Triple Product Identities for the Jacobi Symbol

Kurt Girstmair

Institut für Mathematik, Universität Innsbruck, Technikerstrasse 25/7, A-6020 Innsbruck, Austria

Introduction

Let $n$ be an odd natural number and $m$ an integer with $(m, n) = 1$. The Jacobi symbol $\left(\frac{m}{n}\right)$ generalizes the Legendre symbol in the following way: If $n$ is the product $n = p_1 \ldots p_k$ of (not necessarily distinct) primes $p_j$, then

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right) \cdots \left(\frac{m}{p_k}\right).$$

This definition includes the case $\left(\frac{m}{1}\right) = 1$ (cf. [8], p. 47). The reciprocity law

$$\left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = (-1)^{(m-1)(n-1)/4}$$

holds for odd natural numbers $m, n$ — so it is an obvious analogue of the reciprocity law for the Legendre symbol (ibid., p. 50).

The subsequent Theorem 1 contains two triple product identities which generalize (1) and might be of interest for a wider public. These identities are not completely new but implicit in the literature. Indeed, they arise in a fairly canonical way in the (analytical) context of theta multipliers. It seems, however, that a simple arithmetical proof of them has not been given so far. In Section 1 we fill this gap and derive this result directly from (1). In Section 2 we outline the said technique of theta multipliers. Further, we reduce an apparently more complicated identity of the literature (cf. [1]) to the second identity of Theorem 1. Section 3 contains a sketch of a logarithmic approach via Dedekind sums. This approach leads to another but less direct arithmetical proof of Theorem 1, which can be compiled from known results.

Theorem 1 Let $I$ denote the unit matrix in $\text{SL}(2, \mathbb{Z})$. Further, let

$$A_j = \begin{pmatrix} a_j & b_j \\ c_j & d_j \end{pmatrix}, \quad j = 1, 2, 3,$$

E-mail address: Kurt.Girstmair@uibk.ac.at

0732-0869/01/19/2-179 $15.00/0
be matrices in $\text{SL}(2, \mathbb{Z})$ such that $c_j$, $j = 1, 2, 3$, are odd natural numbers. If $A_1A_2A_3 = -I$, then

$$
\begin{pmatrix}
\frac{a_1}{c_1} \\
\frac{a_2}{c_2} \\
\frac{a_3}{c_3}
\end{pmatrix} = (-1)^{(c_1-1)(c_2-1)/4+(c_1-1)(c_3-1)/4+(c_2-1)(c_3-1)/4}.
$$

If, instead, $A_1A_2A_3 = I$, then the right side of (2) has to be replaced by

$$
(-1)^{(c_1c_2+c_1c_3+c_2c_3-3)/4}.
$$

Because of

$$a_j d_j - b_j c_j = 1, \ j = 1, 2, 3,$$

each number $d_j$ is a (multiplicative) inverse of $a_j$ mod $c_j$. Accordingly,

$$
\begin{pmatrix}
\frac{d_j}{c_j}
\end{pmatrix} = \begin{pmatrix}
\frac{a_j}{c_j}
\end{pmatrix}
$$

and the identities of Theorem 1 remain valid whenever one of the entries $a_j$ on the right side is replaced by the respective number $d_j$, $j = 1, 2, 3$. Each of these identities contains the reciprocity law (1). Suppose, for instance, $A_1A_2A_3 = -I$. By means of matrix multiplications and inversions one verifies that this requires

$$c_1 = c_2 a_3 + d_2 c_3, \ c_2 = c_3 a_1 + d_3 c_1, \ c_3 = c_1 a_2 + d_1 c_2.$$

Therefore, if $c_3 = 1$, say, the third equation in (6) shows that $c_2$ is an inverse of $d_1$ mod $c_1$, i.e., $c_2 \equiv a_1$ mod $c_1$; in the same way $c_1$ is an inverse of $a_2$ mod $c_2$, and (2) comes down to (1).

1. An arithmetical proof of Theorem 1

We restrict ourselves to the case when $A_1A_2A_3 = -I$, the other case being quite similar. From (6) one concludes that the greatest common divisors $(c_1,c_2)$, $(c_1,c_3)$, $(c_2,c_3)$ are all equal. Let $\delta$ denote this common divisor. We distinguish two cases:

Case 1: $\delta = 1$. The relations (6) entail $c_3 a_1 \equiv c_2$ mod $c_1$, $c_1 a_2 \equiv c_3$ mod $c_2$, $c_2 a_3 \equiv c_1$ mod $c_3$, whence

$$
\begin{pmatrix}
\frac{a_1}{c_1}
\end{pmatrix} = \begin{pmatrix}
\frac{c_3}{c_1}
\end{pmatrix} \begin{pmatrix}
\frac{c_2}{c_1}
\end{pmatrix}, \quad \begin{pmatrix}
\frac{a_2}{c_2}
\end{pmatrix} = \begin{pmatrix}
\frac{c_1}{c_2}
\end{pmatrix} \begin{pmatrix}
\frac{c_3}{c_2}
\end{pmatrix}, \quad \begin{pmatrix}
\frac{a_3}{c_3}
\end{pmatrix} = \begin{pmatrix}
\frac{c_2}{c_3}
\end{pmatrix} \begin{pmatrix}
\frac{c_1}{c_3}
\end{pmatrix}
$$
follow by multiplicative inversion. If one expands the left side of (2) in this way and applies the reciprocity law (1), one obtains the right side.

Case 2: $\delta > 1$. We write $c_j = c'_j \delta$, $j = 1, 2, 3$, where the natural numbers $c'_j$ are pairwise relatively prime. Thus,

$$
\left( \frac{a_1}{c_1} \right) \left( \frac{a_2}{c_2} \right) \left( \frac{a_3}{c_3} \right) = \left( \frac{a_1}{c'_1} \right) \left( \frac{a_2}{c'_2} \right) \left( \frac{a_3}{c'_3} \right) \left( \frac{a_1 a_2 a_3}{\delta} \right). \tag{7}
$$

Now $A_1 A_2 A_3 = -I$ implies $-a_3 = c_1 b_2 + d_1 d_2$, i.e., $a_3 \equiv -d_1 d_2 \quad \text{mod} \quad \delta$. Since $\delta$ divides $c_1$ and $c_2$, (4) says that $d_1$, $d_2$ are inverses of $a_1$, $a_2 \quad \text{mod} \quad \delta$, respectively. Altogether, $a_1 a_2 a_3 \equiv -1 \quad \text{mod} \quad \delta$ and the last symbol in (7) reads

$$
\left( \frac{a_1 a_2 a_3}{\delta} \right) = \left( \frac{-1}{\delta} \right) = (-1)^{(\delta-1)/2}. \tag{8}
$$

On the other hand, the matrices

$$
A'_j = \left( \begin{array}{cc} a_j & b_j \\ c'_j & d_j \end{array} \right)
$$

are obviously in $SL(2, \mathbb{Z})$ and $A'_1 A'_2 A'_3 = -I$. So they fall under Case 1, which we have settled already. Hence,

$$
\left( \frac{a_1}{c'_1} \right) \left( \frac{a_2}{c'_2} \right) \left( \frac{a_3}{c'_3} \right) = (-1)^{(c'_1 -1)(c'_2 -1)/4 + (c'_3 -1)/4 + (c'_4 -1)/4 + (c'_5 -1)/4 + (c'_6 -1)/4}.
$$

In view of (7) and (8), we only have to verify the congruence

$$(c_1 -1)(c_2 -1) + (c_1 -1)(c_3 -1) + (c_2 -1)(c_3 -1) \equiv (c'_1 -1)(c'_2 -1) + (c'_3 -1)(c'_4 -1) + (c'_5 -1)(c'_6 -1) + 2\delta - 2 \quad \text{mod} \quad 8$$

now. This is a short calculation based on $\delta^2 \equiv 1 \quad \text{mod} \quad 8$ and

$$
2mn \equiv 2m + 2n - 2 \quad \text{mod} \quad 8, \tag{9}
$$

which holds for arbitrary odd integers $m$, $n$.

### 2. Theta multipliers

Consider the theta series

$$
\theta(z) = \sum_{n=0}^{\infty} (-1)^n q^{(n+1/2)^2}
$$
with $q = e^{\pi iz}$. The series converges for every $z$ in the upper half plane \( \{ z \in \mathbb{C} : \text{Im} \ z > 0 \} \) and defines a modular form of weight 1/2. Accordingly, it has a certain transformation behaviour, which can be found, e.g., in [9], p. 180. For a matrix
\[
A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}),
\]
put $A \circ z = (az + b)/(cz + d)$. If, in particular, $c$ is a natural number, then
\[
\theta(A \circ z) = \left( \frac{d}{c} \right) e^{\pi i(c(a + d + 1) - 3)/4} \sqrt{\frac{cz + d}{i}} \theta(z) \quad (10)
\]
holds for all $z$ with $\text{Im} \ z > 0$ (ibid.). Here the square root of a complex number $w \notin \{ z \in \mathbb{R} : z \leq 0 \}$ is defined by $\sqrt{w} = |w|^{1/2} e^{i \arg(w)/2}$, $\arg(w) \in (-\pi, \pi)$. In other words, the transformation of $\theta(z)$ involves a multiplier that is independent of $z$ and consists of a Jacobi symbol and an eighth root of unity.

Suppose now that $A_1 A_2 A_3 = -I$, i.e., $-A_3^{-1} = A_1 A_2$. Then (10), applied to each of $\theta(-A_3^{-1} \circ z)$ and $\theta(A_1 \circ (A_2 \circ z))$ yields
\[
\left( \begin{array}{c} d_1 \\ c_1 \\ c_2 \\ c_3 \end{array} \right) = e^{\pi i(2 + \sum_{j=1}^{3} c_j(a_j + d_j + 1))/4} \quad (11)
\]
(observe that the square roots require some care). From (5) one sees that the right sides of (11) and (2) must be equal. We give, however, an independent proof of this fact in order to make the proof of Theorem 1 by means of theta multipliers self-contained. To this end we consider the congruence class mod 8 of the exponent
\[
e = 2 + \sum_{j=1}^{3} c_j(a_j + d_j + 1).
\]
From (11) it is clear that $e \equiv 0 \mod 4$, so its congruence class mod 8 does not change if it is multiplied by the odd number $c_1 c_2 c_3$. Using $c_j^2 \equiv 1 \mod 8$ we obtain
\[
e \equiv 2c_1 c_2 c_3 + c_2 c_3(a_1 + d_1 + 1) + c_1 c_3(a_2 + d_2 + 1) + c_1 c_2(a_3 + d_3 + 1) \quad (12)
\]
mod 8. By (6), $c_2 c_3 a_1 = c_2^2 - c_1 c_2 d_3$, $c_1 c_3 a_2 = c_3^2 - c_2 c_3 d_1$, $c_1 c_2 a_3 = c_1^2 - c_1 c_3 d_2$; accordingly, the right side of (12) is reduced to $2c_1 c_2 c_3 + 3 + c_1 c_2 + c_1 c_3 + c_2 c_3$ mod 8. Now for an odd number $m$, $2m \equiv 4 - 2m \mod 8$. If one applies this congruence and, afterwards, (9) to the first term $2c_1 c_2 c_3$, one has
\[
e \equiv c_1 c_2 + c_1 c_3 + c_2 c_3 - 2c_1 - 2c_2 - 2c_3 + 3 \mod 8.
\]
The assertion is clear if one compares this expression with the exponent on the right side of (2).

The paper [1] contains the exact equivalent of (11) in the case $A_1A_2A_3 = I$, its corresponding right hand side being

$$e^{\pi i (4 + \sum_{j=1}^{3} c_j (a_j + d_j - 3))/4}$$

Of course, this number can be brought to the simpler form (3) by the same kind of argument. The said article does not give a proof but refers to [6], an extended Japanese version of [7]. The lastmentioned work is based on the method of this section and contains, as a by-product of other results, an analogous (but more involved) identity for matrices $A_1, A_2, A_3$ such that $A_j \equiv I \mod 4, j = 1, 2$ and $A_1A_2 = A_3$. The author says, in his own words, that a purely arithmetical proof of this formula is possible but rather complicated; cf. also [5]. The paper [3] is more general in some sense but in the same spirit.

One should also consult [5], where $m$th power residue symbols, $m \geq 2$, are attached to matrices over purely imaginary number fields containing a primitive $m$th root of unity. Surprisingly, this situation is better than the present one inasmuch as the symbols define a group homomorphism of a certain matrix group and not only a near homomorphism with properties like Theorem 1.

3. Dedekind sums

In some sense deeper than the method of theta multipliers lies the approach via Dedekind sums

$$s(a, c) = \sum_{k=1}^{c-1} ((k/c))((ka/c));$$

here $a, c$ are relatively prime integers, $c > 0$, and $((x)) = x - \lfloor x \rfloor - 1/2$. These sums occur in the transformation formula of the logarithm $\log \eta(z)$ of Dedekind's eta function $\eta(z)$, cf. [9], p. 145. Since $\eta(z)$ is also a modular form of weight $1/2$, this transformation formula can be regarded as a logarithmic analogue of (10). It leads to the following analogue of (2) which was first observed in [2], as it seems. Let $A_j \in SL(2, \mathbb{Z}), j = 1, 2, 3$, be as in Theorem 1 such that $A_1A_2A_3 = -I$. Then

$$12 \sum_{j=1}^{3} s(a_j, c_j) = \frac{c_1^2 + c_2^2 + c_3^2}{c_1c_2c_3} - 3. \tag{13}$$
It is not hard to obtain (2) from (13) if one knows that \( s(a, c) \) is also a kind of logarithm, namely, of the respective Jacobi symbol. More precisely, \( 6c \cdot s(a, c) \) is an integer and for each odd natural number \( c \)

\[
\left( \frac{a}{c} \right) = e^{\pi i (c-1 - 12c \cdot s(a,c))/4}.
\]

(14)

The relation (14) goes back to Dedekind; it is often rendered as a congruence mod 8 for the (even) integers \( 2^{(a)} \) and \( 12c \cdot s(a, c) \), cf. [9], p. 160. Now (2) quickly follows from (13) and (14) by means of congruence considerations mod 8 like those of Section 2.

It has been observed that (13) can be deduced from the definition of the Dedekind sums in a purely arithmetical way (cf. [1], [4]). For this purpose one uses the reciprocity law for Dedekind sums, of which, in turn, purely arithmetical proofs are known (cf. [9], p. 148 ff.). Since (14) is also of a purely arithmetic nature (ibid., p. 157 ff.), one may say that another arithmetical proof of (2) can be put together from results of the literature. Compared with Section 1, however, a proof of this kind is a detour.

**Acknowledgement**

The author would like to thank R. Sczech for his most valuable comments. Above all, Section 2 is largely based on his hints.

**References**


Received: 29.01.2001
Revised: 12.03.2001