World Scientific
www.worldscientific.com

A general family of congruences for Bernoulli numbers

Julian Rosen

Department of Mathematics, University of Michigan
530 Church Street, Ann Arbor, MI 48109, USA
rosenjh@umich.edu

We prove a general family of congruences for Bernoulli numbers whose index is a polynomial function of a prime, modulo a power of that prime. Our family generalizes many known results, including the von Staudt–Clausen theorem and Kummer's congruence.

Keywords: Bernoulli numbers; congruences; p-adic L-functions; Kummer congruences.

Mathematics Subject Classification 2010: 11B68, 11A07

1. Introduction

1.1. *Bernoulli numbers*

The Bernoulli numbers B_n are rational numbers defined by the power series expansion

$$\frac{x}{e^x - 1} = \sum_{n \geq 0} B_n \frac{x^n}{n!}.$$

The first few values are:

n	0	1	2	3	4	5	6	7	8	9	10	11	12
B_n	1	$-\frac{1}{2}$	$\frac{1}{6}$	0	$-\frac{1}{30}$	0	$\frac{1}{42}$	0	$-\frac{1}{30}$	0	$\frac{5}{66}$	0	$-\frac{691}{2730}$

Terms of odd index greater than 1 vanish, and the nonzero terms alternate in sign.

The Bernoulli numbers are known to have interesting arithmetic properties. One well-known example is the von Staudt–Clausen Theorem, which says that for every even integer $n \geq 2$, the quantity

$$B_n + \sum_{\substack{p \text{ prime,} \\ p-1 \mid n}} \frac{1}{p}$$

is an integer. In particular, the denominator of B_n is the product of those primes p such that $p-1$ divides n. Another well-known result is Kummer's congruence, which

says that for all non-negative even integers m, n not divisible by $p - 1$, satisfying $m \equiv n \mod \varphi(p^k)$,

$$\left(1 - p^{m-1}\right) \frac{B_m}{m} \equiv \left(1 - p^{n-1}\right) \frac{B_n}{n} \mod p^k. \tag{1.1}$$

Here, two rational numbers are said to be congruent modulo p^k if the p-adic valuation of their difference is at least k. Many generalizations of (1.1) are known, some involving additional terms, some relaxing the restriction that $p - 1 \nmid m$. Several generalizations are given in [1, §9.5, §11.4.2].

The results of von Staudt–Clausen and Kummer can be expressed in terms Bernoulli numbers whose index is a polynomial in p.

(1) Let $f(t) \in \mathbb{Z}[t]$ have positive leading coefficient, and set $\delta = -1$ if $f(1) = 0$, and $\delta = 0$ if $f(1) \neq 0$. Then the von Staudt–Clausen theorem implies that

$$pB_{f(p)} \equiv \delta \mod p \tag{1.2}$$

for every prime $p > |f(1)|$.

(2) Let $f(t), g(t) \in \mathbb{Z}[t]$ be distinct non-constant polynomials with positive leading coefficient, and suppose that $f(1) = g(1) \neq 0$. Let k be the largest power of t dividing $f(t) - g(t)$. Then Kummer's congruence implies that

$$\frac{B_{f(p)}}{f(p)} \equiv \frac{B_{g(p)}}{g(p)} \mod p^{k+1} \tag{1.3}$$

holds for every prime $p > |f(1)|$.

Here, we consider the following problem.

Question 1.1. Given polynomials $f_1(t), \ldots, f_n(t) \in \mathbb{Z}[t]$ with positive leading coefficients, rational functions $g_0(t), g_1(t), \ldots, g_n(t) \in \mathbb{Q}(t)$, and a non-negative integer N, determine under which circumstances the congruence

$$\sum_{i=1}^{n} g_i(p) B_{f_i(p)} \equiv g_0(p) \mod p^N \tag{1.4}$$

holds for every sufficiently large prime p.

The polynomial form of the von Staudt–Clausen theorem (1.2) and Kummer's congruence (1.3) are examples of (1.4). Other examples are known. For instance, it is a result of Sun [2] that for integers k, b, with $b \not\equiv 0 \mod p - 1$ even and $k \geq 0$:

$$\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv k \frac{B_{p-1+b}}{p-1+b} - (k-1)(1 - p^{b-1}) \frac{B_b}{b} \mod p^2, \tag{1.5}$$

$$\frac{B_{k(p-1)+b}}{k(p-1)+b} \equiv \binom{k}{2} \frac{B_{2(p-1)+b}}{2(p-1)+b} - k(k-2) \frac{B_{p-1+b}}{p-1+b}$$
$$+ \binom{k-1}{2}(1 - p^{b-1}) \frac{B_b}{b} \mod p^3. \tag{1.6}$$

1.2. *Results*

The main result of this paper is a criterion for (1.4) to hold.

Theorem 1.2. *Fix an integer N, non-constant polynomials $f_1(t), \ldots, f_n(t) \in \mathbb{Z}[t]$ with positive leading coefficients, and rational functions $g_0(t), \ldots, g_n(t) \in \mathbb{Q}(t)$. Write v_t for the t-adic valuation on $\mathbb{Q}(t)$, and set*

$$M = \min\{v_t(g_i(t))\}.$$

Then, the congruence

$$\sum_{i=1}^n g_i(p)B_{f_i(p)} \equiv g_0(p) \mod p^N \tag{1.7}$$

holds for every sufficiently large prime p if all of the following conditions hold:

(1)

$$v_t\left(g_0(t) - \left(1 - \frac{1}{t}\right)\sum_{\substack{i \\ f_i(1)=0}} g_i(t) - \sum_{\substack{i \\ f_i(1)\geq 2}} (1 - t^{f_i(1)-1})\frac{B_{f_i(1)}}{f_i(1)}g_i(t)f_i(t)\right) \geq N.$$

(2) *For every even, non-positive integer $k \in \{f_i(1)\}$ and every $1 \leq m \leq N - M$,*

$$v_t\left(\sum_{\substack{i \\ f_i(1)=k}} g_i(t)f_i(t)^m\right) \geq N + 1 - m.$$

(3) *For every even, positive integer $k \in \{f_i(1)\}$ and $2 \leq m \leq N - M$,*

$$v_t\left(\sum_{\substack{i \\ f_i(1)=k}} g_i(t)\big(f_i(t)^m - k^{m-1}f_i(t)\big)\right) \geq N + 1 - m.$$

The verification of the conditions (1)–(3) of Theorem 1.2 is a finite computation. The condition that the polynomials $f_i(t)$ are non-constant is for simplicity and is inessential: for each $f_i(t)$ that is constant, the term $g_i(p)B_{f_i(p)}$ can be moved to the right-hand side of (1.7) and made part of $g_0(p)$.

Remark 1.3. It can be checked that Theorem 1.2 implies both (1.2) and (1.3), so we may view Theorem 1.2 as a common generalization of the von Staudt–Clausen Theorem and Kummer's congruence. The congruences (1.5) and (1.6) also follow from Theorem 1.2, as do many of the congruences for Bernoulli numbers given in [1].

The author does not know whether the converse of Theorem 1.2 holds. If it does, this is likely quite difficult to prove. In particular, the converse of Theorem 1.2 would imply that there exist infinitely many non-Wolstenholme primes (that is, infinitely many primes p for which $p \nmid B_{p-3}$), which is an open question.

2. The Kubota–Leopoldt *p*-Adic Zeta Function

The Riemann zeta function $\zeta(s)$ takes rational values at the non-positive integers, and we have a formula

$$\zeta(-n) = -\frac{B_{n+1}}{n+1}.$$

Fix a prime $p \geq 3$. Kummer's congruence implies that the values

$$(1 - p^{-s})\zeta(s)$$

are p-adically uniformly continuous if s is restricted to the negative integers in a fixed residue class modulo $p - 1$. For $n \geq 2$ an integer, the *Kubota–Leopoldt p-adic zeta value* is defined by

$$\zeta_p(n) := \lim_{\substack{s \to n \text{ } p\text{-adically,} \\ s \leq 0 \\ s \equiv n \mod p-1}} (1 - p^{-s})\zeta(s).$$

The function $n \mapsto \zeta_p(n)$ is not p-adic analytic, but comes from $p - 1$ analytic functions, one for each residue class modulo $p - 1$.

The following proposition gives a bound on the valuation of the power series coefficients for the p-adic zeta function. It is essentially a repackaging of known results.

Proposition 2.1. *Let p be an odd prime, k an even residue class modulo $p - 1$. Then there exist coefficients $a_i(p, k) \in \mathbb{Q}_p$ for $i = 0, 1, 2, \dots$ such that for every non-negative integer n with $n \equiv k \mod p - 1$, there is a convergent p-adic series identity*

$$B_n = (1 - p^{n-1})^{-1} \sum_{i \geq 0} a_i(p, k) n^i. \tag{2.1}$$

The coefficients $a_i(p, k)$ satisfy the following conditions:

(1)

$$a_0(p, k) = \begin{cases} 1 - \dfrac{1}{p} & \text{if } k \equiv 0 \mod p - 1, \\ 0 & \text{otherwise,} \end{cases}$$

(2) *for all i, p, k,*

$$v_p(a_i(p, k)) \geq \frac{p-2}{p-1}i - 2,$$

(3) *for $p \geq i + 2$ and all k,*

$$v_p(a_i(p, k)) \geq i - 1.$$

Proof. Let ω_p be the Teichmüller character. For every residue class k modulo $p-1$, there is a Laurent series expansion for the Kubota–Leopoldt p-adic L-function:

$$L_p(s, \omega_p^k) = \sum_{i \geq -1} c_{i,k}(s - 1)^i.$$

The relationship between L_p and Bernoulli numbers is given by

$$-(1 - p^{n-1})\frac{B_n}{n} = L_p(1 - n, \omega_p^n),$$

so we may take $a_i(p, k) = (-1)^i c_{i-1,k}$. Statement (1) of the proposition follows from the fact that $L_p(s, \omega_p^k)$ has a simple pole of residue $1 - \frac{1}{p}$ at $s = 1$ if $k \equiv 0 \mod p - 1$, and is analytic otherwise.

To get the desired bounds on the valuation of the a_i, we use [3, Theorem 5.11] (in the case $\chi = \omega_p^k$, $f = p$, $F = p(p-1)$):

$$L_p(s, \omega_p^k) = \frac{1}{p(p-1)}(s-1)^{-1} \sum_{j=0}^{\infty} p^j (p-1)^j \binom{1-s}{j} B_j \sum_{\substack{a=1 \\ p \nmid a}}^{p(p-1)} \frac{\omega_p^k(a)}{a^j} \langle a \rangle^{1-s},$$

where $\langle a \rangle := a/\omega_p(a) \equiv 1 \mod p$. Write $\langle a \rangle = 1 + pq_a$, with $q_a \in \mathbb{Z}_p$. We can expand $\langle a \rangle^{s-1}$ as a binomial series to obtain

$$L_p(s, \omega_p^k) = \frac{1}{p(p-1)}(s-1)^{-1} \sum_{i,j=0}^{\infty} p^{i+j}(p-1)^j \binom{1-s}{i} \binom{1-s}{j} B_j \sum_{\substack{a=1 \\ p \nmid a}}^{p(p-1)} \frac{\omega_p^k(a)}{a^j} q_a^i.$$

The innermost summation is p-integral, so we conclude that

$$a_i(p, k) \in \frac{1}{p} \sum_{s \geq t \geq i} B_t \frac{p^s}{s!} \mathbb{Z}_p.$$

Now we have $v_p(B_t) \geq -1$ by the von Staudt–Clausen Theorem, and $v_p(s!) \leq s/(p-1)$, so

$$v_p(a_i(p, k)) \geq \frac{p-2}{p-1}i - 2,$$

which implies statement (2) of the Proposition. Finally, if $p \geq i + 2$, then

$$\frac{p^s}{s!} B_t \in p^i \mathbb{Z}_p$$

for all $s \geq t \geq i$, so in this case we have $v_p(a_i(p, k)) \geq i - 1$. This completes the proof. □

3. Proof of the Theorem

We start with an easy fact.

Proposition 3.1. *Suppose $g(t) \in \mathbb{Q}(t)$ is nonzero. Then*

$$v_p(g(p)) = v_t(g(t)) \tag{3.1}$$

for all but finitely many primes p.

Proof. We can write

$$g(t) = t^{v_t(g(t))} \frac{a(t)}{b(t)},$$

where $a(t)$, $b(t) \in \mathbb{Z}[t]$ satisfy $a(0)b(0) \neq 0$. The equality (3.1) then holds for every prime not dividing $a(0)b(0)$. □

We are now ready to prove Theorem 1.2.

Proof of Theorem 1.2. Suppose $f_1, \ldots, f_n$ are non-constant integer polynomials with positive leading coefficient, $g_0, \ldots, g_n$ are rational functions, and N is an integer, satisfying conditions (1)–(3). We would like to prove that the quantity

$$A(p) := g_0(p) - \sum_{i=1}^{n} g_i(p) B_{f_i(p)}$$

is divisible by p^N for every sufficiently large prime p. We can compute an expression for $A(p)$ in terms of the $a_i(p, k)$ from the previous section:

$$A(p) = g_0(p) - \sum_{\substack{k \in \mathbb{Z}/(p-1) \\ f_i(p) \equiv k \ (p-1)}} \sum_{i} g_i(p) B_{f_i(p)}$$

$$= g_0(p) - \sum_{\substack{k \in \mathbb{Z}/(p-1) \\ m \geq 0}} \left(\sum_{\substack{i \\ f_i(p) \equiv k \ (p-1)}} \left(1 - p^{f_i(p)-1}\right)^{-1} g_i(p) f_i(p)^m \right) a_m(p, k).$$

We have $f_i(p) \equiv f_i(1)$ modulo $p - 1$, so for every $p > \max\{f_i(1) - f_j(1)\}$,

$$A(p) = g_0(p) - \sum_{\substack{k \in \mathbb{Z} \\ m \geq 0}} \left(\sum_{\substack{i \\ f_i(1) = k}} \left(1 - p^{f_i(p)-1}\right)^{-1} g_i(p) f_i(p)^m \right) a_m(p, k).$$

Because $f_i(t)$ is non-constant, we have $v_p(p^{f_i(p)}) \to \infty$ as $p \to \infty$, so

$$A(p) \equiv g_0(p) - \sum_{\substack{k \in \mathbb{Z} \\ m \geq 0}} \left(\sum_{\substack{i \\ f_i(1) = k}} g_i(p) f_i(p)^m \right) a_m(p, k) \mod p^N \qquad (3.2)$$

for every sufficiently large prime p.

Now, for p larger than $\max\{f_i(1)\}$, we have

$$a_0(p, k) = \begin{cases} 1 - \dfrac{1}{p} & \text{if } k = 0, \\ 0 & \text{otherwise,} \end{cases}$$

for every k for which the inner sum in (3.2) is non-empty. This allows us to rewrite (3.2) using no terms $a_0(p, k)$. We can also eliminate the terms $a_1(p, k)$ for $k \geq 2$. By Proposition 2.1, we have

$$B_k = (1 - p^{k-1})^{-1} \sum_{m \geq 0} a_m(p, k) k^m,$$

so we can solve for $a_1(p, k)$ in terms of $a_m(p, k)$, $m \geq 2$:

$$a_1(p, k) = (1 - p^{k-1}) \frac{B_k}{k} - \sum_{m \geq 2} a_m(p, k) k^{m-1}.$$

We substitute the expressions for $a_0(p, k)$ and $a_1(p, k)$ into (3.2) to obtain

$$A(p) \equiv g_0(p) - \sum_{\substack{k \leq -2 \text{ even} \\ m \geq 1}} \sum_{\substack{i \\ f_i(1) = k}} g_i(p) f_i(p)^m a_m(p, k)$$

$$- \left(1 - \frac{1}{p}\right) \sum_{\substack{i \\ f_i(1) = 0}} g_i(p) - \sum_{m \geq 1} \sum_{\substack{i \\ f_i(1) = 0}} g_i(p) f_i(p)^m a_m(p, 0)$$

$$- \sum_{k \geq 2 \text{ even}} \left(1 - p^{k-1}\right) \frac{B_k}{k} \sum_{\substack{i \\ f_i(1) = k}} g_i(p) f_i(p)$$

$$- \sum_{\substack{k \geq 2 \text{ even} \\ m \geq 2}} \sum_{\substack{i \\ f_i(1) = k}} g_i(p) \left(f_i(p)^m - k^{m-1} f_i(p)\right) a_m(p, k) \mod p^N.$$

Finally, by condition (1) of the hypothesis of the theorem,

$$g_0(p) - \left(1 - \frac{1}{p}\right) \sum_{\substack{i \\ f_i(1) = 0}} g_i(p)$$

$$- \sum_{k \geq 2 \text{ even}} \left(1 - p^{k-1}\right) B_k \sum_{\substack{i \\ f_i(1) = k}} g_i(p) f_i(p) \equiv 0 \mod p^N.$$

By condition (2) of the hypothesis of the theorem, for every even $k \leq 0$ and $m \geq 1$,

$$\sum_{\substack{i \\ f_i(1) = k}} g_i(p) f_i(p)^m a_m(p, k) \equiv 0 \mod p^N.$$

By condition (3) of the hypothesis of the Theorem, for every even $k \geq 2$ and $m \geq 2$,

$$\sum_{\substack{i \\ f_i(1) = k}} g_i(p) \left(f_i(p)^m - k^{m-1}\right) a_m(p, k) \equiv 0 \mod p^N.$$

We conclude that $A(p) \equiv 0 \mod p^N$ for all but finitely many p. $\qquad\square$

References

[1] H. Cohen, *Number Theory. Vol. II. Analytic and Modern Tools*, Graduate Texts in Mathematics, Vol. 240 (Springer, New York, 2007).

[2] Z.-H. Sun, Congruences concerning Bernoulli numbers and Bernoulli polynomials, *Discrete Appl. Math.* **105**(1–3) (2000) 193–223.

[3] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, Vol. 83, 2nd edn. (Springer-Verlag, New York, 1997).