Hokkaido Mathematical Journal Vol. 8 (1979) p. 239-243

Some congruence properties of Eisenstein series

By Shōyū NAGAOKA

(Received February 21, 1979)

§ 1. Introduction.

Let $\Psi_{k}^{(g)}$ be the normalized Eisenstein series of weight k and degree g. Let p be a prime number different from 2 and 3 (we assume this throughout this paper.). Then it is known that $\Psi_{k}^{(1)}$ satisfies the following congruence:

$$\Psi_{p-1}^{(1)} \equiv 1 \pmod{p} .$$

This fact was used by H. P. F. Swinnerton-Dyer in [9] to determine the structure of the ring of mod p modular forms, and was also used by J.-P. Serre in [5] to develop the theory of p-adic modular forms.

We denote by B_m the m-th Bernoulli number. In the previous paper [4], the author showed that $\Psi_{p-1}^{(2)} \equiv 1 \pmod{p}$ for all prime number p satisfying $B_{p-3} \not\equiv 0 \pmod{p}$, generalized the concept of the algebra of mod p modular forms to the case of Siegel modular forms and determined its structure.

In this note we shall show the following theorem.

THEOREM. *There exists a prime number p satisfying*

$$\Psi_{p-1}^{(g)} \not\equiv 1 \pmod{p} .$$

§ 2. On the Fourier coefficients of the Eisenstein series.

Let $\Psi_{k}^{(g)}(Z)$ be the normalized Eisenstein series of weight k and degree g. Then $\Psi_{k}^{(g)}(Z)$ has the Fourier expansion of the form

$$\Psi_{k}^{(g)}(Z) = \sum_{T \geqq 0} a_k(T) \exp\left\{2\pi i tr(TZ)\right\} ,$$

where the sum runs over all half integral positive semi-definite symmetric matrices T.

C. L. Siegel proved in [6] that all Fourier coefficients of $\Psi_{k}^{(g)}$ are rational numbers. Furthermore he proved in [8] that for each fixed k, the rational numbers $a_k(T)$ have bounded denominators, the common denominator being a product of a power of 2 and of the numerators of certain Bernoulli numbers. In the case of degree 2, H. Maass gave in [3] an explicit formula of Fourier coefficient $a_k(T)$ of Eisenstein series $\Psi_{k}^{(2)}$. In particular,

$$(1)\qquad \begin{cases} a_k\left(\begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}\right) = -\dfrac{4k\cdot B_{k-1,\left(\frac{-3}{*}\right)}}{B_k\cdot B_{2k-2}} \\ a_k\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = -\dfrac{4k\cdot B_{k-1,\left(\frac{-4}{*}\right)}}{B_k\cdot B_{2k-2}} \end{cases} .$$

The numerical tables (1) and (2) can be obtained from the formulae (1).

§ 3. Some properties of the generalized Bernoulli numbers.

We shall study some properties of the generalized Bernoulli number $B_{n,\chi}$. Let χ be a Dirichlet character of conductor f.

Let $\boldsymbol{Q}(\chi)$ denote the field generated over $\boldsymbol{Q}$ by the values of χ. For any integer $k \geqq 0$, let

$$S_{n,\chi}(k) = \sum_{a=1}^{k} \chi(a)\, a^n , \qquad n \geqq 0 .$$

The following fact was obtained by H. W. Leopoldt in [2].

PROPOSITION 3.1. *In* $\boldsymbol{Q}(\chi)$, *we have*

$$B_{n,\chi} \equiv \frac{1}{fp} S_{n,\chi}(fp) \qquad (\mathrm{mod}\, p) ,$$

where p *is a prime number satisfying* $(f, p)=1$.

EXAMPLE. Let $\chi = \left(\dfrac{-3}{*}\right)$.

① $\dfrac{2}{3} = B_{3,\left(\frac{-3}{*}\right)} \equiv \dfrac{1}{15} S_{3,\left(\frac{-3}{*}\right)}(15) = -\dfrac{223}{3} \qquad (\mathrm{mod}\ 5) .$

② $-\dfrac{10}{3} = B_{5,\left(\frac{-3}{*}\right)} \equiv \dfrac{1}{21} S_{5,\left(\frac{-3}{*}\right)}(21) = -\dfrac{191551}{3} \qquad (\mathrm{mod}\ 7) .$

PROPOSITION 3.2. *Let* $\chi_d = \left(\dfrac{-d}{*}\right)$ *be the Kronecker symbol with* $d>0$, *and let* p *be an odd prime number satisfying* $(d, p)=1$.
Then

$$\frac{1}{dp} S_{n,\chi_d}(dp) \equiv \frac{n}{d} \sum_{a=1}^{p-1} \left(\sum_{c=1}^{d-1} c\cdot\chi_d(a+cp) \right) a^{n-1} \qquad (\mathrm{mod}\, p) .$$

PROOF. For each integer a $(1 \leqq a \leqq p-1)$,

$$\sum_{m=0}^{d-1} \chi_d(a+mp)\,(a+mp)^n \equiv \sum_{m=0}^{d-1} \chi_d(a+mp)\, a^n + np\left(\sum_{c=1}^{d-1} c\chi_d(a+cp) \right) a^{n-1} \qquad (\mathrm{mod}\, p^2) .$$

Since $(d, p)=1$, we have $\sum_{m=0}^{d-1}\chi_d(a+mp)=0$.
Therefore

$$\frac{1}{dp}\sum_{b=1}^{dp}\chi_d(b)\,b^n\equiv\frac{n}{d}\sum_{a=1}^{p-1}\left(\sum_{c=1}^{d-1}c\cdot\chi_d(a+cp)\right)a^{n-1}\qquad(\mathrm{mod}\ p)\,.$$

This completes the proof.
By Proposition 3. 1 and 3. 2, we have

$$(2)\qquad\begin{cases} B_{n,\left(\frac{-3}{*}\right)}\equiv\dfrac{n}{3}\displaystyle\sum_{b=1}^{p-1}\left\{\left(\frac{-3}{b+p}\right)+2\left(\frac{-3}{b+2p}\right)\right\}b^{n-1} & (\mathrm{mod}\ p)\,.\\ B_{n,\left(\frac{-4}{*}\right)}\equiv\dfrac{n}{4}\displaystyle\sum_{b=1}^{p-1}\left\{\left(\frac{-4}{b+p}\right)+2\left(\frac{-4}{b+2p}\right)+3\left(\frac{-4}{b+3p}\right)\right\}b^{n-1} & (\mathrm{mod}\ p)\,.\end{cases}$$

§4. Congruence properties of the Fourier coefficients $a_k(T)$.

Now we would like to ask the following question.

Is it true that the relation $\Psi_{p-1}^{(g)}\equiv 1\,(\mathrm{mod}\ p)$ is valid for any prime number p?

Our main purpose of this note is to answer the above question. Namely, we shall show the existence of a prime number p satisfying $\Psi_{p-1}^{(2)}\not\equiv 1$ $(\mathrm{mod}\ p)$.

From our previous result (c. f. [4]), if $\Psi_{p-1}^{(2)}\not\equiv 1$ $(\mathrm{mod}\ p)$, then such a prime number p satisfies $B_{p-3}\equiv 0$ $(\mathrm{mod}\ p)$. Such prime numbers are studied in connection with Fermat's problem and the Iwasawa invariants. In particular, it is known that $p=16843$ is the unique prime number satisfying $B_{p-3}\equiv 0$ $(\mathrm{mod}\ p)$ and $p\leqq 125000$. (e. g. c. f. [10]).

Now we are going to calculate $a_{p-1}(T)$ $(\mathrm{mod}\ p)$ for $p=16843$ and

$$T=\begin{pmatrix}1 & \frac{1}{2}\\ \frac{1}{2} & 1\end{pmatrix},\ \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}.$$

From the formulae (1) in §2,

$$a_{p-1}\left(\begin{pmatrix}1 & \frac{1}{2}\\ \frac{1}{2} & 1\end{pmatrix}\right)=-\frac{4(p-1)\cdot B_{(p-1)-1,\left(\frac{-3}{*}\right)}}{B_{p-1}\cdot B_{2(p-1)-2}}\,,$$

$$a_{p-1}\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right)=-\frac{4(p-1)\cdot B_{(p-1)-1,\left(\frac{-4}{*}\right)}}{B_{p-1}\cdot B_{2(p-1)-2}}\,,$$

Since $B_{p-3}\equiv 0$ $(\mathrm{mod}\ p)$, it follows from the theorem of von Staudt-Clausen and Kummer's congruence that p does not appear in the numerator of the rational number $4(p-1)/(B_{p-1}\cdot B_{2(p-1)-2})$. Furthermore, by using the formulae (2) in § 3, the author proved

$$B_{16843-2,\left(\frac{-3}{*}\right)}\equiv 16739 \pmod{16843},$$
$$B_{16843-2,\left(\frac{-4}{*}\right)}\equiv 6022 \pmod{16843}.$$

(This result was obtained by using a computer FACOM 230 in Hokkaido University computing center.)
Consequently, we obtain

$$a_{p-1}\left(\begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}\right)\not\equiv 0 \pmod{p},$$
$$a_{p-1}\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)\not\equiv 0 \pmod{p} \quad \text{for } p=16843.$$

In particular, we have $\Psi^{(2)}_{p-1}\not\equiv 1 \pmod{p}$ for $p=16843$.

REMARK. In the case of $g\geqq 3$, we can calculate the value $a_k(T)$ in terms of p-adic densities. (e. g. c. f. [6], [7]).

From various results (e. g. c. f. [6], [8]), we would like to conjecture the following:

CONJECTURE.

$$\Psi^{(g)}_{p-1}\not\equiv 1 \pmod{p} \Longleftrightarrow B_{p-3}\cdot B_{p-5}\cdot\cdots\cdot B_{p-(g+1)}\equiv 0 \pmod{p} \qquad (g:\text{ even})$$
$$\Psi^{(g)}_{p-1}\not\equiv 1 \pmod{p} \Longleftrightarrow B_{p-3}\cdot B_{p-5}\cdot\cdots\cdot B_{p-g}\equiv 0 \pmod{p} \qquad (g:\text{ odd})$$

where p is a prime number satisfying $p\geqq 5$ and $p-1>g+1$.

Table 1.

k	$B_{k-1,\left(\frac{-3}{*}\right)}$	$a_k\begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$
4	$2\cdot 3^{-1}$	$2^7\cdot 3\cdot 5\cdot 7$
6	$-2\cdot 5\cdot 3^{-1}$	$2^6\cdot 3^2\cdot 7\cdot 11$
8	$2\cdot 7^2\cdot 3^{-1}$	$2^8\cdot 3\cdot 5\cdot 7$
10	$-2\cdot 809\cdot 3^{-1}$	$2^6\cdot 3\cdot 7\cdot 11\cdot 19\cdot 809\cdot 43867^{-1}$
12	$2\cdot 11\cdot 1847\cdot 3^{-1}$	$2^7\cdot 3^2\cdot 5\cdot 7\cdot 13\cdot 23\cdot 1847\cdot 131^{-1}\cdot 593^{-1}\cdot 691^{-1}$
14	$-2\cdot 7\cdot 13^3\cdot 47\cdot 3^{-1}$	$2^6\cdot 3\cdot 7\cdot 13^2\cdot 47\cdot 657931^{-1}$
16	$2\cdot 5\cdot 419\cdot 16519\cdot 3^{-1}$	$2^9\cdot 3\cdot 5^2\cdot 7\cdot 11\cdot 17\cdot 31\cdot 419\cdot 16519\cdot 1721^{-1}\cdot 3617^{-1}\cdot 1001259881^{-1}$
18	$-2\cdot 17\cdot 23\cdot 401\cdot 13687\cdot 3^{-1}$	$2^6\cdot 3^3\cdot 7\cdot 19\cdot 23\cdot 401\cdot 13687\cdot 43867^{-1}\cdot 151628697551^{-1}$

Table 2.

k	$B_{k-1,\left(\frac{-4}{*}\right)}$	$a_k\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$
4	$3\cdot2^{-1}$	$2^5\cdot3^3\cdot5\cdot7$
6	$-5^2\cdot2^{-1}$	$2^4\cdot3^3\cdot5\cdot7\cdot11$
8	$7\cdot61\cdot2^{-1}$	$2^6\cdot3^2\cdot5\cdot61$
10	$-3^2\cdot5\cdot277\cdot2^{-1}$	$2^4\cdot3^4\cdot5\cdot7\cdot11\cdot19\cdot277\cdot43867^{-1}$
12	$11\cdot19\cdot2659\cdot2^{-1}$	$2^5\cdot3^3\cdot5\cdot7\cdot13\cdot19\cdot23\cdot2659\cdot131^{-1}\cdot593^{-1}\cdot 691^{-1}$
14	$-5\cdot13^2\cdot43\cdot967\cdot2^{-1}$	$2^4\cdot3^2\cdot5\cdot13\cdot43\cdot967\cdot657931^{-1}$
16	$3\cdot5\cdot47\cdot4241723\cdot2^{-1}$	$2^7\cdot3^4\cdot5^2\cdot7\cdot11\cdot17\cdot31\cdot47\cdot4241723\cdot1721^{-1}\cdot 3617^{-1}\cdot1001259881^{-1}$
18	$-5\cdot17^2\cdot228135437\cdot2^{-1}$	$2^7\cdot3^2\cdot5\cdot7\cdot17\cdot19\cdot228135437\cdot43867^{-1}\cdot 151628697551^{-1}$

References

[1] J. IGUSA: On the ring of modular forms of degree two over **Z**, to appear.

[2] H. W. LEOPOLDT: Eine Verallgemeinerung der Bernoullischen Zahlen, Abh. Math. Seminar, Hamburg, 22, 1958.

[3] H. MAASS: Die Fourierkoeffizienten der Eisensteinreihen zweiten Grades, Mat-Fys. Medd. Danske Vid. Selsk., 34, 1964.

[4] S. NAGAOKA: P-adic properties of Siegel modular forms of degree 2, Nagoya Math. J. Vol. 71, 1978.

[5] J.-P. SERRE: Formes modulaires et fonctions zêta p-adiques, Lecture Note in Math., 350, Springer Verlag, 1972.

[6] C. L. SIEGEL: Einführung in die Theorie der Modulfunktionen n-ten Grades, Math. Ann. 116, 1939.

[7] C. L. SIEGEL: Über die analytische Theorie der quadratischen Formen, Ann. of Math., 36, 1935.

[8] C. L. SIEGEL: Über die Fourierschen Koeffizienten der Eisensteinschen Reihen, Mat-Fys. Medd. Danske Vid. Selsk., 34, 1964.

[9] H. P. F. SWINNERTON-DYER: On l-adic representations and congruences for coefficients of modular forms, Lecture Note in Math., 350, Springer Verlag.

[10] S. WAGSTAFF: The irregular primes to 125000, to appear.

Department of Mathematics
Hokkaido University