TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 315, Number 2, October 1989

THE UNIVERSAL VON STAUDT THEOREMS

FRANCIS CLARKE

ABSTRACT. We prove general forms of von Staudt's theorems on the Bernoulli numbers. As a consequence we are able to deduce strong versions of a number of congruences involving various generalisations of the Bernoulli numbers. For example we obtain an improved form of a congruence due to Hurwitz involving the Laurent series coefficients of the Weierstrass elliptic function associated with a square lattice.

INTRODUCTION

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

$$F(S) = S + c_1 \frac{S^2}{2} + c_2 \frac{S^3}{3} + \cdots .$$

Let

$$G(T) = T - c_1 \frac{T^2}{2} + (3c_1^2 - 2c_2)\frac{T^3}{6} - \cdots$$

be the inverse series, so that $F(G(T)) = T$. We define the elements $\hat{B}_k$ of $\mathbf{Q}[c_1, c_2, \dots]$ by the formula

$$\frac{T}{G(T)} = \sum_{k \geq 0} \hat{B}_k \frac{T^k}{k!}.$$

We refer to the polynomials $\hat{B}_k$ as the *universal Bernoulli numbers*. Note that, if we substitute $c_i = (-1)^i$, we have $F(S) = \log(1 + S)$ so that $G(T) = e^T - 1$ and we obtain the classical Bernoulli numbers B_k.

In this paper we give congruences modulo $\mathbf{Z}[c_1, c_2, \dots]$ for $\hat{B}_k$, and for the divided Bernoulli number $\hat{B}_k/k$, which generalise the theorems of von Staudt on the fractional part of B_k and the denominator of B_k/k.

For example we shall prove in Corollary 6 that, if k is even, $\hat{B}_k$ is congruent modulo $\mathbf{Z}[c_1, c_2, \dots]$ to $-\sum c_{p-1}^{k/(p-1)}/p$, summing over all primes p such that $p-1$ divides k. The theorem, first proved in [21], and also by Clausen [7], that

Received by the editors August 25, 1988 and, in revised form, January 13, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11B68, 05A19; Secondary 55N22, 33A25.
Key words and phrases. Bernoulli numbers.

B_k is congruent modulo $\mathbf{Z}$ to $-\sum 1/p$, summed over the same set of primes, is an immediate corollary. Thus $\widehat{B}_k$ and B_k both have the same denominator. (The *denominator* of a polynomial f in $\mathbf{Q}[c_1, c_2, \dots]$ is defined to be the least natural number n such that $nf \in \mathbf{Z}[c_1, c_2, \dots]$.)

Von Staudt's second theorem [23] concerns the denominator of B_k/k. It has been reproved many times since; see, for example, [10], [15] and [1]. In effect von Staudt proved that if p is a prime divisor of k such that $p-1$ does not divide k then the numerator of B_k is divisible by p at least as many times as is k. This is true also for the coefficients of $\widehat{B}_k$, so that $\widehat{B}_k/k$ and B_k/k have the same denominator.

In fact we are able to prove a stronger result. We show, for example, that in the case where k is divisible by 4, $\widehat{B}_k/k$ is congruent modulo $\mathbf{Z}[c_1, c_2, \dots]$ to the sum, over the same set of primes as before, of terms of the form $zc_{p-1}^{k/(p-1)}/p^{n+1}$, where $p^n(p-1)$ divides k and the integer z is determined modulo p^{n+1} by the congruence $kz \equiv p^n(p-1) \bmod p^{2n+1}$. See Theorem 5, in which the behaviour for other values of k is also given. The flavour of this theorem is perhaps best appreciated by studying the values of the divided Bernoulli numbers given in the appendix.

A ring homomorphism $\mathbf{Z}[c_1, c_2, \dots] \to R$, where R is a torsion-free ring will give rise to results on the images of $\widehat{B}_k$ and of $\widehat{B}_k/k$ in $R \otimes \mathbf{Q}$ modulo R. As we have just explained, the homomorphism into $\mathbf{Z}$ which sends c_i to $(-1)^i$ gives us von Staudt's theorems on the classical Bernoulli numbers. The case of Corollary 6 in which the c_i are assigned arbitrary integer values, in which case the statement can be slightly simplified, was proved by Carlitz [3]. The proof given by Carlitz can be modified to cover the case where the c_i are indeterminate polynomial variables, see [20], but this approach does not yield a proof of our second von Staudt theorem, Theorem 5.

The inclusion of $\mathbf{Z}[c_1, c_2, \dots]$ in the *Lazard ring* L, which can be defined as the subring of $\mathbf{Q}[c_1, c_2, \dots]$ generated by the coefficients of the power series $G(F(S_1)+F(S_2))$, shows that our congruences for the universal Bernoulli numbers hold modulo L. The epithet "universal" for $\widehat{B}_k$ is, of course, borrowed from the fact that $G(F(S_1)+F(S_2))$ is the universal formal group. This version of the congruences was first proved by Miller [14], in the context where L is interpreted as the unitary bordism ring MU_* and c_i is represented by the complex projective space CP^i. See also [2], [17] and [18]. In fact for k odd, and greater than 1, Miller proves that $\widehat{B}_k/k$ belongs to L. However we show in Theorem 5 that, for such k, $\widehat{B}_k/k$ is congruent to $c_1^{k-3}(c_1^3+c_3)/2$ modulo $\mathbf{Z}[c_1, c_2, \dots]$, and it is easy to see that $(c_1^3+c_3)/2 \in L$.

By assigning different values to the variables c_i we obtain generalisations of theorems of Dibag [9], Ray [18], Katz [13], and Hurwitz [12].

The structure of this paper is as follows. In §1 we prove some elementary arithmetic results on factorials. Our main theorems are stated and proved in 2.

The method of proof is quite elementary. We use the Lagrange inversion principle to give, in Proposition 4, an explicit formula for the coefficients of $\widehat{B}_k$ as a polynomial in $c_1, c_2, \ldots$. A careful analysis shows that only a very limited number of these coefficients can be nonintegral. In §3 we detail various consequences of our theorems, including those mentioned above. In an appendix we list the divided Bernoulli numbers $\widehat{B}_k/k$, for $k = 1$ to 10.

1. Preliminary number-theoretic results

For any natural numbers n and a, it is clear that $(na)!/(n^a a!)$ is an integer, being the product of those integers between 1 and $na-1$ which are not multiples of n. In this section we record some properties of these integers.

Lemma 1. *If p is an odd prime and m is a natural number,*

$$\prod_{\substack{i=1 \\ p\nmid i}}^{p^m-1} i \equiv -1 \mod p^m.$$

If m is a natural number other than 2,

$$\prod_{\substack{i=1 \\ i \text{ odd}}}^{2^m-1} i \equiv 1 \mod 2^m.$$

Proof. The results are simple generalisations of Wilson's theorem and can be proved in the same way by pairing off the units modulo p^n with their inverses. The different behaviour at the prime 2 is due to the fact that the group of units modulo 2^m is not cyclic if $m > 2$.

Proposition 2. *If p is an odd prime and a is divisible by p^n with $n \geq 0$, then $(pa)!/p^a a! \equiv (-1)^a \mod p^{n+1}$.*

If a is odd then $(2a)!/2^a a!$ is odd.

If $a \equiv 2 \mod 4$ then $(2a)!/2^a a! \equiv -1 \mod 4$.

If a is divisible by 2^n with $n \geq 2$ then $(2a)!/2^a a! \equiv 1 \mod 2^{n+1}$.

Proof. There are exactly a numbers between 1 and pa which are divisible by p, namely $p, 2p, \ldots, ap$, and their product is $p^a a!$. Thus, if $a = p^n A$,

$$\frac{(pa)!}{p^a a!} = \prod_{\substack{i=1 \\ p\nmid i}}^{pa} i \equiv \begin{cases} (-1)^A \mod p^{n+1}, & \text{if } p \text{ is odd, or } p^n = 2, \\ 1 \mod 2^{n+1}, & \text{if } p = 2,\ n \neq 1, \end{cases}$$

where the congruence follows by breaking the product into A blocks, reducing modulo p^{n+1}, and applying the lemma to each block. Note that, if p is odd, a and A have the same parity, and that if $p^n = 2$ then A is odd.

Proposition 3. *If r and d are natural numbers then $(rd)!/(r+1)^d d!$ and $(r-1)!/(r+1)$ are integers unless $r = 3$ or $r+1$ is prime.*

Proof. Clearly

$$\frac{(rd)!}{(r+1)^d d!} = \frac{(d+1)(d+2)\cdots(rd-1)rd}{(r+1)^d},$$

the numerator of which is the product of $(r-1)d$ consecutive integers and is thus divisible by any prime p at least $\left[\frac{(r-1)d}{p}\right]$ times. But $\nu_p(r+1) \leq \frac{r-1}{p}$ unless $r=3$ and $p=2$, or $r+1=p$.

If $d=1$ this shows that $r+1$ divides $r!$, but since $r+1$ and r are coprime $r+1$ must divide $(r-1)!$.

Note that if $r+1$ is prime, or $r=3$, both $\frac{(rd)!}{(r+1)^d d!}$ and $\frac{(r-1)!}{r+1}$ belong to $\mathbf{Z}[\frac{1}{r+1}]$.

2. Statements and proofs of the von Staudt theorems

Proposition 4.

$$\hat{B}_k = k \sum \frac{(-1)^{D-1}(k+D-2)!\, c_1^{d_1} c_2^{d_2} \cdots c_s^{d_s}}{2^{d_1} 3^{d_2} \cdots (s+1)^{d_s} d_1!\, d_2! \cdots d_s!},$$

where the summation extends over all sequences $d_1, d_2, \ldots, d_s$ *such that* $k = d_1 + 2d_2 + \cdots + sd_s$, *and* D *denotes* $d_1 + d_2 + \cdots + d_s$.

Proof. The Lagrange inversion principle [8, Theorem A, p. 148], gives formulas for the coefficients of $G(T)^n$ in terms of the coefficients of $F(S)$. We will apply this result with $n=-1$, using the extension provided by exercise 18 (p. 163) of [8]. Thus the coefficient of $T^{k-1}/(k-1)!$ in $1/G(T)$, i.e., $\hat{B}_k/k$, is equal to the coefficient of $S^{k-2}/(k-2)!$ in $(-1/S^2)\big(F(S)/S\big)^{-k+1}$. The result now follows by using the multinomial theorem to evaluate $\big(F(S)/S\big)^{-k+1}$.

Note that this argument degenerates if $k=1$, but that this case of the proposition holds trivially.

A different proof of Proposition 4, which uses universal Stirling numbers, is given in [19]. Haigh [11] has remarked that the formula shows that $\hat{B}_k$ may be interpreted as a multiple of a truncated Schur-function.

In order to state our main theorem we define a numerical function $z(p,k)$, where p is prime and k is a natural number divisible by $p-1$. Suppose that $k = p^n(p-1)K$, where p does not divide K, then $z(p,k)$ is determined modulo p^{n+1} as follows.

If $p=2$ and $n=1$ then $z(2,k) \equiv -K \bmod 4$, otherwise $z(p,k)$ is the multiplicative inverse of K modulo p^{n+1}, so that $Kz(p,k) \equiv 1 \bmod p^{n+1}$.

Theorem 5. *If* k *is divisible by* 4,

$$\frac{\hat{B}_k}{k} \equiv \sum_{\substack{k=a(p-1) \\ p \text{ prime}}} \frac{z(p,k)}{p^{1+\nu_p(k)}} c_{p-1}^a \mod \mathbf{Z}[c_1, c_2, \ldots].$$

If k *is congruent to* 2 *modulo* 4 *and is greater than* 2,

$$\frac{\hat{B}_k}{k} \equiv \frac{c_1^{k-6} c_3^2}{2} + \sum_{\substack{k=a(p-1) \\ p \text{ prime}}} \frac{z(p,k)}{p^{1+\nu_p(k)}} c_{p-1}^a \mod \mathbf{Z}[c_1, c_2, \ldots].$$

If k is odd and greater than 1,

$$\frac{\widehat{B}_k}{k} \equiv \frac{c_1^k + c_1^{k-3}c_3}{2} \mod \mathbf{Z}[c_1, c_2, \dots].$$

Proof. If $c_1^{d_1}c_2^{d_2}\cdots c_s^{d_s}$ is a monomial of weight $k = d_1 + 2d_2 + \cdots + sd_s$ we will write

$$b(c_1^{d_1}c_2^{d_2}\cdots c_s^{d_s}) = \frac{(-1)^{D-1}(k+D-2)!}{2^{d_1}3^{d_2}\cdots(s+1)^{d_s}d_1!\,d_2!\cdots d_s!},$$

for the coefficient of $c_1^{d_1}c_2^{d_2}\cdots c_s^{d_s}$ in $\widehat{B}_k/k$ as given by Proposition 4.

We will show that

(i) if p is prime and $k = a(p-1)$ then $b(c_{p-1}^a) \equiv z(p,k)/p^{1+\nu_p(k)} \mod \mathbf{Z}$,

(ii) if $k \equiv 2 \bmod 4$ and $k > 2$ then $b(c_1^{k-6}c_3^2) \equiv \frac{1}{2} \mod \mathbf{Z}$,

(iii) if k is odd and $k > 1$ then $b(c_1^{k-3}c_3) \equiv \frac{1}{2} \mod \mathbf{Z}$,

(iv) for every other monomial $b(c_1^{d_1}c_2^{d_2}\cdots c_s^{d_s})$ is an integer.

If p is odd and $\nu_p(k) = n$ then (i) is equivalent to $kpb(c_{p-1}^a) \equiv p-1 \bmod p^{n+1}$. But

$$kpb(c_{p-1}^a) = \frac{(-1)^{a-1}(p-1)(ap)!}{(ap-1)p^a a!},$$

so that Proposition 2 gives the required result. Minor modifications cover the case where $p = 2$.

Since $k + D = 2d_1 + 3d_2 + \cdots + (s+1)d_s$, we have the following crucial identity,

$$b(c_1^{d_1}c_2^{d_2}\cdots c_s^{d_s}) = \frac{(-1)^{D-1}}{(k+D)(k+D-1)}(k+D; 2d_1, 3d_2, \dots, (s+1)d_s)\prod_{t=1}^{s}\frac{((t+1)d_t)!}{(t+1)^{d_t}d_t!},$$

where $(n; i_1, i_2, \dots, i_m)$ is the multinomial coefficient $n!/i_1!\,i_2!\cdots i_m!$, with $i_1 + i_2 + \cdots + i_m = n$. The only arithmetic property which we require of multinomial coefficients is that they are integers.

As we remarked in §1 each factor $((t+1)d_t)!/(t+1)^{d_t}d_t!$ is an integer.

If $d_r \geq 2$ we have

$$\left|b(c_1^{d_1}c_2^{d_2}\cdots c_s^{d_s})\right| = (k+D-2)\cdots(k+D-d_r+1) \cdot (k+D-d_r; 2d_1, \dots, rd_r, \dots, (s+1)d_s)\frac{(rd_r)!}{(r+1)^{d_r}d_r!}\prod_{\substack{t=1\\ t\neq r}}^{s}\frac{((t+1)d_t)!}{(t+1)^{d_t}d_t!}, \tag{1}$$

while if $d_r = 1$, the same process yields only

$$\left|b(c_1^{d_1}c_2^{d_2}\cdots c_s^{d_s})\right| = \frac{1}{(k+D-1)} \cdot (k+D-1; 2d_1, \dots, r, \dots, (s+1)d_s)\frac{r!}{(r+1)}\prod_{\substack{t=1\\ t\neq r}}^{s}\frac{((t+1)d_t)!}{(t+1)^{d_t}d_t!},$$

However, taking out the factor r, we obtain

$$(2)\quad \left|b(c_1^{d_1}c_2^{d_2}\cdots c_s^{d_s})\right| = (k+D-2;2d_1,\ldots,r-1,\ldots,(s+1)d_s)\frac{(r-1)!}{(r+1)}\prod_{\substack{t=1\\ t\neq r}}^{s}\frac{\big((t+1)d_t\big)!}{(t+1)^{d_t}d_t!}.$$

Armed with these formulas we can now consider various cases.

If $d_r > 0$ for any r other than 3 such that $r+1$ is not prime, then either (1) or (2), together with Proposition 3, shows that $b(c_1^{d_1}c_2^{d_2}\cdots c_s^{d_s})$ is an integer.

If, on the other hand, $c_{p-1}c_{q-1}$ divides $c_1^{d_1}c_2^{d_2}\cdots c_s^{d_s}$ for distinct primes p and q, either (1) or (2), shows that $b(c_1^{d_1}c_2^{d_2}\cdots c_s^{d_s})$ belongs to both $\mathbf{Z}[\frac{1}{p}]$ and $\mathbf{Z}[\frac{1}{q}]$, and hence is an integer.

Similarly if c_3c_{p-1} divides the monomial where p is an odd prime.

The only remaining case to consider is that of monomials of the form $c_1^a c_3^b$. Now

$$\left|b(c_1^a c_3^b)\right| = \frac{(2a+4b-2)!}{2^{a+2b}a!\,b!},$$

thus $b(c_1^a c_3^b) \in \mathbf{Z}[\frac{1}{2}]$ and we have $\nu_2\big(b(c_1^a c_3^b)\big) = \nu_2\big((a+2b-1)!\big) - \nu_2(a!) - \nu_2(b!) - 1$.

Thus, with $b=1$, we have $b(c_1^a c_3) \equiv \frac{a+1}{2} \bmod \mathbf{Z}$, so (iii) is proved.

If $b > 1$, we have

$$\nu_2\big(b(c_1^a c_3^b)\big) = \nu_2\big(\tbinom{a+b}{b}\big) + \nu_2\big((a+2b-1)(a+2b-2)\cdots(a+b+1)\big) - 1.$$

For $b > 2$ this is certainly nonnegative. In the case $b=2$, however, $\nu_2\big(b(c_1^a c_3^2)\big) = \nu_2\big(\tbinom{a+2}{2}\big) + \nu_2(a+3) - 1$ does equal -1 if a is divisible by 4, proving (ii).

Corollary 6. *If k is even,*

$$\widehat{B}_k \equiv -\sum_{\substack{k=a(p-1)\\ p \text{ prime}}}\frac{c_{p-1}^a}{p} \bmod \mathbf{Z}[c_1,c_2,\ldots].$$

If k is odd and greater than 1,

$$\widehat{B}_k \equiv \frac{c_1^k + c_1^{k-3}c_3}{2} \bmod \mathbf{Z}[c_1,c_2,\ldots].$$

Proof. If p is odd and $\nu_p(k) = n$, the definition of $z(p,k)$ shows that

$$\frac{kz(p,k)}{p^{n+1}} \equiv 1 - \frac{1}{p} \bmod p^n\mathbf{Z},$$

thus

$$\frac{kz(p,k)}{p^{n+1}} \equiv -\frac{1}{p} \bmod \mathbf{Z}.$$

The cases where $p=2$ involve a trivial variation.

Corollary 7. *Let p be a prime such that $k = a(p-1)$. If p is odd, or if $p = 2$ and k is divisible by 4,*

$$p\hat{B}_k \equiv (p-1)c_{p-1}^a \mod p^{1+\nu_p(k)}\mathbf{Z}_{(p)}[c_1, c_2, \dots].$$

If $k \equiv 2 \bmod 4$ and $k > 2$,

$$2\hat{B}_k \equiv 2c_1^{k-6}c_3^2 - c_1^k \mod 4\mathbf{Z}_{(2)}[c_1, c_2, \dots].$$

Proof. Multiply the appropriate congruence from Theorem 5 by pk, and use the definition of $z(p,k)$.

3. Applications

As we remarked in the introduction, von Staudt's first theorem is an immediate consequence of Corollary 6. This result was extended by von Staudt in [23] to show that the denominator of B_k/k is $d_k = \prod p^{1+\nu_p(k)}$, where the product is over all primes p such that $p-1$ divides k. This is an immediate consequence of Theorem 5, but we can deduce a stronger result.

Proposition 8. *If k is even and greater than 2,*

$$\frac{B_k}{k} \equiv \frac{k}{4} + \sum_{\substack{(p-1)|k \\ p \text{ prime}}} \frac{z(p,k)}{p^{1+\nu_p(k)}} \mod \mathbf{Z}.$$

Proof. Set $c_i = (-1)^i$ in Theorem 5.

Corollary 9. *If k is even and p is a prime such that $p-1$ divides k then*

$$pB_k \equiv p - 1 \mod p^{1+\nu_p(k)}\mathbf{Z}_{(p)}.$$

Proof. Set $c_i = (-1)^i$ in Corollary 7.

This result was proved by Carlitz, in [4, Theorem 3], for p odd, and in [5], for $p = 2$.

By refining slightly the analysis of the proof of Theorem 5 it is possible to show that if $k \equiv 2 \bmod 4$ and $k > 2$, then

$$2\hat{B}_k \equiv 2c_1^{k-6}c_3^2 - c_1^k + 4c_1^{k-2}c_2 \mod 8\mathbf{Z}_{(2)}[c_1, c_2, \dots].$$

It follows that $2B_k \equiv 5 \bmod 8\mathbf{Z}_{(2)}$ for such k. This result was first proved in [23]; see also [16, p. 256] and [6].

Assume now that k is divisible by 4. It is clear from the definition of $z(p,k)$ that for each prime p such that $p-1$ divides k, $kz(p,k)$ is congruent to $p^n(p-1)$ modulo $p^{2n+1}(p-1)$, where $n = \nu_p(k)$. Thus $kz(p,k)/p^{n+1}$ is congruent to $1 - 1/p$ modulo $p^n(p-1)\mathbf{Z}$ and hence modulo $2\mathbf{Z}$. A similar analysis applies if k is congruent to 2 modulo 4 and $k > 2$.

Thus we have the following result, first proved in [22]; see also [16, p. 258].

Corollary 10. *If k is even and $k > 2$, $B_k + \sum_{\substack{(p-1)|k \\ p \text{ prime}}} \frac{1}{p}$ has the same parity as the number of primes p such that $p-1$ divides k.*

Dibag [9] has considered the von Staudt theorems for the Bernoulli numbers which are obtained by setting

$$c_i = \begin{cases} 1, & \text{if } i = p^r - 1, \\ 0, & \text{otherwise,} \end{cases}$$

where p is a given prime.

We are able to prove stronger results and also to describe the behaviour at the prime 2, for which Dibag's results do not hold as stated.

Let $\overline{B}_k$ be the rational number obtained by substituting in $\hat{B}_k$ for the variables c_i in the manner specified above. Clearly $\overline{B}_k$ will only be nonzero if $p-1$ divides k. We will assume that this is so, and, for the moment, that p is an odd prime. By Theorem 5,

$$\frac{\overline{B}_k}{k} \equiv \frac{z(p,k)}{p^{1+\nu_p(k)}} \mod \mathbf{Z},$$

and we have $kz(p,k) \equiv p^{\nu_p(k)}(p-1) \bmod p^{2\nu_p(k)+1}(p-1)$, so that

$$\overline{B}_k \equiv \frac{p-1}{p} \mod p^{\nu_p(k)}(p-1)\mathbf{Z}.$$

If $k = n(p-1)$, Dibag defines the integer a_n as $p\overline{B}_k/u_p(k!)$, where we write $u_p(x) = xp^{-\nu_p(x)}$; the congruence for $\overline{B}_k$ becomes

$$a_n \equiv \frac{p-1}{u_p(k!)} \mod p^{1+\nu_p(n)}\mathbf{Z}_{(p)}.$$

Dibag's Theorem 3.9 asserts that this congruence holds modulo $p\mathbf{Z}_{(p)}$. The congruences for small values of n follow as in [9] with the strengthened results $a_p \equiv 1 - p \bmod p^2$, and $a_{2p} \equiv 1 - 3p \bmod p^2$. These follow respectively from the congruences $u_p\big((p(p-1))!\big) \equiv -1 \bmod p^2$ and $u_p\big((2p(p-1))!\big) \equiv -1 - 2p \bmod p^2$, which are consequences of Lemma 1.

For the case where $p = 2$ a similar argument shows that if n is even and $n > 2$,

$$a_n \equiv \frac{1}{u_2(n!)} \mod 2^{1+\nu_2(n)}\mathbf{Z}_{(2)},$$

while if n is odd and $n > 1$,

$$a_n \equiv 2 \mod 4\mathbf{Z}.$$

Weaker forms of these congruences are given in Theorem 7.4 of [18].

The Bernoulli numbers associated with the formal group of Morava's $K(n)$-theory are obtained by the more general substitution

$$c_i = \begin{cases} p^{(n-1)r}, & \text{if } i = p^{nr} - 1, \\ 0, & \text{otherwise.} \end{cases}$$

Following Ray [18] we denote these Bernoulli numbers by $B(n)_k$; thus $B(1)_k = \overline{B}_k$ in our previous notation. For $n \geq 2$ the $B(n)_k$ are all integers; $B(n)_k$ is zero unless $p^n - 1$ divides k.

Theorem 11. *If $n \geq 2$, or if $n = 1$ and $p \geq 3$,*

$$B(n)_{d(p^n-1)} \equiv up^N \mod p^{N+\nu_p(d)+p^n-n-1},$$

where u is a p-adic unit and $N = d(p^{n-1} + \cdots + p^2 + p) - n$.

In [18, Theorem 7.8], and [19, 3.9(iii)], Ray obtained this congruence, but with the smaller modulus p^{N+1}. Theorem 11 is in some sense best possible, for if $d > 1$ and $d \equiv 1 \bmod p^n$ then no larger power of p may occur as the modulus.

Theorem 11 does not follow directly from Theorem 5 as do our other results but requires a detailed analysis of all the terms given by Proposition 4. We omit the proof which, although elementary, involves a lengthy examination of various cases.

For $n = 1$ and $p \geq 5$, even stronger forms of Dibag's results which give a_n modulo $p^{\nu_p(n)+p-2}$ can be deduced.

We now show how strengthened forms of some results of Carlitz [3], Hurwitz [12] and Katz [13] may be obtained.

Let the polynomials $\widehat{BH}_k \in \mathbf{Q}[c_1, c_2, \ldots]$ be defined, for $k \geq 2$, by

$$\frac{T^2}{G(T)^2} = 1 + c_1 T + \sum_{k\geq 2} (k-1)\widehat{BH}_k \frac{T^k}{k!}.$$

We refer to the $\widehat{BH}_k$ as the *universal Bernoulli-Hurwitz numbers.* This terminology follows Katz [13]. The Lagrange inversion principle can be used to give a formula for $\widehat{BH}_k$ analogous to that of Proposition 4.

Carlitz [3, Theorem 3], showed that if the variable c_1 is set equal to zero, $\widehat{BH}_k + \hat{B}_k \in \mathbf{Z}[c_2, c_3, \ldots]$. However more is true.

Theorem 12. *For all $k \geq 2$,*

$$\frac{\widehat{BH}_k}{k} \equiv -\frac{\hat{B}_k}{k} + c_1 \frac{\hat{B}_{k-1}}{k-1} \mod \mathbf{Z}[c_1, c_2, \ldots].$$

Proof. We need only a slight modification of Carlitz' argument. It is clear that

$$\frac{1}{G(T)^2} - \frac{1}{T^2} - \frac{c_1}{T} = \sum_{k\geq 0} \frac{\widehat{BH}_{k+2}}{k+2} \frac{T^k}{k!}, \tag{3}$$

and

$$\frac{1}{G(T)} - \frac{1}{T} = \sum_{k\geq 0} \frac{\hat{B}_{k+1}}{k+1} \frac{T^k}{k!}. \tag{4}$$

Differentiating (4),

$$-\frac{G'(T)}{G(T)^2}+\frac{1}{T^2}=\sum_{k\geq 0}\frac{\widehat{B}_{k+2}}{k+2}\frac{T^k}{k!}, \tag{5}$$

so that, adding (3), (5) and $-c_1$ times (4), we obtain

$$\frac{1}{G(T)^2}-\frac{G'(T)}{G(T)^2}-\frac{c_1}{G(T)}=\sum_{k\geq 0}\left(\frac{\widehat{BH}_{k+2}}{k+2}+\frac{\widehat{B}_{k+2}}{k+2}-c_1\frac{\widehat{B}_{k+1}}{k+1}\right)\frac{T^k}{k!}. \tag{6}$$

Now, since $G(F(S))=S$, the chain rule gives $G'(F(S))=1/F'(S)$, while $F'(S)=1+\sum_{i\geq 1}c_iS^i$. Thus if $S=G(T)$ the left-hand side of (6) may be written as

$$\frac{1}{S^2}\left((1-c_1S)-(1+c_1S+c_2S^2+\cdots)^{-1}\right),$$

which is a power series in S with coefficients in $\mathbf{Z}[c_1,c_2,\dots]$. But S is a divided power series in T over the ring $\mathbf{Z}[c_1,c_2,\dots]$, and hence so is the above expression. The theorem follows.

Corollary 13. *If p is an odd prime such that $p-1$ divides k, with $k=a(p-1)$,*

$$p\widehat{BH}_k\equiv(1-p)c_{p-1}^a \mod p^{1+\nu_p(k)}\mathbf{Z}_{(p)}[c_1,c_2,\dots].$$

If p is an odd prime such that $p-1$ divides $k-1$, with $k-1=b(p-1)$,

$$p\widehat{BH}_k\equiv(p-1)c_1c_{p-1}^b \mod p^{1+\nu_p(k-1)}\mathbf{Z}_{(p)}[c_1,c_2,\dots].$$

Proof. Use Corollary 7.

Note that Corollary 13 generalises a result in [13]. It is clearly possible to describe the behaviour at the prime 2, but we omit the details.

The numbers E_m studied by Hurwitz [12] arise from setting

$$c_i=\begin{cases}\dfrac{1}{2^{2j}}\binom{2j}{j}\in\mathbf{Z}\left[\tfrac{1}{2}\right], & \text{if } i=4j,\\ 0, & \text{otherwise.}\end{cases}$$

Then we have $\widehat{BH}_{4m}=2^{4m}E_m$, where the Weierstrass elliptic function $\wp(u)$ satisfying $\wp'(u)^2=4\wp(u)^3-4\wp(u)$ has the expansion

$$\wp(u)=\frac{1}{u^2}+\sum_{m\geq 1}\frac{2^{4m}E_m}{4m}\frac{u^{4m-2}}{(4m-2)!}.$$

Now if p is a prime such that $p-1$ divides $4m$ and $p\equiv 3 \mod 4$, then Corollary 13 shows that $E_m\equiv 0 \mod p^{\nu_p(m)}\mathbf{Z}_{(p)}$, since $c_{p-1}=0$.

Suppose now that p is a prime such that $p-1$ divides $4m$ with $p\equiv 1 \mod 4$, and write $4m=r(p-1)$. We may determine integers a and b such

that $p = a^2 + b^2$ by the congruences $a \equiv 1 \bmod 2$ and $a \equiv b + 1 \bmod 4$. As Carlitz [3] remarks, a result of Gauss' shows that

$$c_{p-1} = \frac{1}{2^{(p-1)/2}} \binom{(p-1)/2}{(p-1)/4} \equiv 2a \mod p.$$

Since $\nu_p(r) = \nu_p(m)$, it follows that $c_{p-1}^r \equiv (2a)^r \bmod p^{1+\nu_p(m)}$.

Now $2^{4m} \equiv 1 \bmod p^{\nu_p(m)}$, so we have

$$pE_m \equiv (1-p)(2a)^r \mod p^{1+\nu_p(m)},$$

which generalises a result in §10 of [12]; see also [3, (6.9)].

Appendix

We list the divided Bernoulli numbers $\hat{B}_k/k$, for $k = 1$ to 10.

$$\hat{B}_1 = \frac{1}{2}c_1,$$

$$\frac{\hat{B}_2}{2} = -\frac{1}{4}c_1^2 + \frac{1}{3}c_2,$$

$$\frac{\hat{B}_3}{3} = \frac{1}{2}c_1^3 - c_1c_2 + \frac{1}{2}c_3,$$

$$\frac{\hat{B}_4}{4} = -\frac{15}{8}c_1^4 + 5c_1^2c_2 - 3c_1c_3 - \frac{4}{3}c_2^2 + \frac{6}{5}c_4,$$

$$\frac{\hat{B}_5}{5} = \frac{21}{2}c_1^5 - 35c_1^3c_2 + \frac{45}{2}c_1^2c_3 + 20c_1c_2^2 - 12c_1c_4 - 10c_2c_3 + 4c_5,$$

$$\frac{\hat{B}_6}{6} = -\frac{315}{4}c_1^6 + 315c_1^4c_2 - 210c_1^3c_3 - 280c_1^2c_2^2 + 126c_1^2c_4 + 210c_1c_2c_3 - 60c_1c_5 + \frac{280}{9}c_2^3 - 48c_2c_4 - \frac{45}{2}c_3^2 + \frac{120}{7}c_6,$$

$$\frac{\hat{B}_7}{7} = \frac{1485}{2}c_1^7 - 3465c_1^5c_2 + \frac{4725}{2}c_1^4c_3 + 4200c_1^3c_2^2 - 1512c_1^3c_4 - 3780c_1^2c_2c_3 + 840c_1^2c_5 - 1120c_1c_2^3 + 1344c_1c_2c_4 + 630c_1c_3^2 - 360c_1c_6 + 560c_2^2c_3 - 280c_2c_5 - 252c_3c_4 + 90c_7,$$

$$\frac{\hat{B}_8}{8} = -\frac{135135}{16}c_1^8 + 45045c_1^6c_2 - 31185c_1^5c_3 - 69300c_1^4c_2^2 + 20790c_1^4c_4 + 69300c_1^3c_2c_3 - 12600c_1^3c_5 + 30800c_1^2c_2^3 - 30240c_1^2c_2c_4 - 14175c_1^2c_3^2 + 6480c_1^2c_6 - 25200c_1c_2^2c_3 + 10080c_1c_2c_5 + 9072c_1c_3c_4 - 2520c_1c_7 - \frac{5600}{3}c_2^4 + 4032c_2^2c_4 + 3780c_2c_3^2 - 1920c_2c_6 - 1680c_3c_5 - \frac{4032}{5}c_4^2 + 560c_8,$$

$$\frac{\widehat{B}_9}{9} = \frac{225225}{2}c_1^9 - 675675c_1^7c_2 + \frac{945945}{2}c_1^6c_3 + 1261260c_1^5c_2^2 - 324324c_1^5c_4$$
$$- 1351350c_1^4c_2c_3 + 207900c_1^4c_5 - 800800c_1^3c_2^3 + 665280c_1^3c_2c_4$$
$$+ 311850c_1^3c_3^2 - 118800c_1^3c_6 + 831600c_1^2c_2^2c_3 - 277200c_1^2c_2c_5$$
$$- 249480c_1^2c_3c_4 + 56700c_1^2c_7 + 123200c_1c_2^4 - 221760c_1c_2^2c_4$$
$$- 207900c_1c_2c_3^2 + 86400c_1c_2c_6 + 75600c_1c_3c_5 + 36288c_1c_4^2 - 20160c_1c_8$$
$$- 61600c_2^3c_3 + 33600c_2^2c_5 + 60480c_2c_3c_4 - 15120c_2c_7 + 9450c_3^3$$
$$- 12960c_3c_6 - 12096c_4c_5 + 4032c_9,$$

$$\frac{\widehat{B}_{10}}{10} = -\frac{6891885}{4}c_1^{10} + 11486475c_1^8c_2 - 8108100c_1^7c_3 - 25225200c_1^6c_2^2$$
$$+ 5675670c_1^6c_4 + 28378350c_1^5c_2c_3 - 3783780c_1^5c_5 + 21021000c_1^4c_2^3$$
$$- 15135120c_1^4c_2c_4 - \frac{14189175}{2}c_1^4c_3^2 + 2316600c_1^4c_6 - 25225200c_1^3c_2^2c_3$$
$$+ 7207200c_1^3c_2c_5 + 6486480c_1^3c_3c_4 - 1247400c_1^3c_7 - 5605600c_1^2c_2^4$$
$$+ 8648640c_1^2c_2^2c_4 + 8108100c_1^2c_2c_3^2 - 2851200c_1^2c_2c_6 - 2494800c_1^2c_3c_5$$
$$- 1197504c_1^2c_4^2 + 554400c_1^2c_8 + 4804800c_1c_2^3c_3 - 2217600c_1c_2^2c_5$$
$$- 3991680c_1c_2c_3c_4 + 831600c_1c_2c_7 - 623700c_1c_3^3 + 712800c_1c_3c_6$$
$$+ 665280c_1c_4c_5 - 181440c_1c_9 + \frac{640640}{3}c_2^5 - 591360c_2^3c_4 - 831600c_2^2c_3^2$$
$$+ 316800c_2^2c_6 + 554400c_2c_3c_5 + 266112c_2c_4^2 - 134400c_2c_8$$
$$+ 249480c_3^2c_4 - 113400c_3c_7 - 103680c_4c_6 - 50400c_5^2 + \frac{362880}{11}c_{10}.$$

References

1. J. F. Adams, *On the groups* $J(X)$. II, Topology **3** (1965), 137–171.
2. A. J. Baker, *Combinatorial and arithmetic identities based on formal group laws*, Algebraic Topology, Barcelona, 1986 (J. Aguadé and R. Kane, eds.), Lecture Notes in Math., vol. 1298, Springer-Verlag, Berlin and New York, 1987, pp. 17–34.
3. L. Carlitz, *The coefficients of the reciprocal of a series*, Duke Math. J. **8** (1941), 689–700.
4. ____, *Some congruences for the Bernoulli numbers*, Amer. J. Math. **75** (1953), 163–172.
5. ____, *A note on the Staudt-Clausen theorem*, Amer. Math. Monthly **64** (1957), 19–21.
6. ____, *A property of the Bernoulli numbers*, Amer. Math. Monthly **66** (1959), 714–715.
7. T. Clausen, *Theorem*, Astronomische Nachrichten **17** (1840), 351–352.
8. L. Comtet, *Advanced combinatorics*, Reidel, Dordrecht and Boston, Mass., 1974.
9. I. Dibag, *An analogue of the von Staudt-Clausen theorem*, J. Algebra **87** (1984), 332–341.
10. G. Frobenius, *Über die Bernoullischen Zahlen und die Eulerschen Polynome*, Sitzungsberichte Berliner Akademie der Wissenschaften, 1910, pp. 809–847.
11. C. W. Haigh, *Newton's identities, generalised cycle-indices, universal Bernoulli numbers and truncated Schur-functions*, J. Math. Chem. (submitted).

12. A. Hurwitz, *Über die Entwicklungskoeffizienten der lemniskatischen Funktionen*, Math. Ann. **51** (1899), 196–226.
13. N. M. Katz, *The congruences of Clausen-von Staudt and Kummer for Bernoulli-Hurwitz numbers*, Math. Ann. **216** (1975), 1–4.
14. H. Miller, *Universal Bernoulli numbers and the S^1-transfer*, Current Trends in Algebraic Topology, part 2 (London, Ont., 1981), Canad. Math. Soc. Conf. Proc., vol. 2, Amer. Math. Soc., Providence, R.I., 1982, pp. 437–449.
15. J. W. Milnor and J. D. Stasheff, *Characteristic classes*, Ann. of Math. Studies, no. 76, Princeton Univ. Press, Princeton, N.J., 1974.
16. N. Nielsen, *Traité élémentaire des nombres de Bernoulli*, Gauthier-Villars, Paris, 1923.
17. N. Ray, *Extensions of umbral calculus* I: *Penumbral coalgebras and generalised Bernoulli numbers*, Adv. in Math. **61** (1986), 41–100.
18. ____, *Symbolic calculus: a 19th century approach to MU and BP*, Homotopy Theory (E. Rees and J. D. S. Jones, eds.), Proceedings of the Durham Symposium, 1985, London Math. Soc. Lecture Note Ser. No. 117, Cambridge Univ. Press, Cambridge, 1987, pp. 195–238.
19. ____, *Stirling and Bernoulli numbers for complex oriented homology theories*, Proc. Internat. Conf. Algebraic Topology, 1986, Arcata (G. Carlsson, R. L. Cohen, H. R. Miller and D. C. Ravenel, eds.), Lecture Notes in Math. vol. 1370, Springer-Verlag, Berlin and New York, 1989, pp. 362–363.
20. C. Snyder, *A concept of Bernoulli numbers in algebraic function fields*, J. Reine Angew. Math. **307/308** (1978), 295–308.
21. K. G. C. von Staudt, *Beweis eines Lehrsatzes, die Bernoullischen Zahlen betreffend*, J. Reine Angew. Math. **21** (1840), 373–374.
22. ____, *De numeris Bernoullianis*, Erlangen, 1845.
23. ____, *De numeris Bernoullianis, commentatio altera*, Erlangen, 1845.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, UNIVERSITY COLLEGE SWANSEA, SWANSEA SA2 8PP, WALES

E mail: MAFRED@UK.AC.SWAN.PYR