JEFFREY L. MEYER

A reciprocity congruence for an analogue of the Dedekind sum and quadratic reciprocity


<http://www.numdam.org/item?id=JTNB_2000__12_1_93_0>
A Reciprocity Congruence for an Analogue of the Dedekind Sum and quadratic reciprocity

par JEFFREY L. MEYER

1. INTRODUCTION

In Berndt [1] and Goldberg [2] the sum $S_4(d,c)$ is defined for $c > 0$ by

$$S_4(d,c) = \sum_{j=1}^{c-1} (-1)^{[dj/c]}.$$

The sum is one of several involved in the multiplier systems for transformations of the logarithms of the classical theta-functions. We define two of them here. Let $q = e^{\pi iz}$ and for $\text{Im}(z) > 0$ define

$$\theta_3(z) = \sum_{n=-\infty}^{\infty} q^{n^2} \quad \text{and} \quad \theta_4(z) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n^2}.$$

We prove a new reciprocity theorem for the sum $S_4(d,c)$. As an application of the theorem, we deduce the law of quadratic reciprocity.

Let $V = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $ad - bc = 1$ and $Vz = (az + b)/(cz + d)$. We use the principal branch of the logarithm at all times. Berndt [1] proved that
if \( b \) is even, then

\[
\log \theta_4(Vz) = \log \theta_4(z) + \frac{1}{2} \log(cz + d) - \frac{1}{4} \pi i - \frac{1}{4} \pi i S_4(d, c).
\]

Goldberg [2] gives the following formula. If \( a \) is even and \( b, c \) and \( d \) are odd, then

\[
\log \theta_3(Vz) = \log \theta_4(z) + \frac{1}{2} \log(cz + d) - \frac{1}{4} \pi i - \frac{1}{4} \pi i S_4(d, c).
\]

With the reciprocity theorem for the Dedekind sum \( s(d, c) \) and connections between \( s(d, c) \) and the Legendre-Jacobi symbol \( \left( \frac{d}{c} \right) \), one can deduce the quadratic reciprocity law (See Rademacher and Grosswald [3], pp. 34-35). Berndt [1] proved elegant reciprocity theorems for several sums that arise in the transformation formulas of the logarithms of the classical theta-functions. None of these reciprocity theorems allow for both of the arguments in the sum to be odd. For the application of the sums arising in the theta-function transformations to quadratic reciprocity, however, we need a new reciprocity theorem where \( c \) and \( d \) are both odd. And, unlike the Dedekind sum, the sum \( S_4(d, c) \) does not possess a reciprocity theorem. However, a reciprocity relation modulo 8 for the sum \( S_4(d, c) \) does exist and this is sufficient to deduce the quadratic reciprocity theorem. For additional properties of \( S_4(d, c) \) see [7] and [6].

To establish the connection between \( S_4(d, c) \) and the Legendre-Jacobi symbol, we turn to Rademacher’s book [8] (pp. 180-182) for the needed results. We use the same double subscript notation as Rademacher to state the theorem. For \( \text{Im}(z) > 0 \) and \( \mu, \nu \in \{0, 1\} \), let

\[
\theta_{\mu, \nu}(z) = \sum_{n=-\infty}^{\infty} (-1)^{\nu n} e^{(n+\mu/2)^2 \pi i z}.
\]

Thus

\[
\theta_{0,0}(z) = \theta_3(z) \quad \text{and} \quad \theta_{0,1}(z) = \theta_4(z).
\]

Note that we may allow integers other that 1 and 0 as subscripts since it can be shown that

\[
\theta_{\mu+2, \nu}(z) = (-1)^{\nu} \theta_{\mu, \nu}(z) \quad \text{and} \quad \theta_{\mu, \nu+2}(z) = \theta_{\mu, \nu}(z).
\]

We state one of Rademacher’s transformation formulas.

**Theorem 1.** If \( V = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \) and \( c \) is odd and positive, then

\[
\theta_{1+a, 1-b}(Vz) = -i^{b}e^{\pi ibd/4} \epsilon_1 \sqrt{\frac{cz + d}{i}} \theta_4(z),
\]
The next result is the foundation on which the new reciprocity theorem is based.

**Theorem 2.** Let $c$ and $d$ be positive, coprime, odd integers. Then

$$S_4(c,d) + S_4(d,c) = -1 + S_4(c^2, cd + 1).$$

**Proof.** Choose $a$ and $b$ with $b > d$, $b$ even and $ad - bc = 1$ and set

$$V = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \text{and} \quad W = \begin{bmatrix} -d^2 & cd - 1 \\ cd + 1 & -c^2 \end{bmatrix}.$$ 

Then

$$VW = \begin{bmatrix} b - d & c - a \\ d & -c \end{bmatrix}.$$ 

Note that in each matrix the upper right entry is even and the determinant is 1. We use (1) with $V$ replaced with $VW$ to find that

$$\log \theta_4((VW)z) = \log \theta_4(z) + \frac{1}{2} \log(dz - c) - \frac{1}{4} \pi i - \frac{1}{4} \pi i S_4(-c, d).$$

Then we apply (1) with $z$ replaced by $Wz$ to see that

$$\log \theta_4(V(Wz)) = \log \theta_4(Wz) + \frac{1}{2} \log((cd + 1)z - c^2)$$

$$- \frac{1}{4} \pi i - \frac{1}{4} \pi i S_4(d, c),$$

and finally we use (1) with $V$ replaced by $W$ to deduce that

$$\log \theta_4(Wz) = \log \theta_4(z) + \frac{1}{2} \log((cd + 1)z - c^2)$$

$$- \frac{1}{4} \pi i - \frac{1}{4} \pi i S_4(-c^2, cd + 1).$$

We replace $\log \theta_4(Wz)$ in (6) with (7) and then combine the result with (5) to conclude that

$$- \frac{1}{4} \pi i S_4(-c, d) = - \frac{1}{4} \pi i S_4(-c^2, cd + 1) - \frac{1}{4} \pi i - \frac{1}{4} \pi i S_4(d, c).$$

We have used the following lemma [5] to conclude that there are no branch changes with the logarithms, so the complete cancellation is justified.
Lemma 1. Let $A, B, C, \text{ and } D$ be real with $A$ and $B$ not both zero and $C > 0$. Then for $\text{Im}(z) > 0$,

$$\arg((Az + B)/(Cz + D)) = \arg(Az + B) - \arg(Cz + D) + 2\pi k,$$

where $k$ is independent of $z$ and

$$k = \begin{cases} 
1, & \text{if } A \leq 0 \text{ and } AD - BC > 0, \\
0, & \text{otherwise}.
\end{cases}$$

Next we multiply (8) by $4/(\pi i)$, rearrange, and use the fact that $S_4(-c, d) = -S_4(c, d)$ to conclude that

$$S_4(c, d) + S_4(d, c) = -1 + S_4(c^2, cd + 1).$$

\[\square\]

The symmetry between $c$ and $d$ on the left-hand side of the equation in Theorem 3 leads immediately to the next result.

Corollary 1. If $c$ and $d$ are coprime, odd, positive integers, then

$$S_4(c^2, cd + 1) = S_4(d^2, cd + 1).$$

The final step towards the desired reciprocity relation is the following congruence relation.

Lemma 2. Let $d$ be an odd prime and $c > d$ be an odd, positive integer coprime to $d$. Then

$$S_4(d^2, cd + 1) \equiv cd \pmod{8}.$$

Proof. Using the definition of $S_4(d, c)$ and the fact that

$$[x] - 2\left[\frac{x}{2}\right] = \begin{cases} 
0, & \text{if } [x] \text{ is even,} \\
1, & \text{if } [x] \text{ is odd,}
\end{cases}$$

we see that

$$S_4(d^2, cd + 1) = \sum_{j=1}^{cd} (-1)^j \left\lfloor \frac{jd^2}{cd + 1} \right\rfloor$$

$$= \#\{[jd^2/(cd + 1)] \text{ even}\} - \#\{[jd^2/(cd + 1)] \text{ odd}\}$$

$$= cd - 2 \sum_{j=1}^{cd} \left\lfloor \frac{jd^2}{cd + 1} \right\rfloor + 4 \sum_{j=1}^{cd} \left\lfloor \frac{jd^2}{2(cd + 1)} \right\rfloor.$$
We now apply (10) to the first of the final two sums in (9) and separate the terms in the second sum on the right according to the parity of $j$. Thus (9) becomes

\begin{align*}
(11) \quad S_4(d^2, cd + 1) &= cd - (d^2 - 1)cd + 4 \sum_{j=1}^{(cd-1)/2} \left\lfloor \frac{jd^2}{cd + 1} \right\rfloor \\
&\quad + 4 \sum_{j=1}^{(cd+1)/2} \left( \frac{jd^2}{cd + 1} - \frac{d^2}{2(cd + 1)} \right).
\end{align*}

Let

\begin{equation}
N = \# \left\{ j = 1, 2, \ldots, \frac{cd + 1}{2} : \left\{ \frac{jd^2}{cd + 1} \right\} < \frac{d^2}{2(cd + 1)} \right\},
\end{equation}

where $\{x\} = x - \lfloor x \rfloor$ denotes the fractional part of $x$. The final sum in (11) can be simplified since $d < c$ and $\lfloor d^2/2 \rfloor = (d^2 - 1)/2$ for $d$ odd. Note that

\begin{equation}
\sum_{j=1}^{(cd+1)/2} \left[ \frac{jd^2}{cd + 1} - \frac{d^2}{2(cd + 1)} \right] = \sum_{j=1}^{(cd-1)/2} \left[ \frac{jd^2}{cd + 1} \right] + \frac{d^2 - 1}{2} - N.
\end{equation}

We conclude from (11) and (13) that

\begin{equation}
S_4(d^2, cd + 1) = cd - (d^2 - 1)cd + 8 \sum_{j=1}^{(cd-1)/2} \left[ \frac{jd^2}{cd + 1} \right] + 2(d^2 - 1) - 4N.
\end{equation}

Since $d$ is odd and thus $d^2 \equiv 1 \pmod{8}$, we deduce the congruence

\begin{equation}
S_4(d^2, cd + 1) \equiv cd + 4N \pmod{8}.
\end{equation}

We claim that $N$ is even. Let

\begin{equation}
n = \# \left\{ k = 1, 2, \ldots, \frac{d^2 - 1}{2} : LPR_d(k(cd + 1)) > \frac{d^2}{2} \right\},
\end{equation}

where $LPR_l(m)$ denotes the least positive residue of $m$ modulo the positive integer $l$. Observe that

\begin{equation}
\left\{ \frac{jd^2}{cd + 1} \right\} < \frac{d^2}{2(cd + 1)}
\end{equation}

if and only if there exists a positive integer $k$ such that

\begin{equation}
2k(cd + 1) < 2jd^2 < 2k(cd + 1) + d^2.
\end{equation}

We rewrite (16) in the form

\begin{equation}
\frac{k(cd + 1)}{d^2} < j < \frac{k(cd + 1)}{d^2} + \frac{1}{2}.
\end{equation}
Since the interval \((k(cd + 1)/d^2, k(cd + 1)/d^2 + 1/2)\) has length \(1/2\), it contains an integer \(j\) if and only if \(k\) satisfies
\[
\left\{ \frac{k(cd + 1)}{d^2} \right\} > \frac{1}{2},
\]
or, in other words, if and only if \(LPR_{d^2}(k(cd + 1)) > d^2/2\). Thus \(N = n\).

The final claim in the proof of the congruence is the following: The number \(n\) defined above is even.

The proof of this claim is a careful application of the method used in the standard proof of Gauss’s Lemma (see [4], p. 133, for example).

Let \(r_1, r_2, \ldots, r_n\) be the \(n\) residues of \(k(cd + 1), 1 \leq k \leq (d^2 - 1)/2\), falling in the upper half of the least positive residue system \((\text{mod } d^2)\) and let \(s_1, s_2, \ldots, s_l\) be those in the lower half. Then \(n + l = (d^2 - 1)/2\). Next we consider \(r'_i = d^2 - r_i\) for \(i = 1, 2, \ldots, n\). Each of the \(r'_i\) are distinct and we can say further that no \(r'_i = s_j\) for any \(i\) and \(j\).

Note that there are \(\lceil (d^2 - 1)/(2d) \rceil = (d - 1)/2\) positive multiples of \(d\) that are less than \((d^2 - 1)/2\). Now for \(k = md, 1 \leq m \leq (d - 1)/2\),
\[
k(cd + 1) = md(cd + 1) \equiv md \pmod{d^2}.
\]

From (18), we conclude that
\[
LPR_{d^2}(md(cd + 1)) = md < \frac{d^2}{2}.
\]

Thus all of the residues produced when \(k\) is a multiple of \(d\) are among the \(s_j\) and are in fact the positive multiples of \(d\) that are less than \(d^2/2\). We remove them from the list \(\{s_1, \ldots, s_l\}\), reindex this set and put
\[
l' = l - \frac{d - 1}{2}.
\]

So now we consider the \(n\) \(r_i\)'s, and the \(l'\) \(s_j\)'s, with \(n + l' = d(d - 1)/2\) residues altogether. By the distinctness of the \(r'_i\), we conclude that the \(r'_i\) and the \(s_j\) are some rearrangement of the numbers \(1, 2, \ldots, (d^2 - 1)/2\) with the multiples of \(d\) removed. Thus
\[
r'_1 r'_2 \cdots r'_n s_1 s_2 \cdots s_{l'} = \prod_{1 \leq \alpha \leq (d^2 - 1)/2 \atop (d, \alpha) = 1} \alpha;
\]
or, by definition of the \(r'_i\),
\[
(d^2 - r_1) (d^2 - r_2) \cdots (d^2 - r_n) s_1 s_2 \cdots s_{l'} \equiv \prod_{1 \leq \alpha \leq (d^2 - 1)/2 \atop (d, \alpha) = 1} \alpha,
\]
yielding the congruence

\[ (-1)^n r_1 r_2 \cdots r_n s_1 s_2 \cdots s_r \equiv \prod_{1 \leq \alpha \leq (d^2-1)/2} \alpha \quad (\text{mod } d^2). \]

Now we rewrite (19) with the \( r_i \) and the \( s_j \) in their original form, with some possible rearrangement, to get

\[ (cd + 1)^{d(d-1)/2} \equiv (-1)^n \quad (\text{mod } d^2). \]

But by the binomial theorem,

\[ (cd + 1)^{d(d-1)/2} = 1 + \frac{d(d-1)}{2} cd \equiv 1 \quad (\text{mod } d^2). \]

From (21) and (22), we deduce that \( n \) is even and the proof of the claim is complete. And thus, from (14), we have

\[ S_4(d^2, cd + 1) \equiv cd \quad (\text{mod } 8). \]

We now assemble Theorem 3, Corollary 1, and Lemma 2 to reach our reciprocity result.

**Theorem 3.** Let \( d \) be an odd prime and \( c > d \) be an odd, positive integer coprime to \( d \). Then

\[ S_4(c, d) + S_4(d, c) \equiv -1 + cd \quad (\text{mod } 8). \]

3. THE LAW OF QUADRATIC RECIPROCITY

As an application of Theorem 4, we offer a new proof of the law of quadratic reciprocity.

**Theorem 4.** Let \( c \) and \( d \) be distinct odd primes. Then

\[ \left( \frac{c}{d} \right) \left( \frac{d}{c} \right) = (-1)^{\frac{c-1}{2} \frac{d-1}{2}}. \]
Proof. Given $c$ and $d$, there are integers $a$ and $b$ with $b$ even such that $ad - bc = 1$. Let $V = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ and $W = \begin{bmatrix} -b & -a \\ d & c \end{bmatrix}$. Note that $a$ is necessarily odd. From (3), (4) and recalling that $a$, $c$, and $d$ are odd and $b$ is even, we see that

\begin{equation}
\theta_{1+d,1-b}(Vz) = \theta_{1+d,1}(Vz) = (-1)^{(d+1)/2} \theta_{0,1}(Vz) = (-1)^{(d+1)/2} \theta_4(Vz),
\end{equation}

and

\begin{equation}
\theta_{1+c,1+a}(Wz) = \theta_{1+c,0}(Wz) = \theta_{0,0}(Wz) = \theta_3(Wz).
\end{equation}

From Theorem 1, (23) and (24), we have

\begin{equation}
\theta_4(Vz) = (-1)^{(-d-1)/2}(-i^b)e^{\pi i bd/4}
\end{equation}

\begin{equation}
\times \left( \frac{d}{c} \right)^{(c-3)/2} e^{\pi i (ac+dc)/4} \sqrt{\frac{cz + d}{i}} \theta_4(z)
\end{equation}

and

\begin{equation}
\theta_3(Wz) = -i^{-a}e^{-\pi i ac/4} \left( \frac{c}{d} \right)^{(d-3)/2} e^{\pi i (dc-bd)/4} \sqrt{\frac{dz + c}{i}} \theta_4(z).
\end{equation}

We also have, from (1) and (2),

\begin{equation}
\log \theta_4(Vz) = \log \theta_4(z) + \frac{1}{2} \log(cz + d) - \frac{1}{4} \pi i - \frac{1}{4} \pi i S_4(d,c)
\end{equation}

and

\begin{equation}
\log \theta_3(Wz) = \log \theta_4(z) + \frac{1}{2} \log(dz + c) - \frac{1}{4} \pi i - \frac{1}{4} \pi i S_4(c,d).
\end{equation}

Next, we multiply (25) and (26) and partially simplify the result to deduce that

\begin{equation}
\theta_4(Vz)\theta_3(Wz) = (-1)^{(-d-1)/2}i^{b-a}(c+d-6)/2e^{\pi i dc/2}z^{-1}
\end{equation}

\begin{equation}
\times \left( \frac{c}{d} \right) \left( \frac{d}{c} \right) \sqrt{cz + d\sqrt{dz + c}} \theta_4(z)^2.
\end{equation}

We exponentiate and then multiply (27) and (28) to see that

\begin{equation}
\theta_4(Vz)\theta_3(Wz) = \theta_4(z)^2\sqrt{cz + d\sqrt{dz + c}} e^{-\pi i/2}
\end{equation}

\begin{equation}
\times e^{-(\pi i/4)}(S_4(c,d) + S_4(d,c)).
\end{equation}
From (29), (30) and Lemma 1, we deduce that

\[ (-1)^{(d-1)/2}(b-2a+c+d-6)/2e^{\pi ide/2}\left(\frac{c}{d}\right)\left(\frac{d}{c}\right) = e^{-\pi i/2}e^{-(\pi i/4)}(S_4(c, d) + S_4(d, c)). \]

Next, we simplify (31) to find that

\[ e^{(\pi i/4)(-2a+2b+c-d^2+2cd)}\left(\frac{c}{d}\right)\left(\frac{d}{c}\right) = e^{-(\pi i/4)}(S_4(c, d) + S_4(d, c)). \]

Note that since \(d\) is odd and \(ad-bc = 1\), we have that \(a \equiv d + dbc \pmod{8}\). From this fact and the application of Theorem 3 to (32), we conclude that

\[ \left(\frac{c}{d}\right)\left(\frac{d}{c}\right) = e^{(\pi i/4)(3d-2c-2b+2bc-d^2-3cd+1)}. \]

A straight-forward calculation shows that

\[ 3d-c-2b+2bcd-3cd+1 \equiv (c-1)(d-1) \pmod{8}. \]

Using (34) in (33), we deduce that

\[ \left(\frac{c}{d}\right)\left(\frac{d}{c}\right) = e^{(\pi i/4)(c-1)(d-1)} = (-1)^{\frac{c-1}{2}\frac{d-1}{2}} \]

as desired.

\[ \square \]

REFERENCES


