Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Journal of Number Theory 106 (2004) 169–177
JOURNAL OF Number Theory
http://www.elsevier.com/locate/jnt

Adams theorem on Bernoulli numbers revisited

R. Thangadurai*

School of Mathematics, Harish-Chandra Research Institute, Chhatnag Road, Jhusi, Allahabad 211019, India

Received 25 July 2003; revised 11 November 2003

Communicated by D. Goss

Dedicated in the memory of my father

Abstract

If we denote B_n to be nth Bernoulli number, then the classical result of Adams (J. Reine Angew. Math. 85 (1878) 269) says that $p^\ell | n$ and $(p-1) \nmid n$, then $p^\ell | B_n$ where p is any odd prime $p > 3$. We conjecture that if $(p-1) \nmid n$, $p^\ell | n$ and $p^{\ell+1} \nmid n$ for any odd prime $p > 3$, then the exact power of p dividing B_n is either ℓ or $\ell + 1$. The main purpose of this article is to prove that this conjecture is equivalent to two other unproven hypotheses involving Bernoulli numbers and to provide a positive answer to this conjecture for infinitely many n.

Keywords: Bernoulli numbers; Class number of cyclotomic fields

1. Introduction

The nth Bernoulli number B_n in the even suffix notation defined by the recurrence relation

$$\sum_{i=1}^{n+1} \binom{n+1}{i} B_{n+1-i} = 0 \ \ (n \geqslant 1), \quad B_0 = 1.$$

Thus, we have $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$, and so on. It is easy to show that $(-1)^{i-1} B_{2i} > 0$ and $B_{2i+1} = 0$ for $i \geqslant 1$. Let us write $B_n = u_n / v_n$ where $u_n, v_n \in \mathbb{Z}$ and

*Fax: +91-532-266-7576.
E-mail address: thanga@mri.ernet.in.

0022-314X/$ - see front matter © 2004 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2003.12.006

$(u_n, v_n) = 1$. The von Staudt–Clausen theorem (see for instance [11, p. 56]) asserts that v_n is square-free and $p|v_n$ if and only if $(p-1)|n$. Therefore, $6|v_n$ for all positive integer $n \geqslant 2$.

By $p^a||n$ we mean that p^a divides n but p^{a+1} does not divide n.

In 1878, Adams [1] proved the following result regarding the divisibility properties of u_n. More precisely, he proved that if p is a prime such that $p^a||n$ for integer $a \geqslant 1$ and $(p-1) \nmid n$, then $p^a|u_n$.

Adam's classical result seems to be almost sharp.

Conjecture 0. *Let $p > 3$ be any prime number such that $p^\ell||n$ (here $\ell \geqslant 1$ is an integer) for some even positive integer n and $(p-1) \nmid n$. Then $p^\beta||u_n$ implies $\beta \leqslant \ell + 1$.*

Note that when $(p, n) = 1$, Conjecture 0 is false because if we take $p = 37$ and $n = 284$, we have $(37, 284) = 1$ and $37^2|B_{284}$.

Definition 1. An odd prime p is said to be an `irregular prime` if p divides one of numerators of the following Bernoulli numbers; $B_2, B_4, \ldots, B_{p-3}$. Otherwise, the prime p is said to be a `regular prime`.

For example, the first few irregular primes are 37, 59, 67, 101, 103, 131, 149, 157, ... It is known that there are infinitely many irregular primes (see [3,7]). But it is not known whether or not there are infinitely many regular primes, though numerical evidence suggests that about 60% of the primes are regular (see for instance [8, p. 109]).

The following theorem provides a positive answer to Conjecture 0 for infinitely many n's.

Theorem 1. *Let $p \geqslant 5$ be any prime. Let n be any positive even integer such that $p^\ell||n$ (for any positive integer $\ell \geqslant 1$) and $(p-1) \nmid n$. Then Conjecture 0 is true for n whenever p is a regular prime or p is an irregular prime and p less than 12 millions.*

2. Preliminaries

Kummer (see for instance [5]) proved the following congruence property of Bernoulli numbers (which is now, called Kummer congruence).

Kummer Congruence. *If m and n are positive integers such that $n \equiv m \pmod{p^r(p-1)}$ and m is non-zero modulo $p^r(p-1)$, then*

$$\frac{B_n}{n} \equiv \frac{B_m}{m} \pmod{p^{r+1}},$$

whenever $n \geqslant m \geqslant r+1$.

Now, it is easy to see from Kummer congruence that a prime p is irregular if and only if $p^2|B_{np}$ for some even integer $n\in[2,p-3]$.

Lemma 2.1. *Let n be any even positive integer. Let $p>3$ be any odd prime number such that $p^\ell||n$ and $(p-1)\nmid n$. Then*

$$\frac{u_n}{p^\ell}\equiv bu_c \pmod{p},$$

where b is a non-zero element modulo p and c is the least positive residue of n modulo $(p-1)$.

Proof. Result easily follows from Kummer congruence. □

Corollary 2.1.1. *Assume p, n and c as in Lemma* 2.1 *together with $p\nmid u_c$, then $p^\ell||u_n$. In particular, we have*

(i) *if p is regular, then $p||B_{np}$,*
(ii) *if p is irregular and $p\nmid B_n$, then $p||B_{np}$.*

Proof. The result is clear from Lemma 2.1. □

Theorem 2.2. (Sun [9]). *Let p be any odd prime and n be any even integer with $n\not\equiv 0 \pmod{p-1}$. Then*

$$\frac{B_{k(p-1)+n}}{k(p-1)+n}\equiv k\frac{B_{p-1+n}}{p-1+n}-(k-1)(1-p^{n-1})\frac{B_n}{n}\pmod{p^2}$$

for all integer $k\geqslant 1$.

Theorem 2.3. (Johnson [6]). *Let p be any irregular prime such that $p|B_n$ for some even integer $n\in[2,p-3]$. If*

$$\frac{B_{n+p-1}}{n+p-1}\not\equiv\frac{B_n}{n}\pmod{p^2},$$

then, there exists an integer $k\geqslant 2$ with $k\not\equiv n \pmod{p}$ and $(p,k(p-1)+n)=1$ such that

$$B_{k(p-1)+n}\equiv 0 \pmod{p^2}.$$

Theorem 2.4. *Let p be any odd prime. Let n be any even integer in $[2,p-3]$ such that $p|B_n$. Then if $p||\frac{B_{k(p-1)+n}}{k(p-1)+n}$ for some integer $k\geqslant 1$, then $p||B_n$.*

Proof. Assume that $p||\frac{B_{k(p-1)+n}}{k(p-1)+n}$ for some positive integer $k\geqslant 1$. We have to prove $p||B_n$.

Case (i): ($\frac{B_{n+p-1}}{n+p-1} \equiv \frac{B_n}{n} \pmod{p^2}$). Then by Theorem 2.2, for all integer $\ell \geqslant 1$, we get

$$\frac{B_{\ell(p-1)+n}}{\ell(p-1)+n} \equiv \ell \frac{B_{p-1+n}}{p-1+n} - (\ell-1)\frac{B_n}{n} \equiv \frac{B_n}{n} \pmod{p^2}.$$

In particular, when $\ell = k$ itself, then we get

$$\frac{B_{k(p-1)+n}}{k(p-1)+n} \equiv \frac{B_n}{n} \pmod{p^2}.$$

Since $p \| \frac{B_{k(p-1)+n}}{k(p-1)+n}$, we have $p \| B_n$.

Case (ii): ($\frac{B_{n+p-1}}{n+p-1} \not\equiv \frac{B_n}{n} \pmod{p^2}$). In this case, by Theorem 2.3, there exists an integer $m \not\equiv n \pmod{p}$ and $(m(p-1)+n, p) = 1$ such that

$$B_{m(p-1)+n} \equiv 0 \pmod{p^2} \Rightarrow \frac{B_{m(p-1)+n}}{m(p-1)+n} \equiv 0 \pmod{p^2}.$$

Therefore, by Theorem 2.2, we get

$$0 \equiv \frac{B_{m(p-1)+n}}{m(p-1)+n} \equiv m\frac{B_{n+p-1}}{n+p-1} - (m-1)\frac{B_n}{n} \pmod{p^2},$$

which implies

$$\frac{B_{n+p-1}}{n+p-1} \equiv \frac{m-1}{m}\frac{B_n}{n} \pmod{p^2}. \tag{1}$$

Thus, for every $\ell \geqslant 2$, we get,

$$\frac{B_{\ell(p-1)+n}}{\ell(p-1)+n} \equiv \ell \frac{B_{n+p-1}}{n+p-1} - (\ell-1)\frac{B_n}{n} \pmod{p^2}.$$

Therefore by Eq. (1), we get

$$\frac{B_{\ell(p-1)+n}}{\ell(p-1)+n} \equiv \frac{\ell(m-1)-(\ell-1)m}{m}\frac{B_n}{n} \equiv \frac{m-\ell}{m}\frac{B_n}{n} \pmod{p^2}. \tag{2}$$

Put $\ell = k$ in the above, we get

$$\frac{B_{k(p-1)+n}}{k(p-1)+n} \equiv \frac{m-k}{m}\frac{B_n}{n} \pmod{p^2}.$$

By our assumption, we know that $p \| \frac{B_{k(p-1)+n}}{k(p-1)+n}$ and hence $(m-k)/n$ and B_n/n are not congruent to 0 modulo p^2. Since $n < p-2$, we see that $p^2 \nmid B_n$. □

Theorem 2.5. *The following statements are equivalent*:

(i) *Conjecture* 0;

(ii) $B_{np} \not\equiv 0 \pmod{p^3}$ *for every even integer* $n \in \{2, 4, \ldots, p-3\}$;
(iii) $B_n \not\equiv 0 \pmod{p^2}$ *for every even integer* $n \in \{2, 4, \ldots, p-3\}$.

Proof. First, we shall prove that (i) $\Leftrightarrow$ (ii).

That is, assume that Conjecture 0 is true. We have to prove that (ii) is also true. Because of Corollary 2.1.1, it is enough to assume that p is an irregular prime such that $p|B_n$ for some even integer $n \in [2, p-3]$. Since $p|B_n$, we have $0 \not\equiv np \equiv n \pmod{p-1}$. Therefore, by Conjecture 0, we know that $p^\ell || B_{np}$ implies $\ell \leqslant 2$. Since p is irregular, we know that $p^2 | B_{np}$ and hence $p^2 || B_{np}$. Thus, the statement (ii) is true.

Assume that statement (ii) is true. We shall prove the conjecture 0 is true.

First, let us observe the following: if p is any irregular prime such that $p|B_n$ for some even integer $n \in [2, p-3]$, then for any integer $\ell \geqslant 1$, we have $p^{\ell+1} || B_{np^\ell}$ if and only if $p^2 || B_{np}$. One way is obvious by letting $\ell = 1$. To prove the other implication, assume that $p^2 || B_{np}$. That is, when $\ell = 1$ the result is true. Assume that the result is true for all $m \leqslant \ell$. We shall prove for $\ell + 1$. Now, by Kummer congruence and $\ell \geqslant 1$, we have

$$\frac{B_{np^{\ell+1}}}{np^{\ell+1}} = \frac{B_{np^\ell(p-1)+np^\ell}}{np^{\ell+1}} \equiv \frac{B_{np^\ell}}{np^\ell} \pmod{p^2}.$$

By induction, we know that $p^{\ell+1} || B_{np^\ell}$ and hence $p^2 \nmid \frac{B_{np^\ell}}{np^\ell}$. Therefore, we get, $p^{\ell+2} || B_{np^{\ell+1}}$. Thus, we have, $p^2 || B_{np} \Leftrightarrow p^{\ell+1} || B_{np^\ell}$ for every integer $\ell \geqslant 1$.

Let $n = kp^\ell$ be an even positive integer such that $p^\ell || n$ and $(p-1) \nmid n$. By Adams' result, we know that $p^\ell | B_n$. To prove Conjecture 0, it is to prove $p^\beta || B_n$ implies $\beta \leqslant \ell + 1$. Since $(p-1) \nmid n$, it is clear that $n \equiv k \not\equiv 0 \pmod{p-1}$. If $k \in [2, p-3]$, then by the assumption and by the above observation, we have $p^\ell || B_{kp^\ell}$ or $p^{\ell+1} || B_{kp^\ell}$ depending on $p \nmid B_k$ or $p | B_k$ (by Corollary 2.1.1). Suppose $k > p-1$. Then, $k = r(p-1) + c$ for some positive integers r and c with $c \in [2, p-3]$ an even integer. Therefore, by Kummer congruence, we have

$$\frac{B_n}{kp^\ell} = \frac{B_{(r(p-1)+c)p^\ell}}{kp^\ell} = \frac{B_{rp^\ell(p-1)+cp^\ell}}{kp^\ell} \equiv \frac{B_{cp^\ell}}{cp^\ell} \pmod{p^2}.$$

We see from the above observation that $p^2 \nmid \frac{B_{cp^\ell}}{cp^\ell}$ because statement (ii) is true by our assumption. Therefore, $p^\beta || B_n$ implies $\beta \leqslant \ell + 1$. Thus, Conjecture 0 is true.

Now, we shall prove that (ii) $\Leftrightarrow$ (iii). Assume that statement (ii) is true. That is, $p || \frac{B_{np}}{np}$. Since $np = n(p-1) + n$, by Theorem 2.4, we see that statement (iii) is true. For the other implication, let us assume that statement (iii) is true. In case (i) of Theorem 2.4, we have clearly $p || \frac{B_{np}}{np}$. In case (ii) by Eq. (2) we have

$$\frac{B_{np}}{np} \equiv \frac{m-n}{m} \frac{B_n}{n} \pmod{p^2}.$$

Since $m \not\equiv n \pmod{p}$ (by Theorem 2.3) and $p || \frac{B_n}{n}$, we get the result. $\square$

3. Proof of Theorem 1

Let n be any even integer such that $p^{\ell}||n$ and $(p-1)\nmid n$. Let $n=p^{\ell}k$ where $(p,k)=1$. If p is regular, then by Lemma 2.1, it is clear that $p^{\ell}||B_n$. Suppose p is an irregular prime and p is less than 12 millions. In [2], they have verified that

$$B_m \not\equiv 0 \pmod{p^2} \text{ for all } m \in \{2,4,\ldots,p-3\}$$

is true for all irregular primes upto 12 millions. Therefore, for these primes by Theorem 2.5, we know that

$$B_{mp} \not\equiv 0 \pmod{p^3} \text{ for all } m \in \{2,4,\ldots,p-3\}.$$

This implies, for any integer $\ell \geqslant 1$,

$$B_{mp^{\ell}} \not\equiv 0 \pmod{p^{\ell+2}} \text{ for all } m \in \{2,4,\ldots,p-3\}$$

by the observation in first part of Theorem 2.5. If $k<p-1$, then it follows that $p^{\beta}||B_n$ implies $\beta \leqslant \ell+1$. As $(p-1)\nmid n$, it is clear that $(p-1)\nmid k$. If $k>p-1$, then let $k=r(p-1)+c$ where c is an even integer such that $c \in \{2,4,\ldots,p-3\}$. Then, by Kummer congruence, we get

$$\frac{B_{kp^{\ell}}}{n} \equiv \frac{B_{r(p-1)p^{\ell}+cp^{\ell}}}{n} \equiv \frac{B_{cp^{\ell}}}{cp^{\ell}} \pmod{p^2}.$$

Since $c<p-1$ and by the above observation, we see that $p^{\ell+2}\nmid B_{cp^{\ell}}$ and hence $p^{\ell+2}\nmid B_n$. This implies $\beta \leqslant \ell+1$.

4. Connections with cyclotomic fields

The main reference for this section is [11]. Let p be any odd prime. Let $\mathbb{Q}(\zeta_p)$ be the cyclotomic field generated by ζ_p a primitive pth root of unity. Then $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ is its maximal real subfield. Let h be the class number of $\mathbb{Q}(\zeta_p)$ and $h=h^+h^-$ where h^+ is the class number of $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ and h^- is called the relative class number. In fact,

$$h^- = 2p \prod_{j=1, j \text{ odd}}^{p-2} \left(-\frac{1}{2}B_{1,\omega^j}\right), \tag{3}$$

where B_{1,ω^j} is the first generalized Bernoulli number attached to ω^j (here ω^j is any odd character attached to $\mathbb{Q}(\zeta_p)$) and ω is a Teichmüller character modulo p. Note that $B_{1,\omega^{p-2}} \equiv \frac{p-1}{p} \pmod{\mathbb{Z}_p}$ where $\mathbb{Z}_p$ is the ring of p-adic integers. Thus, $pB_{1,\omega^{p-2}}$ has no p-factor in it.

Proposition 4.1. *Let p be any irregular prime. Let n be any even integer in $\{4, 6, \ldots, p-3\}$. Then,*

$$B_{1,\omega^{n-1}} \equiv \frac{B_{(n-1)(p-1)+n}}{(n-1)(p-1)+n} \pmod{p^2}.$$

Proof. Ernvall and Metsänkylä [4] proved the following results. For all $n \in \{4, 6, \cdots, p-3\}$, we have

$$\frac{B_{p-1+n}}{p-1+n} - \frac{B_n}{n} \equiv -\frac{1}{2} p \sum_{a=1}^{p-1} a^n q_a^2 \pmod{p^2}, \tag{4}$$

where $q_a = (a^{p-1}-1)/p$ is the Fermat quotient of a. Also, in the same paper, they proved that for all $n \in \{4, 6, \cdots, p-3\}$,

$$B_{1,\omega^{n-1}} \equiv \frac{B_n}{n} - \frac{n-1}{2} p \sum_{a=1}^{p-1} a^n q_a^2 \pmod{p^2}. \tag{5}$$

Therefore, from the Eqs. (4) and (5), we get

$$\begin{aligned} B_{1,\omega^{n-1}} &\equiv \frac{B_n}{n} - \frac{n-1}{2} 2\left(\frac{B_n}{n} - \frac{B_{p-1+n}}{p-1+n}\right) \pmod{p^2}. \\ &\equiv (n-1)\frac{B_{n+p-1}}{n+p-1} - (n-2)\frac{B_n}{n} \pmod{p^2} \\ &\equiv \frac{B_{(n-1)(p-1)+n}}{(n-1)(p-1)+n} \pmod{p^2}, \end{aligned}$$

since $n \geqslant 4$, we can apply Theorem 2.2 to get the last congruence. □

Corollary 4.1.1. *Let p be any irregular prime. Let n be any even integer such that $n \in \{4, 6, \cdots, p-3\}$. Then*

$$B_{1,\omega^{n-1}} \equiv \frac{B_n}{n} \pmod{p}.$$

Proof. The result follows from Theorem 4.1 and Kummer congruence. □

Also it is known that $B_{1,\omega} \equiv \frac{B_2}{2} \pmod{p}$. Since $u_n = \pm 1$ for all $n = 2, 4, 6, 8, 10$, we can assume that $n \geqslant 12$ for the rest of the article. Also, we denote the number of even integers n's such that $2 \leqslant n \leqslant p-3$ and $p | B_n$ by $I(p)$. This number $I(p)$ is called the *index of irregularity*. Because of Corollary 4.1.1 and from the formula of h^-, we see that

$$\operatorname{ord}_p(h^-) = \operatorname{ord}_p\left(\prod_{i=11,\ j \text{ odd}}^{p-4} B_{1,\omega^j}\right)$$

and we have $\mathrm{ord}_p(h^-) \geqslant I(p)$. If one proves $B_{1,\omega^j} \not\equiv 0 \pmod{p^2}$ for all $j = 1, 3, \cdots, p-4$, then we have $\mathrm{ord}_p(h^-) = I(p)$. Here $\mathrm{ord}_p(a)$ is the exponent of p in the canonical decomposition of a.

Theorem 4.2. *Let n be any even integer such that $n \in [2, p-3]$. We have*

$$B_{1,\omega^{n-1}} \not\equiv 0 \pmod{p^2} \Rightarrow B_n \not\equiv 0 \pmod{p^2}.$$

Proof. Let n be any even integer such that $12 \leqslant n \leqslant p-3$. Assume that $B_{1,\omega^{n-1}} \not\equiv 0 \pmod{p^2}$. We have to prove $B_n \not\equiv 0 \pmod{p^2}$. By Theorem 4.1, we know that

$$B_{1,\omega^{n-1}} \equiv \frac{B_{(n-1)(p-1)+n}}{(n-1)(p-1)+n} \pmod{p^2}.$$

Therefore, by the assumption, we have $p^2 \nmid \frac{B_{(n-1)(p-1)+n}}{(n-1)(p-1)+n}$. Therefore, by Theorem 2.4, we get the result. □

Also, note that $p^3 \nmid B_{np} \Leftrightarrow \mathrm{ord}_p(L_p(1, \omega^n)) \leqslant 1$ where L_p is the p-adic L-function (See [11, p. 162]). Thus, to prove Conjecture 0, $p^3 \nmid B_{np}$ and $p^2 \nmid B_n$ for every even integer $n \in [2, p-3]$, it is enough to prove

$$B_{1,\omega^{n-1}} \not\equiv 0 \pmod{p^2}$$

for all even integer $n \in [2, p-3]$.

These hypotheses play very crucial role in the arithmetic of cyclotomic fields including Fermat last theorem. Also, Bernoulli numbers have numerous applications. For instance, as referee pointed out, in [10], they use these numbers to obtain tight estimations on some apriori infeasible calculation.

Acknowledgments

I am grateful to Professor M. Ram Murty for introducing me to this area of Mathematics. I am also thankful to the referee for his/her useful suggestions.

References

[1] J.C. Adams, Tables of the values of the first 62 numbers of Bernoulli, J. Reine Angew. Math. 85 (1878) 269–272.
[2] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä, M.A. Shokrollahi, Irregular primes and cyclotomic invariants to 12 million, J. Symbolic Comput. 31 (2001) 89–96.
[3] L. Carlitz, Note on irregular primes, Proc. Amer. Math. Soc. 5 (1954) 329–331.
[4] R. Ernvall, T. Metsänkylä, Cyclotomic invariants for primes between 125 000 and 150 000, Math. Comp. 56 (194) (1991) 851–858.

[5] http://www.dms.umontreal.ca/andrew/Binomial/bernoulli.html
[6] W. Johnson, Irregular prime divisors of the Bernoulli numbers, Math. Comp. 28 (126) (1974) 653–657.
[7] T. Metsänkylä, Distribution of irregular prime numbers, J. Reine Angew. Math. 282 (1976) 126–130.
[8] P. Ribenboim, 13 Lectures on Fermat's Last Theorem, Springer, New York, Heidelberg, 1979.
[9] Z.H. Sun, Congruences concerning Bernoulli numbers and Bernoulli polynomials, Discrete Appl. Math. 105 (2000) 193–223.
[10] B. Tsaban, Bernoulli numbers and the probability of a birthday surprise, Discrete Appl. Math. 127 (2003) 657–663.
[11] L.C. Washington, Introduction to Cyclotomic Fields, in: Graduate Text in Mathematics, Vol. 83, Springer, New York, 1997.