# BERNOULLI NUMBERS AND KUMMER'S CRITERION

HARLAN R. STEVENS*
*The Pennsylvania State University, University Park, PA 16802*
*(Submitted April 1984)*

## 1. INTRODUCTION

There is a large literature concerning various properties of the Bernoulli numbers; see, for example, [1, 12, 16, 23] and their references. According to H. S. Vandiver [23], by 1960 over 1500 papers had been written on the subject. The main thrust of the present paper is to consider several congruence properties of the Bernoulli numbers that extend various results of Vandiver, Nielson, Carlitz, and Stevens; see [2, 16, 19, 22]. The Bernoulli numbers $B_n$ $(n \geqslant 0)$ are defined by the expansion

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

which is equivalent to

$$\sum_{r=0}^{n} \binom{n}{r} B_r = B_n \qquad (n > 1) \tag{1.1}$$

together with $B_0 = 1$. It is sometimes convenient to write (1.1) in the form

$$(B + 1)^n = B^n \qquad (n > 1) \tag{1.2}$$

where it is understood that, after expansion of the left-hand side, we replace $B^k$ by $B_k$. It is easy to check that for the first few values of $n$ we have

$$B_1 = -1/2, \quad B_2 = 1/6, \quad B_4 = -1/30,$$

and that in general $B_{2k+1} = 0$ if $k \geqslant 1$.

Bernoulli numbers have numerous interesting properties. For example, if $S_n(k) = 1^n + \cdots + k^n$, then $S_n(k) = (B_{n+1}(k + 1) - B_{n+1})/(n + 1)$, where $B_n(x) = (B + x)^n$. The Bernoulli numbers are related to class numbers and to Fermat's Last Theorem. Moreover, they satisfy numerous recurrences and congruences. For further details regarding various properties of the Bernoulli numbers, the reader should consult the papers [1, 12, 16, 23] and their references.

## 2. CONGRUENCE PROPERTIES

If $p$ is a prime, we now consider several congruence properties of sequences of rational numbers where we say that $a/b$ is integral modulo $p$ if $(b, p) = 1$.

---

**Professor Stevens passed away on December 3, 1983. Many of the results in this paper were presented by him to the departmental number theory seminar held on December 1, 1983. The paper, based on results obtained by Professor Stevens, has been written by several departmental colleagues.*

Moreover, if $a/b$ and $c/d$ are integral modulo $p$, then

$$\frac{a}{b} \equiv \frac{c}{d} \pmod{p} \text{ if } ad \equiv bc \pmod{p}.$$

We assume throughout this paper that $p$ is an odd prime even though similar results could be obtained for the case in which $p = 2$.

In [15] Kummer proved that

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

for all $n > 1$, where $(p-1) \nmid n$. More generally, one can consider congruences of the form

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} \frac{B_{n+s(p-1)}}{n+s(p-1)} \equiv 0 \pmod{p^r} \tag{2.1}$$

for $n > r$, where $(p-1) \nmid n$. In [15] Kummer studied congruences similar to the above but in a more general setting in which he proved the following theorem.

**Theorem 1 (Kummer):** Let $a_n$ be integral modulo $p$ and suppose

$$\sum_{n=0}^{\infty} a_n \frac{x^n}{n!} = \sum_{n=0}^{\infty} A_n (e^x - 1)^n. \tag{2.2}$$

If the $A_n$ are integral modulo $p$, then

$$\sum_{s=0}^{r} (-1)^s \binom{r}{s} a_{n+s(p-1)} \equiv 0 \pmod{p^r}, \text{ for } n \geqslant r \geqslant 1. \tag{2.3}$$

Nielson showed in [16] that if $a_n = B_n$, the $n^{\text{th}}$ Bernoulli number, then the Bernoulli numbers themselves satisfy (2.3) if $(p-1) \nmid n$, where the modulus is replaced by $p^{r-1}$. In attempting to remove the restriction $(p-1) \nmid n$, Vandiver [22] showed that if $n = a(p-1)$ and $a_n = B_n$ then (2.3) holds modulo $p^{r-1}$ provided that $r + a < p - 1$. This latter restriction is, however, a rather severe one. In [2] Carlitz showed that the congruence (2.3) holds if $r < p - 1$ and that some much weaker congruences hold if $r \geqslant p - 1$.

Congruences similar to (2.3) were later studied in a series of papers by Carlitz and Stevens [5-9, 18-21]. Recently, a number of authors have taken renewed interest in the topic of congruences for various sequences of numbers. For example, Rota and Sagan [17], Gessel [13], J. Cowles [10], and J. Cowles, S. Chowla, and M. J. Cowles [11] have used various general combinatorial techniques, such as group actions on sets, to obtain various congruence properties for several sequences of numbers.

If one looks at Kummer's Criterion (2.2) and (2.3), it is easy to see that the condition is sufficient but not necessary. We will make use of the following theorem due to Carlitz [5].

**Theorem 2 (Carlitz):** Let $a_n$ be integral modulo $p$ and suppose

$$\sum_{n=0}^{\infty} a_n \frac{x^n}{n!} = \sum_{k=0}^{\infty} A_k \frac{(e^x - 1)^k}{k!}.$$

Then $A_k \equiv 0 \pmod{p^{[k/p]}}$ for all $k \geqslant 0$ if and only if

$$\sum_{s=0}^{r}(-1)^s\binom{r}{s}a_{n+s(p-1)} \equiv 0 \pmod{p^r}, \text{ for all } n \geqslant r \geqslant 1.$$

## 3. APPLICATIONS

In this section we apply Theorem 2 to the Bernoulli numbers to obtain several congruences that extend various results of Vandiver, Nielson, Carlitz, and Stevens, see [1, 16, 19, 22]. Finally, we use the theorem to obtain an elementary proof of the Staudt-Clausen theorem. Let us put

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!} = \frac{\log(1 + (e^x - 1))}{e^x - 1} = \sum_{n=0}^{\infty}(-1)^n \frac{n!}{n+1}\frac{(e^x - 1)^n}{n!},$$

so that

$$A_n = \frac{(-1)^n n!}{n+1}.$$

Now however, the $A_n$'s do not satisfy the condition of the theorem. If we multiply by $p$, each coefficient in the new series does satisfy the condition, except for the coefficient of

$$\frac{(e^x - 1)^{p^2-1}}{(p^2 - 1)!}.$$

Thus, we have

$$\sum_{n=0}^{\infty} pB_n \frac{x^n}{n!} = \frac{(-1)^{p^2-1}}{p}(e^x - 1)^{p^2-1} + C(x),$$

where $C(x)$ satisfies the condition of the theorem. Hence, if $D$ is the derivative operator, then

$$(D^p - D)^r \sum_{n=0}^{\infty} pB_n \frac{x^n}{n!} \equiv (D^p - D)^r \frac{(-1)^{p^2-1}}{p}(e^x - 1)^{p^2-1} \pmod{p^r},$$

where we say that

$$\sum_{n=0}^{\infty} a_n \frac{x^n}{n!} \equiv \sum_{n=0}^{\infty} b_n \frac{x^n}{n!} \pmod{m}$$

if $a_n \equiv b_n \pmod{m}$ for each $n \geqslant 0$.

We now consider $(D^p - D)^r(e^x - 1)^{p^2-1} \pmod{p^{r+1}}$. Since

$$(e^x - 1)^{p^2-1} = \sum_{j=0}^{p^2-1}(-1)^{p^2-1-j}\binom{p^2-1}{j}e^{jx},$$

if we apply the operator $(D^p - D)^r$, we get after some simplification that, for each $n \geqslant 0$, the coefficient of $x^n/n!$ is

$$\sum_{j=0}^{p^2-1}(-1)^{p^2-1-j}\binom{p^2-1}{j}(j^{p-1} - 1)^r j^{n+r}. \tag{3.1}$$

We now break the sum (3.1) into two sums $\Sigma'$ and $\Sigma''$, where in $\Sigma'$ we sum over those $j$ for which $p \nmid j$, while in $\Sigma''$ we sum over those $j$ for which $p|j$.

To compute $\Sigma'$, suppose that $j^{p-1} - 1 = pk(j)$, so that

$$\Sigma' = p^r \sum_{j=0}^{p^2-1}{}' (-1)^{p^2-1-j}\binom{p^2-1}{j} k(j)^r j^{n+r}.$$

We know that

$$\binom{p^2-1}{j} \equiv (-1)^j \pmod{p}.$$

If $j' \equiv j \pmod{p}$ so that $j' = j + Qp$, then $k(j') \equiv k(j) - j^{p-2}Q \pmod{p}$, and hence

$$(*) \qquad \sum_{j=0}^{p^2-1}{}' (-1)^{p^2-1-j}\binom{p^2-1}{j} (k(j))^r j^{n+r}$$
$$\equiv (-1)^{p^2-1} \sum_{j=1}^{p-1}\left[\sum_{Q=0}^{p-1}(k(j) - j^{p-2}Q)^r\right] j^{n+r} \pmod{p}$$
$$\equiv (-1)^{p^2-1} \sum_{j=1}^{p-1} j^{n+r} \sum_{Q=0}^{p-1} Q^r \pmod{p},$$

since the terms in the brackets run through a complete residue system modulo $p$. If $(p-1) \nmid r$, then the inner sum is zero modulo $p$, while if $(p-1) \nmid (n+r)$, then the outer sum is zero modulo $p$. If $(p-1)|r$ and $(p-1)|(n+r)$, then the left-hand side of (*) is congruent to $(-1)^{p^2-1}$ modulo $p$. Hence,

$$\Sigma' \equiv \begin{cases} 0 \pmod{p^{r+1}} & \text{if } (p-1) \nmid r \\ 0 \pmod{p^{r+1}} & \text{if } (p-1) \nmid (n+r) \\ (-1)^{p^2-1} \pmod{p^{r+1}} & \text{if } (p-1)|r \text{ and } (p-1)|(n+r). \end{cases}$$

Along similar lines, we may compute the sum $\Sigma''$ to obtain

$$\Sigma'' \equiv \begin{cases} 0 \pmod{p^{r+1}} & \text{if } (p-1) \nmid (n+r) \\ (-1)^{p^2+r} p^{n+r} \pmod{p^{r+1}} & \text{if } (p-1)|(n+r) \end{cases}$$

Therefore, combining the congruences obtained for $\Sigma'$ and $\Sigma''$, we see that $pB_n$ is integral modulo $p$. Thus, we may apply Theorem 2 to the sequence $a_n = pB_n$ to obtain

**Theorem 3:** Let $N = \sum_{s=0}^{r} (-1)^{r-s}\binom{r}{s} B_{n+s(p-1)}$

(A) If $(p-1) \nmid n$ where $n \geqslant r \geqslant 1$, then $N \equiv 0 \pmod{p^{r-1}}$.

(B) If $(p-1)|n$ and $(p-1) \nmid r$ where $n > r \geqslant 1$, then $N \equiv 0 \pmod{p^{r-1}}$.

(C) If $(p-1)|n$ and $(p-1)|r$ where $n > r \geqslant 1$, then $N \equiv p^{r-2} \pmod{p^{r-1}}$.

(D) If $n = r$ and $(p-1)|n$, then $N \equiv 0 \pmod{p^{r+1}}$.

We note that (A) is a result of Nielson [16], while the result in (B) improves upon results of Vandiver [22] and Carlitz [2].

We now obtain a generalization of these congruences. Since

$$x^{p^e} - y^{p^e} = (x^{p^{e-1}} - y^{p^{e-1}})(x^{(p-1)p^{e-1}} + x^{(p-2)p^{e-1}}y^{p^{e-1}} + x^{(p-3)p^{e-1}}y^{2p^{e-1}} + \cdots + y^{(p-1)p^{e-1}}),$$

by induction on $e$ one can prove the following identity:

$$x^{p^{e-1}} - y^{p^{e-1}} = \sum_{i=0}^{e-1} p^i (x - y)^{p^{e-1-i}} f_i(x, y) \qquad (e \geqslant 1) \tag{3.2}$$

where each $f_i(x, y)$ is a polynomial in $x$ and $y$. Let $E$ be the difference operator, and suppose $b \geqslant 1$. Let $x = E^{b(p-1)}$ and $y = 1$ in (3.2) and then take the $r^{\text{th}}$ power of both sides. We obtain

$$\sum_{s=0}^{r} (-1)^{r-s}\binom{r}{s} B_{n+sbp^{e-1}(p-1)} \equiv 0 \pmod{p^A} \tag{3.3}$$

where $A$ is the minimum of

$$-1 + \sum_{i=1}^{e-1} i\alpha \;\; + \sum_{i=0}^{e-1} p^{e-1-i}\alpha_i \quad \text{and} \quad \alpha_0 + \cdots + \alpha_{e-1} = r.$$

This minimum occurs when

$$\alpha_0 = \cdots = \alpha_{e-2} = 0 \quad \text{and} \quad \alpha_{e-1} = r.$$

Hence, if $n \geqslant er$, then $A = er - 1$. We may now state

**Theorem 4**: Let $b \geqslant 1$, $e \geqslant 1$, and $M = \sum_{s=0}^{r} (-1)^{r-s}\binom{r}{s} B_{n+sbp^{e-1}(p-1)}$.

(A) If $r \geqslant 1$, $n > er$, and either $(p - 1) \nmid n$ or $(p - 1) \nmid r$, then $M \equiv 0 \pmod{p^{er-1}}$.

(B) If $n > er$, $(p - 1)|n$, and $(p - 1)|r$, then $M \equiv 0 \pmod{p^{er-2}}$.

These results should be compared with Theorem 8 of Stevens [19].

We now apply Theorem 2 to obtain an elementary proof of

**Theorem 5 (Staudt-Clausen)**: If $n \geqslant 1$, then

$$B_{2n} = G_{2n} - \sum_{(p-1)|2n} \frac{1}{p}$$

where $G_{2n}$ is an integer.

**Proof**: It suffices to show that $pB_n \equiv -1 \pmod p$ if and only if $(p - 1)|n$. We have

$$\sum_{k=0}^{\infty} pB_k \frac{x^k}{k!} = \sum_{k=0}^{\infty} (-1)^k \frac{p}{k+1}(e^x - 1)^k.$$

By induction on $n$ in (1.1), it is easy to show that $pB_n \equiv 0 \pmod p$ if $0 \leqslant n \leqslant p - 2$, and hence from (1.1) we have that $pB_{p-1} \equiv -1 \pmod p$. If $n = a(p - 1)$, then for $r = 1$ we have $pB_{a(p-1)} \equiv pB_{p-1} \pmod{p}$ so that $B_{a(p-1)} = -1/p + Q$ where $Q$ is integral modulo $p$. Similarly, $pB_n \equiv 0 \pmod{p}$ if $(p-1) \nmid n$. Thus $p$ divides the denominator of $B_n$ if and only if $(p-1)|n$.

## REFERENCES


1. L. Carlitz. "Bernoulli Numbers." *The Fibonacci Quarterly* **6** (1968):71-85.
2. L. Carlitz. "Some Congruences for the Bernoulli Numbers." *Amer. J. Math.* **75** (1953):163-172.
3. L. Carlitz. "Recurrences for the Bernoulli and Euler Numbers." *J. Reine Ang. Math.* **215** (1964):184-191.
4. L. Carlitz. "Recurrences for the Bernoulli and Euler Numbers." *Math. Nach.* **29** (1965):151-160.
5. L. Carlitz. "Criteria for Kummer's Congruences." *Acta Arith.* **6** (1961): 375-391.
6. L. Carlitz. "A Note on Kummer's Congruences." *Archiv der Math.* **7** (1957): 441-445.
7. L. Carlitz. "Kummer's Congruences (mod $2^r$)." *Monat. für Math.* **63** (1959): 394-400.
8. L. Carlitz. "Composition of Sequences Satisfying Kummer's Criterion." *Collectanea Math.* **11** (1959):137-152.
9. L. Carlitz & H. Stevens. "Criteria for Generalized Kummer's Congruences." *J. Reine Ang. Math.* **207** (1961):203-220.
10. J. Cowles. "Some Congruence Properties of Three Well Known Sequences: Two Notes." *J. Number Theory* **12** (1980):84-86.
11. J. Cowles, S. Chowla, & M. J. Cowles. "Congruence Properties for Apéry Numbers." *J. Number Theory* **12** (1980):188-190.
12. L. E. Dickson. *History of the Theory of Numbers*. II. New York: Chelsea, 1952.
13. I. M. Gessel. "Congruences for Bell and Tangent Numbers." *The Fibonacci Quarterly* **19** (1981):137-144.
14. A. Hurwitz. "Über die Entwickelungscoefficienten der lemniscatischen Funktionen." *Mathematische Werke* **2** (1933):342-373.
15. E. E. Kummer. "Über eine allegemeine Eigenschaft der rational Entwickelungscoefficienten einer bestimmten Gattung analytischer Funktionen." *J. Reine Ang. Math.* **41** (1851):368-372.
16. N. Nielson. *Traite elementaire des nombres de Bernoulli*. Paris, 1923.
17. G. C. Rota & B. Sagan. "Congruences Derived from Group Actions." *Europ. J. Comb.* **1** (1980):67-76.
18. H. Stevens. "Generalized Kummer Congruences for Products of Sequences." *Duke Math. J.* **28** (1961):25-38.
19. H. Stevens. "Generalized Kummer Congruences for Products of Sequences: Applications." *Duke Math. J.* **28** (1961):261-276.
20. H. Stevens. "Kummer Congruences for Products of Numbers." *Math. Nach.* **24** (1962):219-227.
21. H. Stevens. "Kummer's Congruences of a Second Kind." *Math. Zeitschr.* **79** (1962):180-192.
22. H. S. Vandiver. "Certain Congruences Involving the Bernoulli Numbers." *Duke Math. J.* **5** (1939):548-551.
23. H. S. Vandiver. "On Developments in an Arithmetic Theory of Bernoulli and Allied Numbers." *Scripta Math.* **25** (1960):273-303.
24. H. S. Vandiver. "Fermat's Last Theorem." *Amer. Math. Monthly* **53** (1946): 555-578.


◆◇◆◇◆