EXPOSITIONES MATHEMATICAE

Expo. Math. 21 (2003): 75–82

www.urbanfischer.de/journals/expomath

Mathematical Note

A Note on Certain Divisibility Properties of the Fourier Coefficients of Normalized Eisenstein Series

B. Ramakrishnan[1] and R. Thangadurai[2]

[1] Harish-Chandra Research Institute, Chhatnag Road, Jhusi, Allahabad 211 019, India
[2] Stat-Math Division, Indian Statistical Institute, 203, B. T. Road, Kolkata 700 108, India

Abstract: In this note, we shall prove certain divisibility properties of the Fourier coefficients of a class of normalized Eisenstein series modulo certain prime powers.

Keywords: Divisibility property, Fourier coefficients, Divisor Sigma function.

1. Introduction

First we shall fix up the following notations. Throughout this article $\left(\frac{\cdot}{p}\right)$ denotes the Legendre symbol modulo a prime p. For an integer r, the elementary divisor function $\sigma_r(n)$ is defined as $\sigma_r(n) := \sum_{d|n} d^r$. Also, $\phi(n)$ denotes the Euler function which counts the number of positive integers up to n and relatively prime to n.

The normalized Eisenstein series $E_{2k}(z)$ is a modular form of weight $2k$ for the full modular group $SL_2(\mathbf{Z})$ and it is given by the Fourier expansion

$$E_{2k}(z) = 1 - \frac{4k}{B_{2k}} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n,$$

where B_{2k} is the $2k$-th Bernoulli number, $q = \exp(2\pi i z)$ and z is in the upper half plane of the complex plane. Hence, if we write

$$E_{2k}(z) = \sum_{n=0}^{\infty} e_{2k}(n) q^n,$$

2000 AMS Subject Classifications, Primary: 11A25, Secondary: 11A07, 11F30.
E-mail addresses: [1]ramki@mri.ernet.in, [2]thanga_v@isical.ac.in

0732-0869/03/21/1-75 $15.00/0

then, from the definition, it is clear that

$$e_{2k}(n) = -\frac{4k}{B_{2k}}\sigma_{2k-1}(n),$$

whenever $n \geq 1$ and $e_{2k}(0) = 1$. We shall prove the following theorems.

Theorem 1. *For a positive integer k, let $p \equiv 3 \pmod 4$ be a prime such that $2k - 1 = (2r+1)\frac{\phi(p^a)}{2}$, for some integers $a \geq 1$ and $r \geq 0$. Then we have*

$$e_{2k}(n) \equiv 0 \pmod{24p^a} \ \forall\ n \text{ satisfying } \left(\frac{n}{p}\right) = -1.$$

Note 1. The above theorem is true for $p = 3$; $a = 1$. Moreover, if $k \equiv 2 \pmod 3$, then the result is valid for $p = 3; a = 2$ and $p = 7; a = 1$.

Corollary 1. *For a given integer $k \geq 1$, let $p_1 > p_2 > \cdots > p_\ell > 3$ be prime numbers of the form $4m - 1$ and let $r_i \geq 0$, $a_i \geq 0$ be integers, $i = 1, 2, \cdots, \ell$ such that*

$$(2r_i + 1)\frac{\phi(p_i^{a_i})}{2} = 2k - 1, i = 1, 2, \cdots, \ell.$$

Then

$$e_{2k}(n) \equiv 0 \pmod{24P}$$

for all n satisfying

$$\left(\frac{n}{p_i}\right) = -1, \quad i = 1, 2, \cdots, \ell,$$

where $P = \prod_{i=1}^{\ell} p_i^{a_i}$.

Example 1. Let $k = 8$. Then $2k - 1 = 15$. Now, we can choose $p_1 = 31$, $p_2 = 11$ and $p_3 = 7$, $a_1 = a_2 = a_3 = 1$, and $r_1 = 0, r_2 = 1, r_3 = 2$ to get,

$$(2r_1 + 1)\frac{p_1 - 1}{2} = (2r_2 + 1)\frac{p_2 - 1}{2} = (2r_3 + 1)\frac{p_3 - 1}{2} = 15.$$

Now -1 is a quadratic non-residue modulo $7, 11, 31$. Then, Corollary 1 says that

$$e_{15}(2387n - 1) \equiv 0 \pmod{57288} \ \forall\ n \in \mathbf{N}.$$

We need the following notations for further results.

For a fixed prime number p, we define a positive integer $n_p > 1$ as follows. The integer n_p has at least one prime divisor q such that $q \equiv -1 \pmod p$ and $q^r \| n_p \implies r$ is odd. Moreover we write n_p as $n_p = k\prod_{i=1}^{s} q_i^{r_i}$ where $q_i \equiv -1 \pmod p$ are primes and $(k, q_i) = 1$ for every $i = 1, 2, \cdots, s$ and r_i's are odd positive integers.

(Here $p^a \| m$, means that $p^a \mid m$ and $p^{a+1} \nmid m$.) For example, n_2 can be any one of the following integers $3, 5, 6, 7, 10, 11, 12, 13, 14, \cdots$. Obviously, for a fixed prime p, we have infinitely many n_p.

Definition 1. A prime p is said to be regular if p does not divide any of the numerators of the following Bernoulli numbers;

$$B_2, B_4, \cdots, B_{p-3}.$$

For example, any odd prime $p \leq 29$ is a regular prime. The first non-regular prime is 31. It is not known whether there are infinitely many such primes or not.

Theorem 2. *Let k be any positive even integer. Let $p > 3$ be a prime number such that either $(p-1)|k$ or*

$$p > f(k) = 2\frac{k!}{(2\pi)^k} \frac{1}{1 - 2^{\beta - k}},$$

where $\beta = (2 + \log(1 - (6/\pi^2))/\log 2$. If n_p has s number of prime factors q such that $q \equiv -1 \pmod{p}$ and $q^r \| n_p$ where r is odd, then

$$e_k(n_p) \equiv \begin{cases} 0 \pmod{24p^{s+1}} & \text{if } (p-1)|k \\ 0 \pmod{24p^s} & \text{if } p > f(k) \end{cases}.$$

Theorem 3. *Let k be any positive even integer. Let $p = 2$ or 3. If n_p has s number of prime factors q such that $q \equiv -1 \pmod{p}$ with $q^r \| n_p$, r odd, then*

$$e_k(n_p) \equiv 0 \pmod{24p^s}.$$

Corollary 2. *Let k be a positive even integer and let $p > 3$ be any regular prime. If n_p has s number of prime factors q such that $q \equiv -1 \pmod{p}$ with $q^r \| n_p$, r odd, and $p \nmid k$, then*

$$e_k(n_p) \equiv 0 \pmod{24p^s},$$

2. Preliminaries

In 1945, K. G. Ramanathan [Kgr2] (see also [Kgr1]) proved the following congruence, namely,

$$\sigma_{\frac{p-1}{2}}(n) \equiv 0 \pmod{p},$$

if n is a quadratic non-residue modulo any odd prime p. This can be seen as follows: First note that $\sigma_{p-1+m}(n) \equiv \sigma_m(n) \pmod{p}$. Now,

$$\sigma_{\frac{p-1}{2}}(n) = \sum_{d|n} d^{\frac{p-1}{2}} = n^{\frac{p-1}{2}} \sum_{d|n} (d/n)^{\frac{p-1}{2}} = n^{\frac{p-1}{2}} \sigma_{-\frac{p-1}{2}}(n)$$

$$\equiv \left(\frac{n}{p}\right)\sigma_{p-1-\frac{p-1}{2}}(n) = \left(\frac{n}{p}\right)\sigma_{\frac{p-1}{2}}(n) \pmod{p}.$$

Thus Ramanathan's result follows at once. Furthermore, it was generalized by D. B. Lahiri [Lah1] as follows:

Theorem 4. (D. B. Lahiri, [Lah1]) *For an odd prime p and an integer $a \geq 1$, let $m = \frac{1}{2}\phi(p^a) = \frac{1}{2}(p-1)p^{a-1}$, and let n be a quadratic non-residue modulo p. Then*

$$\sigma_m(n) \equiv 0 \pmod{p^a}.$$

Since for any integer $k \geq 0$ and a prime p, we have

$$\sigma_{k\phi(p^a)+m}(n) = \sum_{d|n} d^{k\phi(p^a)+m} \equiv \sum_{d|n} d^m = \sigma_m(n) \pmod{p^a},$$

by Euler's theorem, we obtain, using Theorem 4, the following more general theorem.

Theorem 5. *If p is an odd prime, $a \geq 1$, and n is a quadratic non-residue modulo p, then*

$$\sigma_{(2k+1)\frac{\phi(p^a)}{2}}(n) \equiv 0 \pmod{p^a}$$

for any integer $k \geq 0$. In particular, it is true that

$$\sigma_{(2k+1)\frac{p-1}{2}}(pn-1) \equiv 0 \pmod{p} \quad \forall\, n \in \mathbf{N}$$

for every prime $p \equiv 3 \pmod 4$.

Using Chinese remainder theorem and Theorem 4, we obtain the following corollary.

Corollary 3. *Let $p_1 > p_2 > \cdots > p_r$ be odd prime numbers, which are of the form $4\ell - 1$. For $i = 1, 2, \cdots, r$, let $k_i \geq 0$ and $a_i \geq 0$ be integers such that*

$$(2k_1+1)\frac{\phi(p_1^{a_1})}{2} = (2k_2+1)\frac{\phi(p_2^{a_2})}{2} = \cdots = (2k_r+1)\frac{\phi(p_r^{a_r})}{2} = t \quad (say).$$

Then

$$\sigma_t(n) \equiv 0 \pmod{P}$$

for all n satisfying

$$\left(\frac{n}{p_1}\right) = \left(\frac{n}{p_2}\right) = \cdots = \left(\frac{n}{p_r}\right) = -1,$$

where $P = \prod_{i=1}^{r} p_i^{a_i}$.

Theorem 6. *Let p be any prime number. Let n_p has s number of prime divisors q_j such that $q_j^{2\ell_j+1} \| n_p$ and $q_j \equiv -1 \pmod{p}$ for every $j = 1, 2, \cdots, s$. Then for any odd positive integer m we have*

$$\sigma_m(n_p) \equiv 0 \pmod{p^s}.$$

Proof. Let q be a prime divisor of n_p such that $q \equiv -1 \pmod{p}$ and $q^{2\ell+1} \| n_p$ for some $\ell \geq 0$. Let $n_p = kq^{2\ell+1}$, with $(k, q) = 1$. Since $\sigma_m(n)$ is a multiplicative function, we have

$$\sigma_m(n_p) = \sigma_m(k)\sigma_m(q^{2\ell+1}).$$

Now, consider

$$\sigma_m(q^{2\ell+1}) = 1 + q^m + q^{2m} + \cdots + q^{m(2\ell+1)}.$$

Since $q \equiv -1 \pmod{p}$, we have $q^{2k} \equiv 1 \pmod{p}$ and $q^{2k+1} \equiv -1 \pmod{p}$. Since m is odd, we see that

$$\sigma_m(q^{2\ell+1}) \equiv 1 - 1 + 1 - 1 + \cdots + 1 - 1 \equiv 0 \pmod{p}$$

and hence $\sigma_m(n_p) \equiv 0 \pmod{p}$. Since there are s number of such factors in n_p, the result now follows. □

Before going to the proofs of Theorems 1 and 2, we shall recall some properties of the Bernoulli numbers. The Bernoulli numbers, denoted by B_k, are rational numbers which are obtained by the following generating function.

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} \frac{B_k t^k}{k!}.$$

Since

$$\frac{t}{2} + \sum_{k=0}^{\infty} \frac{B_k t^k}{k!} = \frac{t}{2} + \frac{t}{e^t - 1} = \frac{t(e^t + 1)}{2(e^t - 1)}$$

and the right hand side is an even function of t, we deduce that $B_k = 0$ for odd integer $k \geq 3$. Since B_k are rational numbers, we write $B_k = \frac{u_k}{v_k}$ where u_k, v_k are integers such that $(u_k, v_k) = 1$. The denominators v_k are well understood.

Theorem 7 (von Staudt - Clausen (see [How1], [Joh1])). *For $k \geq 1$, v_{2k} is square free and a prime p divides v_{2k} if and only if $p - 1$ divides $2k$. In particular, 6 divides v_{2k} for every $k \geq 1$.*

Kummer first proved the following periodicity property of these Bernoulli numbers.

Theorem 8. (Kummer, [Kum1]) *Let $p \geq 5$ be a prime. If $n \not\equiv 0 \pmod{p-1}$ and $n \equiv m \pmod{p-1}$, then*

$$\frac{B_n}{n} \equiv \frac{B_m}{m} \pmod{p}.$$

The following theorem is well known in the literature (see for instance ([Joh1], p.257)); but proof is not included in many standard text books. Since this theorem is crucial for our discussion, for the sake of completeness, we give a proof.

Theorem 9. *Let $p > 3$ be a prime number of the form $4k - 1$ for some integer $k \geq 1$. Then p does not divide B_{2k}.*

Proof. Using some well-known properties of Bernoulli polynomials, it can be proved that for any prime $p > 3$ and for any even integer $n \geq 2$, we have

$$\sum_{a=1}^{(p-1)/2} a^{n-1} \equiv -\left(2 - \frac{1}{2^{n-1}}\right)\frac{B_n}{n} \pmod{p}.$$

In particular, if

$$\sum_{a=1}^{(p-1)/2} a^{n-1} \not\equiv 0 \pmod{p}, \quad \text{then} \quad p \not| B_n.$$

In our case, $p = 4k - 1$ and hence $(p-1)/2 = 2k - 1$. Take $n = 2k$. To end the proof, it enough to prove that

$$\sum_{a=1}^{2k-1} a^{2k-1} \not\equiv 0 \pmod{p}.$$

Now consider

$$\sum_{a=1}^{(p-1)/2} a^{2k-1} \equiv \sum_{a=1}^{(p-1)/2} a^{\frac{p-1}{2}} \equiv \sum_{a=1}^{2k-1} \left(\frac{a}{p}\right) \not\equiv 0 \pmod{p}$$

as Legendre symbols takes ± 1 and odd number of summands involving them. □

Conjecture 1. (S. Chowla and P. Chowla, [CC1]) *Let p be a prime number of the form $2^m k - 1$ for any integer $m > 1$ and $k \geq 1$. Then p does not divide B_{2k}.*

Note 2. Here, we have not stated the full version of Conjecture 1 (see [CC1] for the full version). For our purpose, this version suffices.

3. Proofs

Proof of Theorem 1. Let $p \neq 3$. Then,

$$2k = (2r+1)\frac{\phi(p^a)}{2} + 1 \equiv r\phi(p^a) + \frac{\phi(p^a)}{2} + 1 \equiv \frac{p+1}{2} \pmod{p-1}$$

as $\phi(p^a) = p^{a-1}(p-1)$ and $p^a \equiv 1 \pmod{p-1}$. Now, by Theorem 8, we get,

$$\frac{B_{2k}}{2k} \equiv \frac{B_{(p+1)/2}}{(p+1)/2} \pmod{p}.$$

Since, by Theorem 9, we know that $B_{(p+1)/2} \not\equiv 0 \pmod{p}$, it follows that $B_{2k} \not\equiv 0 \pmod{p}$. Also, p cannot divide the denominator of B_{2k}, since $2k \equiv (p+1)/2 \pmod{p-1}$ and by Theorem 7. But, 6 always divides the denominator of B_{2k} which follows again by Theorem 7. Hence 24 always divides $e_{2k}(n)$ for any n. Thus, the factor of p in $e_{2k}(n)$ comes from $\sigma_{2k-1}(n)$ alone for any n. From the expression of $2k-1$ and Theorem 5, it follows that p^a divides $\sigma_{2k-1}(n)$ whenever n is a quadratic non-residue modulo p. Hence p^a divides $e_{2k}(n)$ whenever n is a quadratic non-residue modulo p, which completes the proof in this case.

Now we consider the case $p = 3$. In this case, we have

$$2k - 1 = (2r+1)3^{a-1},$$

for some integers r and a. Now, by Theorem 7, it follows that 6 divides the denominator of B_{2k}. Hence 24 divides $e_{2k}(n)$ for any n. Since -1 is the only quadratic non-residue modulo 3, by Theorem 5, we get $\sigma_{2k-1}(3n-1) \equiv 0 \pmod{3^a}$ for every n. By putting together all these information, we get $e_{2k}(3n-1)0 \equiv 0 \pmod{24 \cdot 3^a}$. This completes the proof. □

Proof of Corollary 1. This follows easily from Theorem 1 and Corollary 3. □

Remark 1. In our proof of Theorem 1, the crucial result we used is Theorem 9. So, if we assume Conjecture 1, then we can extend the same divisibility conditions to many different moduli p. More precisely, we obtain similar divisibility results as in Theorem 1 for $e_{2k}(n)$ for prime moduli p, which are of the form $2^m\ell - 1$.

Proof of Theorem 2. Given that k is an even positive integer. In 2000, H. Alzer [Alz1] gave a tight upper bound for Bernoulli numbers as follows.

$$|B_k| \leq 2\frac{k!}{(2\pi)^k}\,\frac{1}{1-2^{\beta-k}},$$

where $\beta = (2 + \log(1 - (6/\pi^2))/\log 2$. If the prime p is such that $(p-1)|k$, then by Theorem 7, we know that p divides the denominator of B_k and hence it cannot appear in the numerator of B_k. That is, a p-factor appears in $2k/B_k$. Also, by Theorem 6, we have $\sigma_{k-1}(n_p) \equiv 0 \pmod{p^s}$. Therefore, in this case, $e_k(n_p) \equiv 0 \pmod{24p^{s+1}}$. If the prime p is such that $(p-1) \not| k$, then, by assumption, p is bigger than the Alzer's bound. Therefore, p cannot divide B_k. Thus, by Theorem 6, it follows that $e_k(n_p) \equiv 0 \pmod{24p^s}$. Note that the factor 24 appears in the moduli because of the fact that 6 divides all the Bernoulli numbers $k \geq 2$ and a factor of 4 is already there. □.

Proof of Theorem 3. Let $p = 2$ or 3. Then by Theorem 7, we see that p divides the denominator of B_k for any even integer k and hence p never divides the numerator of B_k. Now, we proceed as the proof of Theorem 2 to get the result. □

Proof of Corollary 2. By Theorem 2, we can assume that $(p-1) \not| k$. Therefore, p doesn't divide the denominator of B_k (by Theorem 7). Let $\ell \equiv k \pmod{p-1}$ be such that $2 \leq \ell \leq p-3$. By assumption, we have $p \not| k$. Also by Definition 1, it is clear that p doesn't divide any of the numerators of $B_2, B_3, \cdots, B_{p-3}$. If possible, let p divide B_k; i.e., p divides the numerator of B_k. Then by Theorem 8, we know that

$$0 \equiv \frac{B_k}{k} \equiv \frac{B_\ell}{\ell} \pmod{p}.$$

Note that as $(k,p) = 1$, the p factor of B_k doesn't get cancelled with k. Also, since $\ell < p$ and p divides $\frac{B_\ell}{\ell}$, we see that p divides B_ℓ. This contradicts the fact that p is a regular prime. Now proceeding as in the proof of Theorem 2, we arrive at the required congruence. □

References

[Alz1] H. Alzer, Sharp bounds for the Bernoulli numbers, *Arch. Math (Basel)*, **74** (2000), no. 3, 207-211.

[Ber1] J. Bernoulli, *Ars Conjectandi*, Bâle. (1713).

[CC1] P. Chowla and S. Chowla, On Bernoulli numbers – II, *J. Number Theory*, **14** (1982), 65-66.

[How1] F. T. Howard, Applications of a recurrence for the Bernoulli numbers, *J. Number Theory*, **52** (1995), no. 1 157-172.

[Joh1] W. Johnson, p-adic proofs of congruences for the Bernoulli numbers, *J. Number Theory*, **7** (1975), 251-265.

[Kum1] E. E. Kummer, Bestimmung der Anzahl nicht äquivalenter Classen fur die aus λten Wurzel der Einheit gebildeten complexen Zahlen und die Idealen Factoren derselben, *J. reine u. angew. Math.*, **40**, (1850) 117-129.

[Lah1] D. B. Lahiri, Some congruences for the elementary divisor functions, *Amer. Math. Monthly*, **76** (1969), 395–397.

[Kgr1] K. G. Ramanathan, Congruence properties of $\sigma(n)$, the sum of the divisors of n, *Math. Student*, No. 1 and 2, Vol XI (1943), 33-35.

[Kgr2] K. G. Ramanathan, Congruence properties of Ramanujan's function $\tau(n)$ II, *J. Indian Math. Soc.*, **9** (1945), 55–59.

Received: 26. 06. 2002
Revised: 23. 09. 2002