tau_u) \geqslant 0$ by Proposition 2.7.

To prove (ii), first observe that if $w \leqslant n-(p-1)$ then $v(\tau_u) > 0$, namely $n-w+1 \geqslant p$, so this is obvious if $p-1 \nmid w$, in which case $(d+w-2)!\ \gamma_u \in \mathbf{Z}_p$. If, on the other hand, $p-1 \mid w$ and $w = (p-1)\,d$, then $n-w+1 \geqslant p+2$ since $\sigma > 1$. Again $v(\tau_u) > 0$ by Proposition 2.7.

Next we have to dispose of a couple of cases.

Case 1. $u_i \geqslant p$ for some $1 < i < p-1$ or $u_i > 0$ for some $i > p-1$, where $p \nmid i+1$.

In this case, let $u'_1 = u_1 + u_i$, $u'_i = 0$, and $u'_j = u_j$ for $j \neq 1, i$. Clearly, $w - w' \geqslant p-1$, $d = d'$, and $v(u'!) \geqslant v(u!)$. It follows that $v(\tau_u) \geqslant v(\tau_{u'}) > 0$.

Case 2. $u_i > 0$ for some $i > p-1$, where $p \mid i+1$.

In this case, let $u'_{p-1} = u_{p-1} + u_i$, $u'_i = 0$, and $u'_j = u_j$ for $j \neq p-1, i$. Let $\alpha = v(i+1)$. If $\alpha = 1$, the argument is the same as in Case 1, namely $w - w' \geqslant p$ and $d = d'$, so $v(\tau_u) \geqslant v(\tau_{u'}) > 0$. However, the argument is more subtle if $\alpha > 1$. Now $w - w' \geqslant u_i(p^\alpha - p) \geqslant u_i(\alpha+1)\,p$, since $\alpha \geqslant 2$ and $p \geqslant 5$. It follows that $v((n+d-1)!) = v((n-w'-1+w'+d)!) \geqslant u_i\alpha + v((w'+d)!)$.

On the other hand, $v(\Lambda^{u'}) = v(\Lambda^u) - (\alpha-1)\,u_i$, so $v(\gamma_{u'}) - v(\gamma_u) \geqslant -(\alpha-1)\,u_i$. Since $(w'+d')!\ \gamma_{u'} \in \mathbf{Z}_p$, we have $v(\tau_u) \geqslant u_i\alpha - u_i(\alpha-1) + v((w'+d)!\ \gamma_{u'}) > 0$.

Hence if $v(\tau_u) = 0$ then $v(\tau_u) = v((n+d-1)!) - v(u_1!\ u_{p-1}!\ p^{u_{p-1}})$. Let $u_{p-1} = m-k$ and $l = [u_1/p]$. We will show that $k = 0$. Suppose $k > 0$. Then $v(u!\ \Lambda^u) = v((lp)!) + v(((m-k)\,p)!) \leqslant v(((m-k+l)\,p)!)$. On the other hand, $d \geqslant m-k+lp$, so $n+d-1 \geqslant mp+\sigma-k+lp-1$. Since $\sigma \geqslant 2$ and $k \geqslant 1$, it follows that $n+d-1 \geqslant (m+l-(k-1))\,p$. Hence $v(\tau_u) > 0$ if $u_{p-1} = m-k$ with $k \neq 0$. ∎

THEOREM 3.2 (Universal Kummer Congruence). *Suppose* $n \not\equiv 0, 1 \pmod{p-1}$. *Then*

$$\frac{\hat{B}_{n+p-1}}{n+p-1} \equiv \frac{\hat{B}_n}{n}\, c_{p-1} \qquad (\mathrm{mod}\ p).$$

Proof. Let $S = \{(u) \mid w \leqslant n \text{ and } u_{p-1} = m\}$, and let $S' = \{(u') \mid w' = w(u') \leqslant \sigma\}$. If $(u) \in S$, let $u'_{p-1} = 0$ and $u'_j = u_j$ for $j \neq p-1$. Then $(u) \mapsto (u')$ gives a one–one correspondence between S and S', with $w' = w - m(p-1)$, $d' = d - m$, and $n - w = \sigma - w'$.

If $(u) \in S$ then $n+d-1 = mp+\sigma+d-1$, so by (2)

$$(n+d-1)!\,\gamma_u \equiv (-1)^m (\sigma+d'-1)!\,\gamma_{u'} \pmod{p}.$$

Thus by the preceding lemma and Corollary 2.5(ii),

$$\frac{\hat{B}_n}{n} \equiv \sum_{u \in S} (-1)^d \tau_u c^u c_{n-w} \pmod{p}$$

$$\equiv \sum_{w \leqslant \sigma} (-1)^d \tau_u c^u c_{\sigma-w} c_{p-1}^m \pmod{p}.$$

Therefore

$$\frac{\hat{B}_n}{n} \equiv \frac{\hat{B}_\sigma}{\sigma} c_{p-1}^m \pmod{p}, \tag{13}$$

which is clearly equivalent to the theorem. ▮

Remark 3.3. The preceding congruence is nontrivial for odd n. However, the assumption $\sigma > 1$ is essential since it follows easily from Corollary 2.5(i) that if $p > 2$ then

$$\hat{B}_p/p \equiv -c_p + (c_1 c_{p-1} + c_1^p)/2 \pmod{p}.$$

Hence the conclusion of the preceding theorem does not hold for $n = p$, in which case $m = \sigma = 1$.

Recall that

$$\widehat{BH}_n^{(l)} = \frac{\hat{B}_n^{(l+1)}}{n-l} \quad \text{if} \quad l = 0, 1, ..., n-1. \tag{14}$$

In particular,

$$\widehat{BH}_n^{(0)} = \hat{B}_n/n \quad \text{if } n > 0, \quad \text{and} \quad \widehat{BH}_n^{(1)} = \widehat{BH}_n = \hat{B}_n^{(2)}/(n-1) \quad \text{if } n > 1. \tag{15}$$

THEOREM 3.4 (Generalized Bernoulli–Hurwitz Congruence).

$$\frac{\widehat{BH}_n^{(l)}}{(n)_l} \equiv -\sum_{i=0}^{l-1} c_i \frac{\hat{B}_{n-i}^{(l-i)}}{(l-i)(n-i)_{l-i}} + c_l \frac{\hat{B}_{n-l}}{n-l}$$

$$\bmod (c_l, c_{l+1}, ...)\, \mathbf{Z}[c_1, c_2, ...].$$

Proof. From Corollary 2.3, with $\gamma_u = 1/(u!\, \Lambda^u)$,

$$\widehat{BH}_n^{(l)}/(n)_l = \hat{B}_n^{(l+1)}/(n)_{l+1}$$

$$= (l+1) \sum_{w=n} (-1)^{d-1} (n-l+d-2)!\, \gamma_u c^u \tag{16}$$

$$= \sum_{i \leqslant n} c_i \sum_{w=n-i} (-1)^d (n+d-l-1)!\, \gamma_u c^u. \tag{17}$$

If $i > l$, then $(n+d-l-1)!\, \gamma_u = (i-l+1+w+d-2)!\, \gamma_u$ which is in $\mathbf{Z}$ by Proposition 2.7. If $i = l$, then $(n+d-l-1)!\, \gamma_u = (w+d-1)!\, \gamma_u \equiv -(w+d-2)!\, \gamma_u \bmod \mathbf{Z}$, since $(w+d)(w+d-2)!\, \gamma_u \in \mathbf{Z}$ by Proposition 2.7.

Finally, if $i < l$, then from (16) we get

$$\sum_{w=n-i} (-1)^d (-(l-i-1)+(w+d-2))!\, \gamma_u c^u = -\frac{1}{l-i} \frac{\hat{B}_{n-i}^{(l-i)}}{(n-i)_{l-i}}.$$

The result now follows immediately from (17). ∎

4. HIGHER ORDER THEOREMS

Some of the classical p-adic divisibility results hold for universal higher order Bernoulli numbers, and some of the classical congruences have obvious extensions, but some do not. For example, if $1 \leqslant \sigma < p-1$ and l is a p-adic integer, then Remark 2.4 implies that $l \mid \hat{B}_\sigma^{(l)}$ and similarly that

$$p\hat{B}_{p-1}^{(l)} \equiv -lc_{p-1} \qquad (\bmod\ pl).$$

(Recall our convention stated at the beginning of Section 2 that divisibility and congruences are understood p-adically in the context of an implied domain.) On the other hand, it follows from [2, Corollary 6] that $l^2 \mid B_p^{(l)}$ in the classical case if p is odd, whereas the following proposition shows that if $p \mid l$ then $pl \nmid \hat{B}_p^{(l)}$ for the universal Bernoulli numbers.

PROPOSITION 4.1. *Suppose p is an odd prime and l is a p-adic integer. Then*

(i) $l \mid \hat{B}_p^{(l)}$ *and*

(ii) *if* $p \mid l$ *then* $\hat{B}_p^{(l)} \equiv l(c_1 c_{p-1} - c_1^p)/2 \ (\bmod\ pl)$.

Proof. By Remark 2.4,

$$\hat{B}_p^{(l)} \equiv lp! \sum_{w=p} \binom{l-p-1}{d-1}\binom{d}{u} c^u \Big/ d\Lambda^u.$$

Clearly, $v(d\Lambda^u)=0$ except for the two terms where $u_1=p$ and where $u_1=u_{p-1}=1$, and for these terms $v(d\Lambda^u)=1$. Thus (i) follows, while if $p \mid l$,

$$\hat{B}_p^{(l)} \equiv lp! \left(\binom{l-p-1}{p-1} c_1^p \Big/ p2^p + (l-p-1)\, c_1 c_{p-1}/(2p) \right) \pmod{pl}.$$

Part (ii) follows immediately by Wilson's theorem and Fermat's Little Theorem. ∎

The following theorems are adaptations of classical results which we have proved in [2, 3]. We will concentrate on the necessary modifications. Again assume throughout this section that

$$m=[n/(p-1)],\ \sigma=n-m(p-1), \qquad \text{and also} \qquad r(k)=v(k!). \tag{18}$$

The next theorem gives a bound for the powers of p in the denominators of $\hat{B}_n^{(l)}$. For fixed n, the bound is good, but it is not necessarily a good estimate for fixed l. See [1, 12, 22] for discussions of this point.

THEOREM 4.2. *If l is a p-adic integer and $S(n)$ is the base p digit sum, then $v(\hat{B}_n^{(l)}) \geqslant -[S(n)/(p-1)]$, or equivalently $v(\hat{B}_n^{(l)}/n!) \geqslant -m$.*

Proof. Since by Corollary 2.3(ii)

$$\frac{\hat{B}_n^{(l)}}{n!} = \sum_{w \leqslant n} \frac{\binom{l-n-1}{d}\binom{d}{u} c^u}{\Lambda^u} c_{n-w}, \tag{19}$$

the theorem follows immediately from [2, Lemma 2(i)], which says that

$$v(\Lambda^u) \leqslant m. \tag{20}$$

This completes the proof. ∎

The following theorem, which resembles formula (13), gives a Kummer-type congruence for higher order universal Bernoulli numbers. The congruence is trivial for certain values of l, e.g., if $l=1$ and $S(n)>p-1$, but, as the remark after the theorem shows, the congruence is sharp for other values of l. This is primarily a theorem for higher order universal Bernoulli numbers.

THEOREM 4.3.

$$p^m \frac{\hat{B}_n^{(l)}}{n!} \equiv (-1)^m \binom{n+m-l}{m} \frac{\hat{B}_\sigma^{(l)}}{\sigma!} c_{p-1}^m \pmod{p}.$$

Proof. The proof, which uses Corollary 2.3(ii), is based on [2, Lemma 2(ii)] that

$$v(\Lambda^u) < m \quad \text{if} \quad u_{p-1} \neq m. \tag{21}$$

The proof is essentially the same as that for [2, Theorem 1(i)]. ∎

Remark 4.4. For given n, the preceding theorem demonstrates that the estimate for the p-adic denominator given by Theorem 4.2 is sharp. We know that if $p-1 \mid n$ then the bound is achieved by the Nörlund number $\hat{B}_n^{(n)}$. (See [1, Remark 2].) We can easily deduce from Theorem 4.3 that if $p \nmid n$ then the bound is sharp for $\hat{B}_n^{(n)}$, while if $p \mid n$ it is sharp for $\hat{B}_n^{(n-1)}$ since in this case $p \nmid m+1$. In both cases the coefficient of $c_\sigma c_{p-1}^m$ in the right-hand side of the congruence in Theorem 4.3 is nonzero.

THEOREM 4.5. *If $p(p-1) \nmid n$ then $l \mid p^m \hat{B}_n^{(l)}/n!$.*

Proof. The proof is essentially the same as [2, Theorem 2(i)], using a restatement of [2, Lemma 4(ii)] that

$$w = n \text{ and } p(p-1) \nmid n \text{ implies that } s \mid p^m t_u(s) \text{ } p\text{-adically.} \quad \blacksquare \tag{22}$$

The next theorem is our higher order universal Kummer congruence. The hypothesis $\sigma > 1$ is essential, as shown by Proposition 4.1(ii), with $l = p$.

THEOREM 4.6. *If $\sigma > 1$ then*

$$p^m \frac{\hat{B}_n^{(l)}}{n!} \equiv (-1)^m \binom{n+m-l}{m} \frac{\hat{B}_\sigma^{(l)}}{\sigma!} c_{p-1}^m \pmod{pl}.$$

Proof. We must modify the proof of [2, Theorem 2(ii)], since that proof uses the higher order Bernoulli polynomial. The modification is not entirely trivial.

By [2, Lemma 4(iii)] and Corollary 2.3(i), if $S = \{(u) \mid w(u) = n \text{ and } u_{p-1} = m\}$ and $S' = \{(u') \mid w' = \sigma\}$, then

$$p^m \frac{\hat{B}_n^{(l)}}{n!} \equiv p^m \frac{l}{l-n} \sum_{u \in S} t_u(l-n)\, c^u \pmod{pl}. \tag{23}$$

But if $(u) \in S$, then

$$p^m \frac{l}{l-n} t_u(l-n) = \frac{l}{l-n}\binom{l-n}{m} t_{u'}(l-n-m)$$
$$= l\binom{l-n-1}{m}(l-n-m-1)_{d'-1}\gamma_{u'}$$
$$\equiv \binom{l-n-1}{m}\frac{l}{l-\sigma}(l-\sigma)_{d'}\gamma_{u'} \qquad (\text{mod } pl).$$

Since

$$\binom{l-n-1}{m} = (-1)^m \binom{n+m-l}{m},$$

the result follows using Corollary 2.3(i) by summation over $(u) \in S$. ∎

The following corollary gives important special cases where $S(n) < p-1$, so that $p^m/n!$ is a p-adic unit.

COROLLARY 4.7. *Let* $1 < \sigma < p-1$. *Then*

(i) $\hat{B}^{(l)}_{p+\sigma-1} \equiv (1-l/\sigma)\,\hat{B}^{(l)}_{\sigma}\, c_{p-1} \pmod{pl}$.

(ii) $\hat{B}^{(l)}_{\sigma p} \equiv (-l)^{\sigma}\binom{l-1}{\sigma}\,\hat{B}^{(l)}_{\sigma}\, c^{\sigma}_{p-1} \pmod{pl}$.

Proof. (i) is the special case $m=1$ and (ii) is the special case $m=\sigma$ of the theorem. Since $S(n) = \sigma < p-1$ in both cases,

$$\hat{B}^{(l)}_n \equiv (-1)^m \frac{n!}{p^m}\binom{n+m-l}{m}\frac{\hat{B}^{(l)}_{\sigma}}{\sigma!} c^m_{p-1} \qquad (\text{mod } pl).$$

Part (i) follows since $(p+\sigma-1)!/p \equiv -(\sigma-1)! \pmod{p}$, and part (ii) follows since $(\sigma p)!/p^{\sigma} \equiv (-1)^{\sigma}\sigma! \pmod{p}$ by formula (2). Note that $l \mid \hat{B}^{(l)}_{\sigma}$ here. ∎

We now turn our attention to the universal Nörlund polynomials $\hat{B}^{(x)}_n$. Examples found for small n by Corollary 2.3(i) are

$$\hat{B}^{(x)}_0 = 1, \qquad \hat{B}^{(x)}_1 = \tfrac{1}{2}xc_1, \qquad \hat{B}^{(x)}_2 = \tfrac{1}{4}x^2c_1^2 + x(-\tfrac{3}{4}c_1^2 + \tfrac{2}{3}c_2),$$

and (24)

$$\hat{B}^{(x)}_3 = \tfrac{1}{8}x^3c_1^3 + x^2(c_1c_2 - \tfrac{9}{8}c_1^3) + x(\tfrac{5}{2}c_1^3 - 4c_1c_2 + \tfrac{3}{2}c_3).$$

The following theorem gives a precise formula for the highest power of p in a denominator of the universal Nörlund polynomial.

THEOREM 4.8.

$$v(\hat{B}_n^{(x)}/n!) = -v((mp)!).$$

Proof. It should be noted that the classical version of this result was first found by Lundell [15, Proposition 2.2] and was rediscovered by the author [3, Theorem 1]. The proof, which is based on [3, Lemma 2], works here as well. The main idea is to show that $v(u!\,\Lambda^u) \leqslant r(mp)$, with equality iff $u_{p-1} = m-k$, $u_1 \geqslant kp$, and $p \nmid \binom{m}{k}$. ∎

We will now prove a stronger version of the lemma mentioned above, which is necessary for the stronger version of the congruence [3, Theorem 3] that we will prove below.

LEMMA 4.9. *Let* $v_1(u) = v(u!\,\Lambda^u)$. *Suppose* $w(u) < (m+1)(p-1)$. *Then*

(i) $v_1(u) \leqslant r(mp)$,

(ii) $v_1(u) \leqslant r((m-1)p)$ *unless* $u_{p-1} + [u_1/p] \geqslant m$.

Proof. We give a proof like [3, Lemma 2], but sharpened slightly. It is easy to see that $u_{p-1} + [u_1/p] \geqslant m$ if and only if $u_{p-1} + [u_1/p] = m$, namely, if $u_{p-1} = m-k$ and $[u_1/p] = l$, then $m-k+l \geqslant m$ if and only if $l \geqslant k$. But $(m+1)(p-1) > (m-k)(p-1) + lp = m(p-1) + (l-k)(p-1) + l$, so $l \leqslant k$. Also, if $w(u) \leqslant n = m(p-1) + \sigma$ and $l \geqslant k$ then $k = l \leqslant \sigma$.

We now prove both parts of the lemma simultaneously by induction on m. The $m = 0$ case is trivial. The proof now becomes quite similar to that of Lemma 3.1.

Case 1. $u_i \geqslant p$ for some $1 < i < p-1$ or $u_i > 0$ for some $i > p-1$ such that $p \nmid i+1$. In this case, let $u_i' = 0$, $u_1' = u_1 + u_i$, and $u_j' = u_j$ for $j \neq 1, i$. Then $w(u') \leqslant w(u) - (p-1)$ and $v(u'!) \geqslant v(u!)$, so $v_1(u) \leqslant v_1(u') \leqslant r((m-1)p)$, by the inductive assumption.

Case 2. $u_i > 0$ for some $i > p-1$ such that $p \mid i+1$. This case is treated differently from Lemma 3.1. If $\alpha = v(i+1)$, let $u_i' = 0$, $u_{p-1}' = u_{p-1} + \alpha u_i$, and $u_j' = 0$ for $j \neq i, p-1$. Then $v_1(u) \leqslant v_1(u')$ and again $v_1(u') \leqslant r((m-1)p)$ since $w(u') \leqslant w(u) - (p-1)$, since $kp - 1 - (p-1) \geqslant p-1$ if $k \geqslant 2$ and $p^\alpha - 1 - \alpha(p-1) \geqslant p-1$ if $\alpha \geqslant 2$. Hence $v_1(u) \leqslant v_1(u') \leqslant r((m-1)p)$.

Thus from Cases 1 and 2, if $v(u) > r((m-1)p)$ then $v_1(u) = v(u_1!\,u_{p-1}!\,p^{u_{p-1}})$. If $u_{p-1} = m-k$ and $l = [u_1/p]$ then $v_1(u) = r(lp) + r((m-k)p) \leqslant r((m-k+l)p) \leqslant r(mp)$. Also, if $m-k+l < m$, i.e., $l \leqslant k-1$, then $v_1(u) \leqslant r((l+m-k)p) \leqslant r((m-1)p)$. Hence $v(u) > r((m-1)p)$ implies $l = k$.

Finally, observe that

$$v_1(u) = r(mp) \qquad \text{iff} \quad u_1 \geqslant kp,\ u_{p-1} = m-k, \text{ and } p \nmid \binom{m}{k}. \tag{25}$$

The largest k satisfying (25) is $\min\{\sigma, m \bmod p\}$. ∎

The following theorem is the universalization of the mod mp congruence that was stated in [3], but where only the mod p congruence was proved [3, Theorem 3]. As usual, $m=[n/(p-1)]$, $\sigma=n-m(p-1)$, and $r(k)=v(k!)$. Recall that polynomial congruence means the congruence of all respective coefficients.

THEOREM 4.10.

$$p^{r(mp)}\frac{\hat{B}_n^{(x)}}{n!}\equiv\frac{p^{r(m)}}{m!}\sum_k\binom{m}{k}\left(-\frac{1}{2}\right)^k(x-n-1)_{k(p-1)+m}\frac{\hat{B}_{\sigma-k}^{(x)}}{(\sigma-k)!}c_1^{kp}\,c_{p-1}^{m-k}$$

$$(\bmod mp),$$

where $0\leqslant k\leqslant\min\{\sigma, m\}$ is the range of summation.

Proof. Let $S_k=\{(u)\mid w(u)\leqslant n,\ u_{p-1}=m-k, \text{ and } u_1\geqslant kp\}$, for $0\leqslant k\leqslant\min\{m,\sigma\}$. Then, by Corollary 2.3(ii) and the preceding lemma, it suffices to consider $p^{r(mp)}\sum_k\sum_{u\in S_k}t_u(x-n-1)\,c^u c_{n-w}$.

If $(u)\in S_k$, let $u_1'=u_1-kp$, $u_{p-1}'=0$, and $u_j'=u_j$ if $j\neq 1,\ p-1$. Then it is easy to see that $(u)\mapsto(u')$ gives a one–one correspondence between S_k and $\{(u')\mid w(u')\leqslant\sigma-k\}$, and that if $(u)\mapsto(u')$, then $w'=w-kp-(m-k)(p-1)=w-n+(\sigma-k)$ and $d'=d-kp-(m-k)=d-k(p-1)-m$. Also, if $(u)\in S_k$ then by (2) and Fermat's Little Theorem we have mod mp,

$$p^{r(mp)}t_u(x-n-1)\,c^u$$

$$\equiv\frac{p^{r(m)}}{m!}\binom{m}{k}\left(-\frac{1}{2}\right)^k(x-n-1)_{k(p-1)+m}\,t_{u'}(x-(\sigma-k)-1)\,c^{u'}c_1^{kp}\,c_{p-1}^{m-k}.$$

The result follows by summing over k and over $(u)\in S_k$. ∎

Remark 4.11. The preceding theorem and lemma show that $(mp)!$ is the p-adic least common denominator of $\hat{B}_n^{(x)}/n!$, and the highest degree coefficient where it occurs has degree $m+\sigma+k(p-2)$, where $k=\min\{\sigma, m \bmod p\}$.

Also, if $m\neq 0$ the preceding congruence does not hold mod mp^2, namely, the term with $u_{p-1}=m-1$, $u_\sigma=1$, and $u_j=0$ for $j\neq p-1$, σ satisfies $v_1(u)=r((m-1)p)$ and alters the coefficient of $c_\sigma c_{p-1}^m$ mod mp^2.

The following corollaries to Theorem 4.10 involve cases where $\sigma = 0$.

COROLLARY 4.12. *If* $p-1 \mid n$ *and* $m = n/(p-1)$ then

$$p^{r(mp)} \frac{\hat{B}_n^{(x)}}{n!} \equiv p^{r(m)} \binom{x-n-1}{m} c_{p-1}^m \pmod{mp}.$$

The next corollaries have $p = 2$, where the situation is easy because we can explicitly list the relevant terms.

COROLLARY 4.13.

$$2^n \hat{B}_n^{(x)} \equiv (x-n-1)_n \, c_1^n \pmod{2n}.$$

Proof. In this case $m = n$ and $p-1 \mid n$. ∎

Remark 4.14. In his paper on the classical Nörlund polynomials [8], the only congruence that Carlitz gave [8, (6.3)] is the weaker mod 2 version of this corollary. His method, using the theory of Hurwitz series, does not appear to be generalizable.

COROLLARY 4.15.

$$2^n \hat{B}_n^{(x)} \equiv x(x-n-1)_{n-1} \, c_1^n \pmod{4n}.$$

Proof. It is easy to see that the two terms with $u_1 = n$ and with $u_1 = n-1$ are the only ones that must be considered mod $4n$. The critical term with $u_1 = n-3$ and $u_3 = 1$ does not contribute mod $4n$ since in this case $v_1(u) = r(n-3) + n - 1$ and $r(n-3) < r(n)$. ∎

In principle we can get congruences modulo higher powers of 2 by explicitly listing the relevant terms.

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. A. Adelberg, Arithmetic properties of the Nörlund polynomial $B_n^{(x)}$, *Discrete Math.* (Gould Anniversary Volume) **204** (1999), 5–13.
4. A. J. Baker, F. Clarke, N. Ray, and L. Schwartz, On the Kummer congruences and the stable homotopy of *BU*, *Trans. Amer. Math. Soc.* **316** (1989), 385–432.
5. J. Bernoulli, "Ars Conjectandi," Basel, 1713.

6. L. Carlitz, The coefficients of the reciprocal of a series, *Duke Math. J.* **8** (1941), 689–700.
7. L. Carlitz, Criteria for Kummer's congruences, *Acta Arith.* **6** (1961), 375–391.
8. L. Carlitz, Some properties of the Nörlund polynomial $B_n^{(x)}$, *Math. Nachr.* **33** (1967), 297–311.
9. F. Clarke, The universal von Staudt theorems, *Trans. Amer. Math. Soc.* **315** (1989), 591–603.
10. I. Dibag, An analogue of the von Staudt–Clausen theorem, *J. Algebra* **87** (1984), 332–341.
11. I. P. Goulden and D. M. Jackson, "Combinatorial Enumeration," Wiley, New York, 1983.
12. F. T. Howard, Congruences and recurrences for Bernoulli numbers of higher order, *Fibonacci Quart.* **32** (1994), 316–328.
13. W. Johnson, *p*-Adic proofs of congruences for the Bernoulli numbers, *J. Number Theory* **7** (1975), 251–265.
14. N. M. Katz, The congruences of Clausen–von Staudt and Kummer for Bernoulli–Hurwitz numbers, *Math. Ann.* **216** (1975), 1–4.
15. A. T. Lundell, On the denominator of generalized Bernoulli numbers, *J. Number Theory* **26** (1987), 79–88.
16. I. Niven, H. Zuckerman, and H. Montgomery, "An Introduction to the Theory of Numbers," 5th ed., Wiley, New York, 1991.
17. N. E. Nörlund, "Vorlesungen über Differenzenrechnung," Springer, Berlin, 1924.
18. N. Ray, Extensions of umbral calculus: penumbral coalgebras and generalized Bernoulli numbers, *Adv. in Math.* **61** (1986), 41–100.
19. C. Snyder, Kummer congruences for the coefficients of Hurwitz series, *Acta Arith.* **40** (1982), 175–191.
20. C. Snyder, Kummer congruences in formal groups and algebraic groups of dimension one, *Rocky Mountain J. Math.* **15** (1985), 1–11.
21. K. C. G. von Staudt, Beweis eines Lehrsatzes die Bernoullischen Zahlen betreffend, *J. Reine Angew. Math.* **21** (1840), 372–374.
22. P. T. Young, Congruences for Bernoulli, Euler, and Stirling numbers, *J. Number Theory* **78** (1999), 204–227.