COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 47, No. 1 1998

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171 JAPAN

On Some Elementary Character Sums

by

Tomoyoshi IBUKIYAMA

(Received July 22, 1997)

For any prime p, the action of the symplectic group $Sp(2, \mathbb{F}_p)$ on the Siegel modular forms of degree 2 belonging to the principal congruence subgroup $\Gamma(p)$ was investigated by Tsushima, Lee and Weintraub, and Hashimoto independently. Tsushima [3], [4], and Lee and Weintraub [2] used the Lefschetz fixed point theorem and Hashimoto [1] used the trace formula. Now, let p be an odd prime and denote by $\left(\frac{*}{p}\right)$ the Legendre symbol. By comparing some part of apparently different results by Tsushima [4] and Hashimoto [1], one gets easily a formula expressing the following character sum

$$\sum_{n,m=1}^{p-1}\left(\frac{m-4n}{p}\right)\left(\frac{m}{p}\right)mn$$

by the class number of the quadratic field $\mathbb{Q}(\sqrt{-p})$ (cf. Hashimoto [1] Remark 3). The aim of this paper is to give an elementary alternative proof and a generalization of this formula.

1. Theorems

We fix an odd prime p. For short, we denote by ψ the Legendre symbol: $\psi(a)=\left(\frac{a}{p}\right)$. We also put $\zeta=\exp(2\pi i/p)$.

THEOREM 1. *Notation and assumptions being the same as above, let l be any positive integer which is prime to p. Put*

$$I(l, p)=\sum_{a,b=1,a\neq b}^{p-1}\frac{\psi(a)\psi(b)}{(1-\zeta^{a-b})(1-\zeta^{lb})}.$$

Then, we get

$$\begin{aligned}I(l, p)&=\frac{1}{p}\sum_{m,n=1}^{p-1}\psi(m)\psi(m-ln)mn+\frac{(p-1)^2}{4}\\&=-\frac{p-1}{4}+\frac{l(p^2-1)}{24}-\frac{1}{2p}\sum_{c=0}^{l-1}S_{l,c}(\psi)^2,\end{aligned}$$

where we put

$$S_{l,c}(\psi)=\sum_{n=0}^{p-1}\psi(ln+c)n\,.$$

We shall describe the values $S_{l,c}(\psi)$ more explicitly in the next theorem. Since we would like to treat some more general case, we prepare more notation. For any Dirichlet character δ, we denote by f_δ the conductor of δ and by $B_{1,\delta}$ the first generalized Bernoulli number belonging to $\delta: B_{1,\delta}=f_\delta^{-1}\sum_{m=1}^{f_\delta}\delta(m)m$. Incidentally, for non trivial δ, we have $B_{1,\delta}\neq 0$, if and only if $\delta(-1)=-1$. We fix a Dirichlet character χ with conductor f_χ. For any natural number l prime to f_χ and an integer c, define a character sum $S_{l,c}(\chi)$ by

$$S_{l,c}(\chi)=\sum_{n=0}^{f_\chi-1}\chi(ln+c)n\,.$$

This value depends not only on $c \bmod l$, but also on a choice c of the representative of $c \bmod l$.

It seems more or less known in principle how to execute a calculation to get a formula expressing $S_{l,c}(\chi)$ by generalized Bernoulli numbers (e.g. Yamamoto [5]). But, since we could not find any reference containing a general closed explicit formula of this type, we shall give it here. For any natural number m, we denote by $X(m)$ the set of *primitive* Dirichlet characters δ such that m is divisible by f_δ, and by $Y(m)$ the set of *primitive* Dirichlet characters with conductor m.

THEOREM 2. *Let l be a natural number prime to f_χ and c be a natural number prime to l with $1\leq c\leq l-1$. For any integer u with $u\mid l$, denote by l_u the u-primary part of l, that is, the maximum integer which divides l and is prime to u. We get*

$$S_{l,c}(\chi)=\varphi(l)^{-1}f_\chi\sum_{u\mid l}\sum_{\delta\in Y(u)}\left(\delta(c^{-1})B_{1,\delta_\chi}\prod_{q\mid l_u}(1-\chi(q)\delta(q))\right),$$

where q runs over prime numbers dividing l_u and φ is the Euler function.

As an easy corollary to the above two theorems, we get

COROLLARY 2.1 (Tsushima [4] and Hashimoto [1]). *Notation and assumptions being as in Theorem 1, denote by $h(-p)$ the class number of the quadratic number field $\mathbb{Q}(\sqrt{-p})$. Then, we get*

$$\sum_{a,b=1,a\neq b}^{p-1}\frac{\psi(a)\psi(b)}{(1-\zeta^{a-b})(1-\zeta^{4b})}=\frac{1}{p}\sum_{n,m=1}^{p-1}\psi(m-4n)\psi(m)mn+\frac{(p-1)^2}{4}$$

$$=\frac{(p-1)(2p-1)}{12}-\begin{cases} 7/6 & \text{if } p=3\,, \\ p\cdot h(-p)^2/4 & \text{if } p\equiv 1 \bmod 4\,, \\ 7p\cdot h(-p)^2/2 & \text{if } p\equiv 3 \bmod 8\,,\ p\neq 3\,, \\ p\cdot h(-p)^2/2 & \text{if } p\equiv 7 \bmod 8\,. \end{cases}$$

2. Proofs

We shall prove the results in section 1.

Proof of Theorem 1. We show the first equality. For any c with $(c, p)=1$, we easily get

$$\frac{1}{1-\zeta^c}=-\frac{1}{p}\sum_{n=1}^{p-1}\zeta^{cn}n\,.$$

So, we have

$$\begin{aligned} p^2 I(l, p) &= \sum_{n,m=1}^{p-1}\ \sum_{a,b=1,a\neq b}^{p-1} \psi(a)\psi(b)\zeta^{(a-b)m}\zeta^{lbn}nm \\ &= \sum_{n,m=1}^{p-1} mn\left(\sum_{a=1}^{p-1}\psi(a)\zeta^{am}\right)\left(\sum_{b=1}^{p-1}\psi(b)\zeta^{b(ln-m)}\right)-\sum_{n,m,b=1}^{p-1}\zeta^{lbn}mn \\ &= \tau(\psi)^2\left(\sum_{n,m=1}^{p-1}\psi(m)\psi(ln-m)mn\right)+\frac{p^2(p-1)^2}{4}\,, \end{aligned}$$

where $\tau(\psi)$ is the Gaussian sum $\tau(\psi)=\sum_{n=1}^{p-1}\psi(n)\zeta^n$. Since $\tau(\psi)^2=\psi(-1)p$, we get the first equality. Next we shall show the second equality. Replacing b by $-b$ in the definition of $I(l, p)$, and noting $1/(1-\zeta^{lb})=1-1/(1-\rho^{lb})$, we get

$$\psi(-1)I(l, p)=\sum_{a,b=1,a+b\neq p}^{p-1}\frac{\psi(ab)}{1-\zeta^{(a+b)}}-\sum_{a,b=1,a+b\neq p}^{p-1}\frac{\psi(ab)}{(1-\zeta^{lb})(1-\zeta^{(a+b)})}\,.$$

Exchanging a and b in the above expression, and taking the average of both expressions, we see that the second term is equal to

$$\frac{1}{2}\sum_{a,b=1,a+b\neq p}\frac{\psi(ab)}{1-\zeta^{a+b}}\times\left(\frac{1}{1-\zeta^{la}}+\frac{1}{1-\zeta^{lb}}\right).$$

Since

$$2-\zeta^{la}-\zeta^{lb}=(1-\zeta^{la})(1-\zeta^{lb})+(1-\zeta^{l(a+b)})\,,$$

we get

$$2\psi(-1)I(l, p)=\sum_{a,b=1,a+b\neq p}^{p-1}\left(\frac{\psi(ab)}{1-\zeta^{a+b}}-\frac{\psi(ab)(1-\zeta^{l(a+b)})}{(1-\zeta^{la})(1-\zeta^{lb})(1-\zeta^{a+b})}\right).$$

The first term can be calculated easily. Indeed, expanding $1/(1-\zeta^{a+b})$ as before, we get

$$\sum_{a,b=1,a+b\neq p}^{p-1}\frac{-p\psi(ab)}{1-\zeta^{a+b}}=\sum_{n=1}^{p-1}\sum_{a,b=1,a+b\neq p}^{p-1}\psi(ab)\zeta^{(a+b)n}n$$

$$=\sum_{a,b,n=1}^{p-1}\psi(ab)\zeta^{(a+b)n}n-\sum_{a,n=1}^{p-1}\psi(-a^2)n=\frac{\psi(-1)(p-1)p}{2}.$$

Next, we shall evaluate the second term. Since

$$\frac{1-\zeta^{l(a+b)}}{1-\zeta^{a+b}}=\sum_{c=0}^{l-1}\zeta^{c(a+b)},$$

we get

$$\sum_{a,b=1,a+b\neq p}^{p-1}\frac{\psi(ab)(1-\zeta^{l(a+b)})}{(1-\zeta^{la})(1-\zeta^{lb})(1-\zeta^{a+b})}=\frac{\tau(\psi)^2}{p^2}\sum_{c=0}^{l-1}\left(\sum_{n=1}^{p-1}\psi(ln+c)n\right)^2$$

$$-\psi(-1)\sum_{a=1}^{p-1}\frac{l}{(1-\zeta^{la})(1-\zeta^{-la})}.$$

Hence, we get

$$I(l,p)=-\frac{p-1}{4}+\frac{l(p^2-1)}{24}-\frac{1}{2p}\sum_{c=0}^{l-1}S_{l,c}(\psi)^2.$$

q.e.d.

To prove Theorem 2, we prepare several lemmas.

LEMMA 1. *For a natural number l prime to f_χ and any $\delta\in X(l)$, we get*

$$\sum_{c=0}^{l-1}\delta(c)S_{l,c}(\chi)=f_\chi B_{1,\delta_\chi}.$$

Proof. For the sake of simplicity, put $T_l(\chi,\delta)=\sum_{c=0}^{l-1}\delta(c)S_{l,c}(\chi)$. Since $\delta(c)=\delta(ln+c)$ and $\sum_{n=0}^{f_\chi-1}\chi(ln+c)=0$, we get

$$T_l(\chi,\delta)=l^{-1}\sum_{c=0}^{l-1}\sum_{n=0}^{f_\chi-1}\delta(ln+c)\chi(ln+c)(ln+c)$$

$$=l^{-1}\sum_{m=0}^{f_\chi l-1}\delta(m)\chi(m)m.$$

Since $(l,f_\chi)=1$, the Dirichlet character $\delta\chi$ is primitive and $f_{\delta\chi}=f_\delta f_\chi$. Hence, we get

$$T_l(\chi,\delta)=l^{-1}\sum_{a=0}^{lf_\delta^{-1}-1}\sum_{b=0}^{f_{\delta\chi}-1}(\delta\chi(f_{\delta\chi}a+b))(f_{\delta\chi}a+b)$$

$$=l^{-1}(lf_\delta^{-1})\sum_{b=0}^{f_\delta f_\chi-1}\delta_\chi(b)b$$

$$=f_\chi B_{1,\delta\chi}.$$

q.e.d.

From this formula, we shall extract a kind of inversion formula. Since δ is primitive, we need a careful treatment for c with $(c, l)>1$. We fix a natural number l which is prime to f_χ and put $L=\prod_{q|l} q$, where q runs over primes. For any $m|L$, denote by l_m the m-primary part of l.

Lemma 2. *For any fixed number $d\in(Z/lZ)^\times$, we get*

$$\sum_{m|L}\varphi(l_m)\chi(m)S_{l_m,e}(\chi)=f_\chi\sum_{\delta\in X(l)}\delta(d^{-1})B_{1,\delta\chi},$$

where e is the unique integer such that $me\equiv d \bmod l_m$ with $0\le e\le l_m-1$.

Proof. We shall show this lemma by taking the sum over $\delta\in X(l)$ of the both sides of the formula in Lemma 1. For an integer c with $0\le c\le l-1$, there exists the unique $m|L$ such that $m|c$ and $(c, L/m)=1$. For such c, we have $\sum_{\delta\in X(l)}\delta(c)=\sum_{\delta\in X(l_m)}\delta(c)$, since $\delta(c)\neq 0$ only if $(f_\delta, m)=1$. Besides,

$$\sum_{\delta\in X(l_m)}\delta(d^{-1}c)=\begin{cases}\varphi(l_m) & \text{when } d\equiv c \bmod l_m,\\ 0 & \text{otherwise}.\end{cases}$$

Now we denote by $C(m)$ the following set of integers.

$$C(m)=\{c\in\mathbb{Z}\,;\,0\le c\le l-1,\ m|c,\ (c, L/m)=1, \text{ and } c\equiv d \bmod l_m\}.$$

If we take the unique integer e such that $me\equiv d \bmod l_m$ with $0\le e\le l_m-1$, then $(e, l_m)=1$, since $(d, l)=1$. Hence we get

$$C(m)=\{(e+l_m a)m\,;\,a\in Z,\ 0\le a\le(l_m m)^{-1}l-1\}.$$

Obviously, we get

$$f_\chi\sum_{\delta\in X(l)}\delta(d^{-1})B_{1,\delta_\chi}=\sum_{\delta\in X(l)}\sum_{c=0}^{l-1}\delta(d^{-1}c)S_{l,c}(\chi)=\sum_{m|L}\varphi(l_m)\sum_{c\in C(m)}S_{l,c}(\chi),$$

and

$$\begin{aligned}\sum_{c\in C(m)}S_{l,c}(\chi)&=\sum_{a=0}^{l/l_m m-1}S_{l,m(e+l_m a)}(\chi)\\&=\sum_{a=0}^{l/l_m m-1}\sum_{n=0}^{f_\chi-1}\chi(ln+(e+l_m a)m)n\\&=\chi(m)\sum_{a=0}^{l/l_m m-1}\sum_{n=0}^{f_\chi-1}\chi\left(\frac{ln}{m}+e+l_m a\right)n\\&=\chi(m)l_m m l^{-1}\sum_{a=0}^{l/l_m m-1}\sum_{n=0}^{f_\chi-1}\chi\left(l_m\left(\frac{ln}{l_m m}+a\right)+e\right)\left(\frac{ln}{l_m m}+a\right)\end{aligned}$$

$$
\begin{aligned}
&=\chi(m)l_m ml^{-1}\sum_{b=0}^{f_\chi l/l_m m-1}\chi(l_m b+e)b\\
&=\chi(m)l_m ml^{-1}\sum_{b_1=0}^{(l_m m)^{-1}l-1}\sum_{b_0=0}^{f_\chi-1}\chi(l_m(b_1 f_\chi+b_0)+e)(f_\chi b_1+b_0)\\
&=\chi(m)S_{l_m,e}(\chi)\,.
\end{aligned}
$$

Hence, the lemma is proved.

LEMMA 3. *We fix natural numbers l prime to f_χ and c prime to l with $1\le c\le l-1$. We define L and l_m for $m\mid l$ in the same way as in Lemma 2. Then, we get*

$$\varphi(l)f_\chi^{-1}S_{l,c}(\chi)=\sum_{m\mid L}\mu(m)\chi(m)\sum_{\delta\in X(l_m)}\delta(mc^{-1})B_{1,\delta_\chi}\,,$$

where μ is the Möbius function.

Proof. For $u\mid v\mid L$ and any $d\in(Z/lZ)^\times$, we put

$$g(u, v, d)=\varphi(l/l_u)\chi(u^{-1}v)S_{l/l_u,w}(\chi)\,,$$

where w is defined as the unique integer such that $(u^{-1}v)w\equiv d \bmod (l/l_u)$ with $1\le w\le l/l_u-1$. We also put

$$f(v, d)=f_\chi\sum_{\delta\in X(l/l_v)}\delta(d^{-1})B_{1,\delta_\chi}\,.$$

Now, we apply Lemma 2 for $(v, l/l_v)$ instead of (L, l). Noting that $(l/l_v)_m=l_m/l_v$ for any $m\mid v$, we get

$$\sum_{m\mid v}\varphi(l_m/l_v)\chi(m)S_{l_m/l_v,e}(\chi)=f_\chi\sum_{\delta\in X(l/l_v)}\delta(d^{-1})B_{1,\delta_\chi}\,,$$

where e is determined by $me\equiv d \bmod (l_m/l_v)$ with $1\le e\le l_m/l_v-1$. Now for each $m\mid v$, define u by $mu=v$, then we get $l_m/l_v=l/l_u$ and

$$\sum_{u\mid v}g(u, v, d)=f(v, d)\,.$$

Next, for any $u\mid L$, we put $G(u)=g(u, L, c)$ and $F(u)=\chi(u^{-1}L)f(v, L^{-1}uc)$. For any $v\mid L$, we get $g(u, L, c)=\chi(v^{-1}L)g(u, v, L^{-1}vc)$, where $L^{-1}vc$ is regarded as an element of $(Z/l_vZ)^\times$. Hence we see

$$\sum_{u\mid v}G(u)=\chi(v^{-1}L)\sum_{u\mid v}g(u, v, L^{-1}vc)=\chi(v^{-1}L)f(v, L^{-1}vc)=F(v)\,.$$

By Möbius inversion formula, we get

$$G(L)=\sum_{m\mid L}\mu(m)F\left(\frac{L}{m}\right),$$

which is the assertion of our Lemma. q.e.d.

Proof of Theorem 2. We fix $\delta\in X(l)$ and denote the conductor of δ shortly by u. By definition, we get $\delta\in X(l_m)$ if and only if $u\,|\,l_m$. This is also equivalent to the condition $m\,|\,l_u$. So the coefficient of B_{1,δ_χ} in the right hand side of Lemma 3 is given by

$$\sum_{m|l_u}\mu(m)\chi(m)\delta(mc^{-1})=\delta(c^{-1})\prod_{q|l_u}(1-\chi(q)\delta(q))\,,$$

where q runs over all primes which divide l_u. Hence, we get Theorem 2.

Proof of Corollary. We see easily that $S_{4,0}(\psi)=pB_{1,\psi}$ and $S_{4,2}(\psi)=\psi(2)S_{2,1}(\psi)=(\psi(2)-1)pB_{1,\psi}$. Also, by Theorem 2, we get $S_{4,1}(\psi)=2^{-1}((1-\psi(2))pB_{1,\psi}+pB_{1,\delta\psi})$ and $S_{4,3}(\psi)=2^{-1}((1-\psi(2))pB_{1,\psi}-pB_{1,\delta\psi})$, where δ is the unique primitive Dirichlet character modulo 4. Hence,

$$\sum_{c=0}^{3}S_{4,c}(\psi)^2=(4-3\psi(2))p^2B_{1,\psi}^2+2^{-1}p^2B_{1,\delta\psi}^2\,.$$

If $p\equiv 1 \bmod 4$, then $B_{1,\psi}=0$ and $B_{1,\delta\psi}=h(-p)$. If $p\equiv 3 \bmod 4$ and $p\neq 3$, then $B_{1,\delta\psi}=0$ and $B_{1,\psi}=h(-p)$. Hence Corollary is proved.

References

[1] K. Hashimoto, Representations of the finite symplectic group $Sp(4, \mathbb{F}_p)$ in the spaces of Siegel modular forms, *Contemporary Mathematics* Vol. 53, (1986), 253–276.

[2] R. Lee and S. H. Weintraub, On a generalization of a theorem of Erich Hecke, Proc. Nat. Acad. Sci. U.S.A. **79** (1982), 7955–7957.

[3] R. Tsushima, On the spaces of Siegel cusp forms of degree two, *Amer. J. Math.* **104** (1982), 843–885.

[4] R. Tsushima, The spaces of Siegel cusp forms of degree two and the representation of $Sp(2, F_p)$, *Proc. Japan Acad.* **60** (1984), 209–211.

[5] Y. Yamamoto, Dirichlet series with periodic coefficients, Algebraic Number Theory (1977), 275–289, Papers contributed for the Kyoto International Symposium, 1976. Japan Society for the Promotion of Science.

Department of Mathematics
Graduate School of Science
Osaka University
Machikaneyama 1–16
Toyonaka, Osaka, 560 Japan