# EVALUATING SYMPLECTIC GAUSS SUMS AND JACOBI SYMBOLS

#### ROBERT STYER

#### §1. Introduction

Stark [9] has explicitly evaluated some symplectic Gauss sums when the "denominator" matrix has odd prime level. This result is useful in computing the exact transformation formulas of multivariable theta functions (see Stark [10], Friedberg [3] and Styer [11]). It is particularly useful when considering theta functions with quadratic forms having an odd number of variables, often a troublesome case (see Eichler [2] and Andrianov-Maloletkin [1]).

Stark restricted his evaluation to symplectic Gauss sums with odd prime level denominators. In this paper, we find results analogous to the classical "reduction" theorems that allow one to decompose a Gauss sum into ones with odd prime level or level 4 or 8. To compute Gauss sums with denominators of even level, we must define 4-signatures and 8-signatures of certain submatrices. These signatures involve invariants which are more subtle than the determinants used in the odd prime level case.

Consideration of Gauss sums naturally suggests the concept of Jacobi symbols. We define a symplectic Jacobi symbol, verify a number of expected properties, and finally state a reciprocity law for this symbol.

In the final section, we apply our results to extend a theorem of Stark [10] calculating the transformation formulas for theta functions over algebraic number fields. Stark did the case when the lower right corner of the transformation matrix is odd, but not when it is even. By introducing the concept of 4-signatures for algebraic integers, we are able to handle the general case. We end with a brief comment referring to Andrianov and Maloletkin's paper [1] concerning theta functions with quadratic forms. We evaluate the multiplier system when the quadratic

Received August 4, 1982.

form has an odd number of variables, illustrating the usefulness of our results on the symplectic Gauss sum and symplectic Jacobi symbol.

# §2. The symplectic Gauss sum

Multivariate Gauss sums appear in the literature as far back as 1872 (see Weber [12]). We, however, will give the definition used by Stark [9].

Maass [7] defines coprime symmetric pairs of  $n \times n$  integral matrices (C, D) and shows that a pair is coprime symmetric iff it can be completed to give a symplectic matrix whose lower "row" is (C, D), The pair (C, D) is called an even symmetric pair if  $D^{\iota}C$  is an even symmetric matrix, that is, an integral symmetric matrix with even diagonal elements. We will be interested in coprime even symmetric pairs (C, D) with  $\det D \neq 0$ . For convenience, we will abbreviate "coprime even symmetric with  $\det D \neq 0$ " by CESD.

Given (C, D) CESD, and given  $m \in \mathbb{Z}^n$ , the symplectic Gauss sum is defined by:

$$G_{\scriptscriptstyle D}(C) = \sum\limits_{\substack{m \bmod t_D}} e({}^t m D^{\scriptscriptstyle -1} C m) \; .$$

Here  $e(x) = \exp \{\pi i x\}$  and  $m_1 \equiv m_2 \mod {}^t D$  iff  $m_1 - m_2 = {}^t D m_0$  for some  $m_0 \in \mathbb{Z}^n$ . One can easily show that a complete set of representatives  $m \mod {}^t D$  has  $|\det D|$  members.

In the classical case, one reduces the explicit calculation of the Gauss sum to the case where the denominator D is either prime or 4. With matrices, the concept of "prime" is replaced by "prime level." Given (C, D) CESD, the martix D is said to have level d if d is the least positive integer such that  $dD^{-1}C$  is an integral even symmetric matrix. Since (C, D) is coprime even, this means that d is precisely the highest invariant factor d' of D whenever d' is odd. (See Newman [8] for definitions). If d' is even, however, the level d is 2d'. In any event, the level d does not depend on C.

The following theorem is exactly analogous to the classical reciprocity law; this version follows Stark.

Theorem 1 (Reciprocity Law). Let (C,D) be CESD and suppose that  $\det C \neq 0$ . Then

$$rac{G_{\scriptscriptstyle D}\!(C)}{|\det D|^{^{1/2}}} = e \Big\{ rac{1}{4} \, {
m sgn}\,(D^{\scriptscriptstyle t} C) \Big\} \cdot rac{G_{\scriptscriptstyle C}\!(-D)}{|\det C|^{^{1/2}}} \,\, .$$

Here sgn  $D^tC$  is the usual signature of a symmetric matrix.

The following lemma will simplify later calculations.

Lemma 1. (a) Let (C, D) be CESD and assume that

$$D=egin{pmatrix} D_1 & 0 \ 0 & D_2 \end{pmatrix}$$
 and  $C=egin{pmatrix} C_1 & C_2 \ C_3 & C_4 \end{pmatrix}$  with

 $D_1$  and  $C_1$  being the same size. Suppose that  $(C_4, D_2)$  is CESD, and thus there exists an integral matrix we denote  $C_4^*$  such that  $C_4C_4^* = I + DM_2$  with  $({}^tC_4^*, {}^tM)$  CESD. Then

$$G_D(C) = G_{D_1}(C_1 - C_2C_4^*C_3) \cdot G_{D_2}(C_4)$$
.

(b) If  $D_2$  is unimodular, then

$$G_D(C) = G_{D_1}(C_1)$$
.

(c)  $C_2 = 0$  iff  $C_3 = 0$  in which case

$$G_D(C) = G_{D_1}(C_1)G_{D_2}(C_4)$$
.

*Proof.* The condition (C, D) CESD implies that  $D_1^{-1}C_1$  and  $D_2^{-1}C_4$  are symmetric and that  $D_1^{-1}C_2 = {}^{\iota}(D_2^{-1}C_3)$ . Maass [7] shows that any coprime symmetric pair can be completed to give a matrix in the symplectic group, and similarly  $({}^{\iota}C_4^*, {}^{\iota}M)$  exists.

In general,  $G_{\scriptscriptstyle D}(C)=G_{\scriptscriptstyle U\,\scriptscriptstyle D^{\scriptscriptstyle Y}}(UC^{\iota}\,V^{-1})$  for unimodular matrices U and V. We will take U=I and  ${}^{\iota}V=\Big(\frac{I}{C_{\star}^{\prime}\,C_{\star}^{\prime}}\Big|\frac{0}{I}\Big)$ . Then

$$egin{aligned} G_{\scriptscriptstyle D}(C) &= \sum_{m_1 mod t_{D_2} top 1 \ m_2 mod t_{D_2}} e \Big\{ ({}^t m_1{}^t m_2) \Big[ \Big(rac{I}{0} igg| rac{-{}^t C_3{}^t C_4^*}{I} \Big) igg( egin{aligned} D_1^{-1} & 0 \ 0 & D_2^{-1} \end{matrix} \Big) \ & \cdot igg( egin{aligned} C_1 & C_2 \ C_3 & C_4 \end{matrix} igg( rac{I}{-C_4^* C_3} igg| rac{0}{I} igg) \Big] igg( m{m_1} \ m_2 \end{matrix} igg) \Big\} \;. \end{aligned}$$

Consider the matrix product in brackets. One can multiply this out and use the relations and symmetry conditions to simplify the product. After tedious but trivial calculations, one gets

$$\left(rac{D_1^{-1}(C_1-C_2C_4^*C_3)+ {}^tC_3{}^tC_4^*MC_3}{-MC_3} \left|rac{-{}^tC_3{}^tM}{D_2^{-1}C_4}
ight).$$

When we put this back into the Gauss sum and notice that

$$e\{{}^{t}m_{1}{}^{t}C_{3}{}^{t}C_{4}^{*}MC_{3}m_{1}\}=e\{2{}^{t}m_{2}MC_{3}m_{1}\}=1,$$

we obtain the desired result for part (a).

Part (b) is an immediate corollary of (a) by taking  $C_4^* = 0$  and  $M = D_2^{-1}$ .

Part (c) is also an immediate consequence of the relations used in the proof of (a), since  $(C_4, D_2)$  will be CESD. In fact, it is easy to show that the hypotheses of (c) may be weakened to either  $D_1^{-1}C_2$  or  $D_2^{-1}C_3$  integral. This concludes the proof of Lemma 1.

The next theorem is the heart of Stark's calculation of the explicit transformation formulas for theta functions [9].

Theorem 2 (Stark). Let (C, D) be CESD, and suppose that level D = p, p an odd prime. Let  $\det D = \pm p^k$  for some  $1 \le k \le n$  and define  $(pD^{-1}C)^{(k)}$  to be any  $k \times k$  principal submatrix with non-zero determinant  $\mod p$ . Then

$$G_{\scriptscriptstyle D}\!(C) = arepsilon_{\scriptscriptstyle p}^{\scriptscriptstyle k}\!\!\left(rac{\det{(2pD^{\scriptscriptstyle -1}C)^{\scriptscriptstyle (k)}}}{p}
ight)\!p^{\scriptscriptstyle k/2} \,.$$

Here  $\varepsilon_p = 1$  if  $p \equiv 1 \mod 4$  and  $\varepsilon_p = i$  if  $p \equiv -1 \mod 4$ .

A crucial idea in Stark's proof is to "diagonalize"  $pD^{-1}C$  modulo p. One then uses Lemma 1 (c) to reduce the multivariable Gauss sum to a product of classical Gauss sums. Diagonalization essentially involves the Smith normal form (see Newman [9]) and we will also use this important tool. The Smith normal form says that there exist unimodular matrices U and V such that  $UDV = \operatorname{diag}(d_1, d_2, \dots, d_n)$  with the invariant factors  $d_i$  satisfying  $d_1|d_2|\cdots|d_n$ . One can easily verify that (C, D) CESD implies that  $(UC^iV^{-1}, UDV)$  is CESD, and

$$G_{\scriptscriptstyle D}(C) = G_{\scriptscriptstyle UDV}(UC^{\scriptscriptstyle t}\,V^{\scriptscriptstyle -1})$$
 .

In the classical case, one reduces the Gauss sums to be prime powers. This theorem is the analogy in the symplectic case.

THEOREM 3. (a) Let (C, D) be CESD and suppose that  $D = D_1D_2 = D_2'D_1'$  with  $|\det D_1| = |\det D_1'|$ . Suppose that there exist matrices  $R_1, R_1', R_2, R_2'$ , such that  $D_1R_1 + D_2'R_2' = I$  and  $R_1'D_1' + R_2D_2 = I$ . Further assume that  $R_2D_1^{-1}C^tD_1'^tR_1'$  is an integral matrix.

Then

$$G_D(C) = G_{D_1}(C^tD_2) \cdot G_{D_2'}(C^tD_1')$$
.

(b) Suppose  $D = D_1D_2$  with (level  $D_1$ , level  $D_2$ ) = 1. Then there exists

suitable  $D'_1$  and  $D'_2$  such that this equation of Gauss sums is true for any C with (C, D) CESD.

*Proof.* Let  $m_1 \mod {}^tD_1'$  and  $m_2 \mod {}^tD_2$  be complete sets of representatives. We claim that  ${}^tD_2{}^tR_2m_1 + {}^tD_1'{}^tR_1'm_2$  is a complete set of representatives mod  ${}^tD$ . Since  $|\det D| = |\det D_1'| \cdot |\det D_2|$ , we need only show that  ${}^tD_2{}^tR_2m_1 + {}^tD_1'{}^tR_1'm_2 \equiv 0 \mod {}^tD$  implies that  $m_1 \equiv 0 \mod {}^tD_1'$  and  $m_2 \equiv 0 \mod {}^tD_2$ . Let  ${}^tD_2{}^tR_2m_1 + {}^tD_1'{}^tR_1'm_2 = {}^tDm_0$  for some  $m_0 \in \mathbb{Z}^n$ . Then  ${}^tD_2{}^tR_2m_1 + (I - {}^tD_2{}^tR_2)m_2 = {}^tD_2{}^tD_1m_0$ . Thus,  $m_2 \equiv 0 \mod {}^tD_2$ . Similarly, one shows that  $m_1 \equiv 0 \mod {}^tD_1'$ .

Choose the  $m \mod {}^tD$  to be this set  ${}^tD_2{}^tR_2m_1 + {}^tD_1{}^{\prime}{}^tR_1{}^{\prime}m_2$ . Then

$$\begin{split} G_D(C) &= \sum_{\substack{m \bmod{}^t D_1}} e\{{}^t m D^{-1} C m\} = \sum_{\substack{m_1 \bmod{}^t D_1' \bmod{}^t D_2' \bmod{}^t D_2}} \\ & \cdot e\{{}^t ({}^t D_2{}^t R_2 m_1 + {}^t D_1'{}^t R_1' m_2) \cdot D^{-1} C({}^t D_2{}^t R_2 m_1 + {}^t D_1'{}^t R_1' m_2)\} \\ &= \sum_{\substack{m_1 \bmod{}^t D_1' \bmod{}^t D_2' \bmod{}^t D_2}} \sum_{\substack{m_2 \bmod{}^t D_2' \end{bmatrix}} e({}^t m_1 R_2 D_2 D^{-1} C^t D_2{}^t R_2 m_1) \\ & \cdot e({}^t m_1 R_2 D_2 D^{-1} C^t D_1'{}^t R_1' m_2) \cdot e({}^t m_2 R_1' D_1'{}^t C^t D^{-1}{}^t D_2{}^t R_2 m_1) \\ & \cdot e({}^t m_2 R_1' D_1' D^{-1} C^t D_1'{}^t R_1' m_2) \\ &= \sum_{\substack{m_1 \bmod{}^t D_1' \\ m_2 \bmod{}^t D_2'}} e({}^t m_1 R_2 D_1^{-1} C^t D_2{}^t R_2 m_1) \\ & \cdot \sum_{\substack{m_2 \bmod{}^t D_2' \\ m_2 \bmod{}^t D_2'}} e({}^t m_2 R_1' D_2'^{-1} C^t D_1'{}^t R_1' m_2) \;. \end{split}$$

Here we have used the hypothesis that  $R_2D_1^{-1}C^tD_1^{\prime t}R_1^{\prime}={}^t(R_1^{\prime}D_1^{\prime t}C^tD_1^{-1}{}^tR_2)$  is an integral matrix.

We will now show that  $m_1$  is a complete set of representatives  $\operatorname{mod}{}^{i}D_1'$  iff  ${}^{i}R_2m_1$  is a complete set of representatives  $\operatorname{mod}{}^{i}D_1$ . Since  $|\det D_1| = |\det D_1'|$ , we need only show that  ${}^{i}R_2m_1 \equiv 0 \operatorname{mod}{}^{i}D_1$  implies that  $m_1 \equiv 0 \operatorname{mod}{}^{i}D_1'$ . Let  ${}^{i}R_2m_1 = {}^{i}D_1m_0$  for some  $m_0 \in \mathbb{Z}^n$ . Multiply both sides by  ${}^{i}D_2$  and use the hypotheses to obtain  $(I - {}^{i}D_1'{}^{i}R_1')m_1 = {}^{i}D_1'{}^{i}D_2'm_0$ , from which one deduces that  $m_1 \equiv 0 \operatorname{mod}{}^{i}D_1'$ . A very similar argument shows that  $m_2 \operatorname{mod}{}^{i}D_2$  is a complete set of representatives iff  ${}^{i}R_1'm_2 \operatorname{mod}{}^{i}D_2'$  is a complete set of representatives. Applying these facts to the two exponential sums above, we get the desired Gauss sums.

For the proof of (b), let  $D = D_1D_2$  with  $d_1 = \text{level }D_1$  and  $d_2 = \text{level }D_2$ . Choose unimodular matrices U and V such that UDV is diagonal; thus,  $UDV = {}^tV^tD^tU$ . Define  $D_2' = U^{-1t}V^tD_2$  and  $D_1' = {}^tD_1{}^tUV^{-1}$ ; clearly  $D = D_2'D_1'$  and  $|\det D_1| = |\det D_1'|$ . Since by hypothesis  $(d_1, d_2) = 1$ , there exist  $r_1, r_2 \in Z$  with  $d_1r_1 + d_2r_2 = 1$ . Define  $R_1 = r_1d_1D_1^{-1}$ ,  $R_1' = r_1d_1D_1'^{-1}$ ,  $R_2 = r_2d_2D_2^{-1}$ , and  $R_2' = r_2d_2D_2'^{-1}$ . Clearly  $D_1R_1 + D_2'R_2' = R_1'D_1' + R_2D_2 = I$ . Also,

 $R_2D_1^{-1}C^tD_1^{\prime t}R_1 = R_2r_1d_1D_1^{-1}C$  is integral for any C, hence we can apply part (a) to conclude the proof of this theorem.

The next step in the classical case is to reduce prime power Gauss sums to prime Gauss sums. The following theorem is the analogy in the symplectic case.

THEOREM 4. (a) Let (C, D) be CESD and let  $C = C_1C_2C_1'$  with  $C_1, C_2$ , and  $C_1'$  integral matrices. Let  $D_2$  satisfy  $C_1D_2 = D^tC_1'$  and  $|\det D_2| = |\det D|$ . If  $(C_2, D_2)$  is CESD, then

$$G_{\scriptscriptstyle D}(C) = G_{\scriptscriptstyle D_2}(C_{\scriptscriptstyle 2}) .$$

(b) Let (C, D) be CESD and let  $D = D_1D_2D_1'$  with  $D_1, D_2$ , and  $D_1'$  integral matrices satisfying  $|\det D_1| = |\det D_1'|$ . Define  $C_2 = D_1^{-1}C^tD_1'$ . If  $(C_2, D_2)$  is CESD, then

$$G_{\mathcal{D}}(C) = |\det D_1| \ G_{\mathcal{D}_2}(C_2) \ .$$

(c) Let (C, D) be CESD. Then there exists an integral decomposition  $D = D_1D_2D_1'$  with  $|\det D_1| = |\det D_1'|$  and  $(C_2, D_2)$  CESD. Furthermore, if level D is odd, then level  $D_2$  is an odd squarefree integer, and if level D is even, then level  $D_2$  is either four or eight times an odd squarefree integer.

Proof of (a).

$$G_{\scriptscriptstyle D}(C) = \sum_{m \bmod {}^t D} e({}^t m D^{\scriptscriptstyle -1} C_{\scriptscriptstyle 1} C_{\scriptscriptstyle 2} C_{\scriptscriptstyle 1}' m) = \sum_{m \bmod {}^t D} e({}^t m^{\scriptscriptstyle t} C_{\scriptscriptstyle 1}' D_{\scriptscriptstyle 2}^{\scriptscriptstyle -1} C_{\scriptscriptstyle 2} C_{\scriptscriptstyle 1}' m) \;.$$

We will be done if we show that  $m \mod {}^{\iota}D$  is a complete set of representatives iff  $C'_1m \mod {}^{\iota}D_2$  is a complete set of representatives. Let  $m = {}^{\iota}Dm_0$  for some  $m_0 \in \mathbb{Z}^n$ . Then  $C'_1m = C'_1{}^{\iota}Dm_0 = {}^{\iota}D_2({}^{\iota}C_1m_0)$  so  $C'_1m_0 \equiv 0 \mod {}^{\iota}D_2$ . This finishes the proof of (a).

If det  $C \neq 0$ , we may use the reciprocity law to get a proof of (b). For when det  $C \neq 0$ , we have the following equalities by applying Theorem 1 and part (a) above.

$$egin{aligned} G_{\scriptscriptstyle D}(C) &= e\{rac{1}{4} \operatorname{sgn} \left(D^{\iota}C
ight)\}\{\det C^{-1}D\}^{1/2}G_{\scriptscriptstyle C}(-D) \ &= e\{rac{1}{4} \operatorname{sgn} \left(D^{\iota}C
ight)\}\{\det C^{-1}D\}^{1/2}G_{\scriptscriptstyle C_2}(-D_2) \ &= e\{rac{1}{4} \left[\operatorname{sgn} \left(D^{\iota}C
ight) - \operatorname{sgn} \left(D_2^{\,\iota}C_2
ight)\right]\}|\det C^{-1}D|^{1/2}|\det D_2^{-1}C_2|^{1/2}\cdot G_{\scriptscriptstyle D_2}(C_2) \ &= |\det D_1| \, G_{\scriptscriptstyle D_2}(C_2) \;. \end{aligned}$$

If det C=0, tedious but straightforward unimodular transformations reduce us to the above case. Choose unimodular matrices U and V such that

$$UDV = egin{pmatrix} D^* & 0 \ 0 & I \end{pmatrix}$$
 and  $UC^tV^{-1} = egin{pmatrix} C^* & 0 \ 0 & 0 \end{pmatrix}$ 

with det  $C^* \neq 0$ . (See Maass [7]). Choose unimodular U' and V' such that

$$U'D_2V'=egin{pmatrix} D_2^* & 0 \ 0 & I \end{pmatrix} \quad ext{and} \quad U'C_2{}^tV'^{-1}=egin{pmatrix} C_2^* & 0 \ 0 & 0 \end{pmatrix}$$

with det  $C_2^* \neq 0$ . Since rank  $C = \text{rank } C_2$ , one easily verifies that  $D^*$ ,  $D_2^*$ ,  $C^*$ , and  $C_2^*$  are all the same size.

Let  $\tilde{D}_1 = U^{-1}D_1U'$  and  $\tilde{D}_1' = V'D_1'V^{-1}$ . One can check that

$$\begin{pmatrix} C_2^* & 0 \\ 0 & 0 \end{pmatrix} = \tilde{D}_1^{-1} \! \begin{pmatrix} C^* & 0 \\ 0 & 0 \end{pmatrix}^t \! \tilde{D}_1' \quad \text{and} \quad \begin{pmatrix} D^* & 0 \\ 0 & I \end{pmatrix} = \tilde{D}_1 \! \begin{pmatrix} D_2^* & 0 \\ 0 & I \end{pmatrix} \! \tilde{D}_1' \; .$$

Matrix multiplication shows that  $\tilde{D}_1$  and  $\tilde{D}_1'$  are of the forms

$$ilde{D_1} = egin{pmatrix} D_1^* & 0 \ 0 & W^{-1} \end{pmatrix} \quad ext{and} \quad ilde{D_1'} = egin{pmatrix} D_1'^* & 0 \ 0 & W^{-1} \end{pmatrix}$$

where  $D_1^*$  and  $D_1'^*$  are the same size as  $D^*$ , and W is a unimodular matrix which we may take to be I. We conclude that

$$G_{\scriptscriptstyle D}(C) = G_{\scriptscriptstyle D*}\!(C^*) = |\!\det D_{\scriptscriptstyle 1}^*|\, G_{\scriptscriptstyle D_2^*}\!(C_{\scriptscriptstyle 2}^*) = |\!\det D_{\scriptscriptstyle 1}|\, G_{\scriptscriptstyle D_2}\!(C_{\scriptscriptstyle 2})$$
 ,

which finishes the proof of (b).

To prove part (c), we use the Smith normal form for D. Choose unimodular U and V such that  $D^* = UDV = \operatorname{diag}(d_1, \cdots, d_n)$  where the invariant factors satisfy  $d_1|d_2|\cdots|d_n$  and each  $d_i>0$ . Let  $C^*=UC^tV^{-1}$ . Let  $v_p(d)$  be the p-adic valuation, so  $v_p(p^r)=r$  and  $v_p(0)=\infty$ . Write each  $d_i$  as  $d_i''d_i''$ ,  $1 \le i \le n$ ; here  $d_i''$  is the odd squarefree part of  $d_i$  when  $d_i$  is odd,  $d_i''$  is twice the odd squarefree part of  $d_i$  when  $v_2(d_i)$  is odd, and  $d_i''$  is four times the odd squarefree part of  $d_i$  when  $v_2(d_i)$  is non-zero even. One can verify that  $d_1'|d_2'|\cdots|d_n'$ . Let

$$D_1^* = \operatorname{diag}\left(d_1', d_2', \, \cdots, d_n'
ight) \ \ ext{ and } \ \ D_2^* = \operatorname{diag}\left(d_i'', d_2'', \, \cdots, d_n''
ight)$$
 .

We will show that  $C_2 = D_1^{*-1}C^{*i}D_1^*$  is integral and that  $(C_2, D_2)$  is CESD. Fix an arbitrary prime p, and let  $v = v_p$ . Define  $\alpha_i = v(d_i)$  and  $\beta_i = v(d_i')$ ; then by hypothesis  $2\beta_i \leq \alpha_i \leq 2\beta_i + 2$  for  $1 \leq i \leq n$ . One can easily show that  $\alpha_i - \alpha_j \geq \beta_i - \beta_j$  for  $1 \leq j \leq i \leq n$ , and also that  $\beta_1 \leq \beta_2 \leq \cdots \leq \beta_n < \infty$ .

Set  $C^* = (c_{ij})_{1 \le i,j \le n}$  and  $C_2 = (c_{ij}^{(2)})_{1 \le i,j \le n}$ . By hypothesis, (C,D) is symmetric so  $(C^*,D^*)$  is symmetric, hence  $c_{ij}d_j = d_ic_{ji}$ . Thus,  $v(c_{ji}) =$ 

 $v(c_{ij})+(\alpha_j-\alpha_i)$ . Since  $C_2=D_1^{*-1}C^*D_1^*=(d_i'^{-1}c_{ij}d_j')_{1\leq i,j\leq n}$ , we also have  $v(c_{ij}^{(2)})=v(c_{ij})+(\beta_j-\beta_i)$  for  $1\leq i,\ j\leq n$ . If  $i\leq j$  then  $\beta_i\leq \beta_j$ , hence  $v(c_{ij}^{(2)})\geq 0$ . If i>j, then  $v(c_{ij}^{(2)})=v(c_{ij})+(\beta_j-\beta_i)=v(c_{ji})+(\alpha_i-\alpha_j)-(\beta_i-\beta_j)\geq v(c_{ji})\geq 0$ . In any case,  $v(c_{ij}^{(2)})\geq 0$  for  $1\leq i,\ j\leq n$ , so  $C_2$  is p-integral. Since p is an arbitrary prime,  $C_2$  is integral.

We need to show that  $D_2{}^tC_2$  is even, equivalently, that  $v_2(d_i''c_{ii}^{(2)}) \ge 1$ . Since  $D^{*t}C^*$  is even,  $v_2(d_ic_{ii}) \ge 1$ . If  $v_2(c_{ii}) \ge 1$ , then  $v_2(c_{ii}^{(2)}) = v_2(c_{ii}) \ge 1$  follows from above. If  $v_2(d_i) \ge 1$ , then by the construction of  $d_i''$ ,  $v_2(d_i'') \ge 1$ . In any case,  $v_2(d_i''c_{ii}^{(2)}) \ge 1$ .

Finally, we set  $D_1 = U^{-1}D_1^*$  and  $D_1' = D_1^*V^{-1}$ . Then  $D = D_1D_2D_1'$  with  $|\det D_1| = |\det D_1'|$  and  $(C_2, D_2)$  is CESD, so we may apply part (b). Level  $D_2$  is either  $d_n''$  when  $d_n''$  is odd or  $2d_n''$  when  $d_n''$  is even. This concludes the proof of Theorem 3.

Using Theorems 3 and 4, we can reduce the computation of the symplectic Gauss sum to the computation of sums with odd prime level, with level 4, or with level 8. Theorem 2 of Stark evaluates the odd prime level case. We wish to compute the even level cases. First, however, we need to refine some classical algebraic results.

Let  $A \oplus B$  be the matrix  $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$  and  $\bigoplus_r A$  be the matrix  $\begin{pmatrix} A & 0 \\ 0 & \cdots & A \end{pmatrix}$  with r copies of A on the diagonal. Further, let  $I_k$  be the  $k \times k$  identity matrix.

Lemma 2. Let S be an integral symmetric  $n \times n$  matrix with odd determinant.

Suppose S is not even. Then there exists a unimodular matrix U such that  ${}^{\iota}USU=(I_{k}\oplus -I_{n-k})+2S'=(I_{k_{1}}\oplus 3I_{k_{2}}\oplus -3I_{k_{3}}\oplus -I_{k_{4}})+4S''$  where S' and S'' are integral even symmetric matrices,  $0\leq k\leq n$ , and  $k_{1}+k_{2}+k_{3}+k_{4}=n$ .

Suppose S is even. Then there exists a unimodular matrix U such that

$$egin{aligned} {}^{t}USU &= \left( \oplus_{k} inom{2}{1} \ rac{1}{2} 
ight) \oplus \oplus_{n/2-k} inom{0}{1} \ rac{1}{0} 
ight) 
ight) + 2S' \ &= \left( \oplus_{k_{1}} inom{4}{1} \ rac{1}{4} 
ight) \oplus \oplus_{k_{2}} inom{2}{1} \ rac{1}{-2} 
ight) \oplus \oplus_{k_{3}} inom{0}{1} \ rac{1}{0} 
ight) 
ight) + 4S'' \,, \end{aligned}$$

where S' and S'' are integral even symmetric matrices,  $0 \le k \le n/2$ , and  $k_1 + k_2 + k_3 = n/2$ .

*Proof.* Newman [8, pg. 68] shows that over  $\mathbb{Z}/2\mathbb{Z}$ , if S has odd determinant, there exists U unimodular over  $\mathbb{Z}/2\mathbb{Z}$  such that  ${}^tUSU\equiv I \bmod 2$  when S is not even or  $\equiv \bigoplus_{n/2} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \bmod 2$  when S is even.

We can in fact take U to be unimodular over Z ([9], pg. 109). Newman's construction of U involves elementary row and column operations which actually give that  ${}^{\iota}USU \equiv \mathrm{diag}\,(a_1,\,\cdots,\,a_n) \bmod 8$  or  $\equiv \bigoplus_{i=1}^{n/2} \binom{2a_i}{1} \mod 4$ . When S is not even, the results of the lemma follow immediately. When S is even, we consider conjugations of  $\binom{2a}{1} \pmod 4$  for all  $a,b \mod 4$ . For instance,

$$\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & -2 \end{pmatrix} + 4 \begin{pmatrix} 0 & 1 \\ 1 & 4 \end{pmatrix}.$$

Similar calculations reduce one to the matrices stated in the lemma, which concludes the proof.

These results motivate the following definitions. Let S be an integral symmetric matrix with odd determinant. If S is not even, define the 4-signature and the 8-signature of S by  $\operatorname{sgn}_4 S = 2k - n$  and  $\operatorname{sgn}_8 S = k_1 3k_2 - 3k_3 - k_4$ . If S is even, define the 4-signature and 8-signature of S by  $\operatorname{sgn}_4 S = 4k$  and  $\operatorname{sgn}_8 S = 0$ .

When det S is even, there generally are not 4 or 8 signatures. For special S, however, there are well-defined signatures. Let  $S=U[(0\oplus S_1)+2S']^tU$  with U unimodular, det  $S_1$  odd and S' integral even symmetric. We define  $\operatorname{sgn}_4S=\operatorname{sgn}_4(S_1)$ . When  $S=U[(0\oplus S_1)+4S']^tU$ , define  $\operatorname{sgn}_8S=\operatorname{sgn}_4(S_1)$ . Straightforward matrix manipulations show that the signatures are defined independently of the choice of U,  $S_1$ , or S'. The particular cases of interest are  $S=2D^{-1}C$  for D of level 4 and  $S=4D^{-1}C$  for D of "strict" level 8, which are discussed in the following theorem.

Theorem 5. Let (C, D) be CESD. Let  $r = \operatorname{rank}_2 D$  be the rank of D over  $\mathbb{Z}/2\mathbb{Z}$ .

(a) If D has level 4, then

and

$$G_{\scriptscriptstyle D}\!(C) = e \Big\{ rac{1}{4} \, {
m sgn}_{\scriptscriptstyle 4}(2D^{\scriptscriptstyle -1}C) \Big\} | \det D|^{\scriptscriptstyle 1/2} \ .$$

(b) If D has level 8 and  $|\det D| = 4^{n-r}$ , equivalently, if every invariant factor of D is either 1 or 4, then

$$G_{\scriptscriptstyle D}\!(C) = e \Big\{ rac{1}{4} \, {
m sgn_8} (4D^{\scriptscriptstyle -1}C) \Big\} | \det D|^{\scriptscriptstyle 1/2} \ .$$

Proof of (a). D has level 4, so there exist unimodular U and V such that  $UDV = \left(\frac{I_r}{0} \middle| \frac{0}{2I_{n-r}}\right)$ . One can easily verify that (C, D) CESD implies that

$$V^{-1}(2D^{-1}C)^{t}V^{-1} = \left(\begin{array}{c|c} 2C_{r} & 2C' \\ \hline 2^{t}C' & C_{n-r} \end{array}\right)$$

where  $C_r$  is an  $r \times r$  integral even symmetric matrix and  $C_{n-r}$  is an  $(n-r) \times (n-r)$  integral symmetric matrix with odd determinant. In fact, a usual construction of V shows that one may take  $C_{n-r}$  to be conjugate to any principal  $(n-r) \times (n-r)$  submatrix with odd determinant. By Lemma 1 (b),  $G_D(C) = G_{2I_{n-r}}(C_{n-r})$ . Suppose  $C_{n-r}$  is not even. Choose a unimodular W such that  ${}^tWC_{n-r}W = (I_k \oplus -I_{n-r-k}) + 2S$  for some integral even symmetric S. Then using Lemma 1 (c),

$$G_{2I_{n-r}}(C_{n-r}) = G_{2I_{n-r}}(I_k \oplus -I_{n-r-k}) = \prod_{i=1}^k G_i(1) \cdot \prod_{i=1}^{n-r-k} G_i(-1),$$

which is a product of one-dimensional Gauss sums. Direct computation shows that  $G_2(1) = e(1/4) \cdot 2^{1/2}$  and  $G_2(-1) = e(-1/4)2^{1/2}$ .

We conclude that

$$G_{\scriptscriptstyle D}(C) = e \Big\{ rac{1}{4} \left( k - (n-r-k) 
ight) \Big\} 2^{{\scriptscriptstyle (n-r)/2}} = e \Big\{ rac{1}{4} \operatorname{sgn}_{\scriptscriptstyle 4} C_{\scriptscriptstyle n-r} \Big\} |\det D|^{\scriptscriptstyle 1/2} \, .$$

The proof when  $C_{n-r}$  is even is exactly the same, except that one reduces the Gauss sum to a product of Gauss sums of the form  $G_{\binom{2}{0}2}\binom{2}{1}\binom{2}{1}$  and  $G_{\binom{2}{0}2}\binom{0}{1}\binom{0}{1}$ . Once again direct computation yields the desired result.

The proof of (b) is essentially the same; when the appropriate  $C_{n-r}$  is not even, one gets a product of Gauss sums of the forms  $G_4(1)$ ,  $G_4(3)$ ,  $G_4(-3)$ , and  $G_4(-1)$  which one can easily evaluate. When  $C_{n-r}$  is even, the appropriate Gauss sums are  $G_{\binom{4}{0}0}\binom{4}{1}\binom{4}{1}$ ,  $G_{\binom{4}{0}0}\binom{2}{1}\binom{2}{1}$ , and  $G_{\binom{4}{0}0}\binom{0}{1}\binom{0}{1}$  which are all equal to 4. This concludes the proof of this theorem.

When D has level 8, but contains 2 as an invariant factor, the situation is much more complicated.

THEOREM 6. Let (C, D) be CESD, and let D have level 8. Let  $r = \operatorname{rank}_2(D)$  and  $|\det D| = 2^d$ . Then there exists a unimodular matrix V such that

$$V^{-1}(4D^{-1}C)^tV^{-1} = egin{pmatrix} 4S_1 & 4M_1 & 4M_2 \ 4^tM_1 & 2S_2 & 2M_3 \ 4^tM_2 & 2^tM_3 & S_4 \end{pmatrix}.$$

 $S_1$  is an integral even symmetric matrix.  $M_1$ ,  $M_2$ , and  $M_3$  are integral matrices;  $S_2$  is an integral symmetric  $(2r-d)\times(2r-d)$  matrix with odd determinant; and  $S_4$  is an integral symmetric  $(d-r)\times(d-r)$  matrix with odd determinant.

Finally,

$$egin{aligned} rac{G_{\scriptscriptstyle D}(C)}{|\det D|^{1/2}} &= e \Big\{ rac{1}{4} \left[ ext{sgn}_4(S_{\scriptscriptstyle 2}) + ext{sgn}_8(S_4 - 2 M_3 S_2^{*t} M_3) 
ight] \Big\} \ &= e \Big\{ rac{1}{4} \left[ ext{sgn}_4(S_2 - 2^t M_3 S_4^* M_3) + ext{sgn}_8(S_4) 
ight] \Big\} \,. \end{aligned}$$

Here  $S_2^*$  is any integral symmetric matrix such that  $S_2S_2^* \equiv I \mod 4$ , and  $S_4^*$  is integral symmetric matrix such that  $S_4S_4^* \equiv I \mod 2$ .

*Proof.* The conditions on D imply that there exist U and V with  $UDV = (I_{n-r} \oplus 2I_{2r-d} \oplus 4I_{d-r})$ . One can easily show that (C, D) CESD implies that

$$UC^{\iota}V^{-1} = egin{pmatrix} S_1 & M_1 & M_2 \ 2^{\iota}M_1 & S_2 & M_3 \ 4^{\iota}M_2 & 2^{\iota}M_3 & S_4 \end{pmatrix}$$

and that  $V^{-1}(4D^{-1}C)^tV^{-1}$  has the desired form. Using Lemma 1, one can verify that

$$egin{align*} G_{\scriptscriptstyle D}(C) &= G_{\scriptscriptstyle (2I_{2r-d}\oplus 4I_{d-r})}\!\!\left(\!\!\! \begin{pmatrix} S_2 & M_3 \ 2^t M_3 & S_4 \end{pmatrix}\!\!
ight) = G_{\scriptscriptstyle 2I_{2r-d}}\!\!\left(S_2 - 2^t M_3 S_4^* M_3
ight) G_{\scriptscriptstyle 4I_{d-r}}\!\!\left(S_4
ight) \ &= G_{\scriptscriptstyle 2I_{2r-d}}\!\!\left(S_2
ight) G_{\scriptscriptstyle 4I_{d-r}}\!\!\left(S_4 - 2 M_3 S_2^{*t} M_3
ight) \,. \end{split}$$

 $S_2^*$  and  $S_4^*$  are easy to find since the determinants of  $S_2$  and  $S_4$  are odd. Applying Theorem 5 completes the proof.

This theorem now completes the results needed to calculate an arbitrary Gauss sum. Theorems 3 and 4 decompose a Gauss sum into the basic cases which Theorems 2, 5, and 6 evaluate explicitly.

## § 3. The symplectic Jacobi symbol

In the classical case,  $G_d(cc_0) = (c/d)G_d(c_0)$  when d is odd. This suggests the following definition.

DEFINITION. Let  $(CC_0, D)$  and  $(C_0, D)$  be CESD and suppose that det D is odd. The symplectic Jacobi symbol is defined by

$$(C/D, C_0) = G_D(CC_0)/G_D(C_0)$$
.

This lemma will later yield the multiplicativity of the symplectic Jacobi symbol.

LEMMA 3. Let D have odd determinant, and let  $C_1$ ,  $C_2$ ,  $C_3$ , and  $C_4$  be integral matrices such that the pairs  $(C_1C_2, D)$ ,  $(C_3C_4, D)$ ,  $(C_1C_4, D)$  and  $(C_3C_2, D)$  are CESD. Furthermore, assume that for each prime  $p|\det D$ , one of the products  $C_1C_2$ ,  $C_3C_4$ ,  $C_1C_4$  or  $C_3C_2$  has non-zero determinant mod p. Then

$$G_{D}(C_{1}C_{2})G_{D}(C_{3}C_{4}) = G_{D}(C_{1}C_{4})G_{D}(C_{3}C_{2})$$
.

*Proof.* Choose U and V so that UDV is in Smith normal form. Let  $C_1' = UC_1$ ,  $C_2' = C_2^t V^{-1}$ ,  $C_3' = UC_3$ , and  $C_4' = C_4^t V^{-1}$ . Since  $G_D(C_i C_j) = G_{UDV}(UC_i C_j^t V^{-1})$ , the lemma and its hypotheses will be true for  $(C_1, C_2, C_3, C_4; D)$  iff it is true for  $(C_1', C_2', C_3', C_4'; UDV)$ . Therefore, without loss of generality we may assume D is diagonal.

For D diagonal, if level D is not a prime power, write  $D = D_1D_2 = D_2D_1$  with  $D_1$  and  $D_2$  diagonal matrices with (level  $D_1$ , level  $D_2$ ) = 1. By Theorem 3,

$$G_D(C_iC_j) = G_D(C_iC_jD_j) \cdot G_D(C_iC_jD_j)$$
.

If a prime  $p|\det D_1$ , then  $p \nmid \det D_2$ , hence there exists a product  $C_iC_j$  such that  $p \nmid \det(C_iC_jD_2)$ . Therefore, the lemma and its hypotheses hold for  $(C_1, C_2, C_3, C_4; D)$  iff they hold for  $(C_1, C_2D_2, C_3, C_4D_2; D_1)$  and  $(C_1, C_2D_1, C_3, C_4D_1; D_2)$ . Thus, without loss of generality we may assume that D is a diagonal matrix with odd prime-power level.

Let level  $D=p^k$  for some odd prime p. By renumbering, we may assume  $p \nmid \det C_1C_2$ . There exists a unimodular U such that  $C_1U=$  diag  $(1, 1, \dots, 1, \det C_1) \bmod p^k$ , hence by replacing  $(C_1, C_2, C_3, C_4; D)$  by  $(C_1U, U^{-1}C_2, C_3U, U^{-1}C_4; D)$  we may assume that  $C_1=C_{1,1}+p^kC_{1,2}$  for  $C_{1,1}$  a diagonal matrix. (See Newman [8] pg. 36). Now  $D=D_1D_2D_1$  for  $D_1$ ,  $D_2$  diagonal matrices with level  $D_2=p$ . We know from the proof of Theorem 4(c) that  $(C_1C_2, D)$  CESD implies that  $(D_1^{-1}C_1C_2D_1, D_2)$  is CESD. Clearly  $D_1^{-1}C_{1,1}D_1$  is an integral matrix, and therefore so is  $C_1'=D_1^{-1}C_1D_1$ . Now  $D_1^{-1}C_1C_2D_1=C_1'\cdot(D_1^{-1}C_2D_1)$ . Since  $C_1'$  is invertible over the p-adic integers,

 $D_1^{-1}C_2D_1$  is p-adically integral. But  $p^kD_1^{-1}C_2D_1$  is integral over the ordinary integers, hence  $C_2'=D_1^{-1}C_2D_1$  is an integral matrix. Similar arguments which use the fact that  $p \nmid \det C_1C_2$  show that  $C_3'=D_1^{-1}C_3D_1$  and  $C_4'=D_1^{-1}C_4D_1$  are also integral matrices. One can now verify that the lemma and its hypotheses hold for  $(C_1, C_2, C_3, C_4; D)$  iff they hold for  $(C_1', C_2', C_3', C_4'; D_2)$ . We may therefore assume that D has odd prime level p, that  $p \nmid \det C_1C_2$ , and that  $C_1$  is a diagonal matrix mod p.

A simple permutation transformation shows that we may assume that  $D=(I_{n-r}\oplus pI_r)$  for some  $1\leq r\leq n$ . For i=1,2,3,4, let  $C_i=\begin{pmatrix} P_i&Q_i\\R_i&S_i\end{pmatrix}$  where  $P_i$  is an  $(n-r)\times (n-r)$  matrix and  $S_i$  is an  $r\times r$  matrix. If  $(C_iC_j,D)$  is CESD, straightforward matrix multiplication shows that  $R_iP_j+S_iR_j\equiv 0 \ \mathrm{mod}\ p$  and  $(pD^{-1}C_iC_j)^{(r)}=R_iQ_j+S_iS_j$ .

Because of the assumption that  $C_1$  is an invertible diagonal matrix  $\operatorname{mod} p$ ,  $R_1 \equiv 0 \operatorname{mod} p$  and  $P_1$  and  $S_1$  are invertible  $\operatorname{mod} p$ . Then  $(C_1C_2, D)$  CESD implies that  $R_2 \equiv 0 \operatorname{mod} p$ . By hypothesis,  $C_2$  is invertible  $\operatorname{mod} p$  so  $P_2$  and  $S_2$  must be invertible  $\operatorname{mod} p$ . Similar arguments show that  $R_3 \equiv R_4 \equiv 0 \operatorname{mod} p$ .

Now we will apply Theorem 2 of Stark. For  $(C_i C_j, D)$  CESD,

$$egin{aligned} G_{\scriptscriptstyle D}(C_{\scriptscriptstyle i}C_{\scriptscriptstyle j}) &= arepsilon_p^r igg(rac{\det(2pD^{-1}C_{\scriptscriptstyle i}C_{\scriptscriptstyle j})^{({\scriptscriptstyle i})}}{p}igg) p^{r/2} \ &= arepsilon_p^r igg(rac{2^r}{p}igg) igg(rac{\det(R_{\scriptscriptstyle i}Q_{\scriptscriptstyle j}+S_{\scriptscriptstyle i}S_{\scriptscriptstyle j})}{p}igg) p^{r/2} = arepsilon_p^r igg(rac{2^r}{p}igg) igg(rac{\det(S_{\scriptscriptstyle i}S_{\scriptscriptstyle j})}{p}igg) p^{r/2} \,. \end{aligned}$$

The lemma now follows as a corollary of the multiplicativity of the usual Jacobi symbol, which concludes the proof.

Lemma 3 underlies the multiplicative properties of the Jacobi symbol, as is evident in the next theorem.

THEOREM 7. Let  $(CC_0, D)$  and  $(C_0, D)$  be CESD with det D odd.

- (a) Suppose there exists  $C'_0$  with  $(\det C'_0, \det D) = 1$  such that  $(CC'_0, D)$  and  $(C'_0, D)$  are CESD. Then  $(C/D, C_0) = (C/D, C'_0)$ .
- (b) Suppose that  $C = C_1C_2$  with  $(C_1C_0, D)$  and  $(C_2C_0, D)$  CESD. Assume that  $(\det C_0, \det D) = 1$ . Then  $(C_1C_2/D, C_0) = (C_1/D, C_0) \cdot (C_2/D, C_0)$ .
- (c) Let  $D=D_1D_2=D_2'D_1'$  satisfy the hypotheses of Theorem 3 for both pairs  $(CC_0, D)$  and  $(C_0, D)$ . Then  $(C/D, C_0)=(C/D_1, C_0^{\ t}D_2)\cdot (C/D_2', C_0^{\ t}D_1')$ .

Proof of (a). We need only show that  $G_D(CC_0)G_D(C_0') = G_D(CC_0')G_D(C_0)$  which follows from the hypotheses about  $C_0'$  and Lemma 2. To prove (b), need to verify that  $G_D(C_1C_2C_0)G_D(C_0) = G_D(C_1C_0)G_D(C_2C_0)$  which also follows from the hypotheses about  $C_0$  and Lemma 2.

The proof of (c) follows easily from the definitions and Theorem 3, completing the proof of Theorem 7.

We remark, however, that the hypothesis concerning  $C_0'$  in Theorem 7(a) is necessary. For instance, let  $D=\begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix}$ ,  $C=\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ,  $C_0=\begin{pmatrix} 1 & 15 \\ 3 & 0 \end{pmatrix}$ , and  $C_0'=\begin{pmatrix} 1 & 5 \\ 1 & 0 \end{pmatrix}$ . Then one can calculate that  $(C/D,\,C_0)=1$  whereas  $(C/D,\,C_0')=-1$ .

Another standard property of Jacobi symbols is periodicity. For the symplectic Jacobi symbol, the presence of  $C_0$  complicates matters, but one could easily show periodicity from that of the Gauss sums. The presence of  $C_0$  also complicates the removal of square factors from the levels of C and D. We could easily derive such results, however, by slightly revising the hypotheses of Theorem 4. We will content ourselves with the following theorem that will be useful later.

Theorem 8. Let  $(CC_0, D)$  and  $(C_0, D)$  be CESD with det D odd.

- (a)  $(C/D, C_0) = \pm 1$
- (b) If  $c \in \mathbb{Z}$  with  $(c, \det D) = 1$ , then  $(cI/D, C_0) = (c/\det D)$  where the right side is the usual Jacobi symbol.

*Proof.* The proof of a) closely parallels that of Lemma 2. We first reduce to the case of D diagonal, next to the case of D prime-power level, and finally to the case of D prime level. Theorem 2 of Stark implies that

$$(C/D, C_0) = \left(\frac{\det(pD^{-1}CC_0)^{(k)}}{p}\right) \left(\frac{\det(pD^{-1}C_0)^{(k)}}{p}\right) = \pm 1$$

where  $|\det D| = p^k$ . This proves a).

From this equation it is clear that when C = cI,  $(cI/D, C_0) = (c^k/p) = (c/p^k)$  for D of level p. If one retraces the steps used to decompose D, one reconstructs the invariant factors of D. This demonstrates b) and concludes the proof of the theorem.

In the classical case,  $\varepsilon_p = e\{1/4(1-\operatorname{sgn}_4 p)\}$  for p an odd positive integer, and the reciprocity law says that  $(p/q) = \varepsilon_{pq}/\varepsilon_p\varepsilon_q(q/p)$  (see Eichler [2]). This suggests the following definition: for an integral symmetric S

with odd determinant, let  $\varepsilon(S) = e\{(1/4)(\operatorname{sgn} S - \operatorname{sgn}_4 S)\}$ . We will now state the reciprocity law for the symplectic Jacobi symbol.

THEOREM 9. Let  $(CC_0, D)$ ,  $(C_0, D)$ ,  $(D^{\iota}C_0, C)$  and  $({}^{\iota}C_0, C)$  be CESD with det C and det D odd. If  $C_0 = 2U$  for some unimodular U, then

$$(C/D, 2U) = \varepsilon(D^{\iota}(CU))\varepsilon(-D^{\iota}U)\varepsilon(-CU)\cdot(D/C, -2^{\iota}U)$$
.

*Proof.* The proof is a straightforward application of Theorem 1 and Theorem 3.

$$egin{aligned} &(C/D,\,C_0) = rac{G_D(CC_0)}{G_D(C_0)} = e igg\{rac{1}{4} \left[ \operatorname{sgn} D^\iota(CC_0) - \operatorname{sgn} D^\iota C_0 
ight] igg\} \cdot rac{G_{CC_0}(-D)}{|\det C|^{1/2} G_{C_0}(-D)} \ &= e igg\{rac{1}{4} \left[ \operatorname{sgn} D^\iota(CC_0) - \operatorname{sgn} D^\iota C_0 
ight] igg\} \ &\cdot rac{G_{\iota C_0}(-DC)}{G_{c_0}(-D)} \cdot rac{G_c(-D^\iota C_0)}{G_c(-{}^\iota C_0)} \cdot rac{G_c(-{}^\iota C_0)}{|\det C|^{1/2}} \ &= e igg\{rac{1}{4} \left[ \operatorname{sgn} D^\iota(CC_0) - \operatorname{sgn} D^\iota C_0 - \operatorname{sgn} CC_0 
ight] igg\} \ &\cdot igg\{rac{G_{\iota C_0}(-DC)G_{\iota C_0}(C)}{G_{c_0}(-D)|\det C_0|^{1/2}} igg\}(D/C,\,-{}^\iota C_0) \,. \end{aligned}$$

When  $C_0 = 2U$ , the evaluation given is a corollary of Theorem 5, concluding the proof of this theorem.

It is interesting to note, however, that in the classical case when  $C=c,\ D=d,$  and  $C_0=2,$  one can verify that

$$e\Big\{rac{1}{4}\left[\operatorname{sgn}dc-\operatorname{sgn_4}\!dc
ight]-\left[\operatorname{sgn}d-\operatorname{sgn_4}\!d
ight]-\left[\operatorname{sgn}c-\operatorname{sgn_4}\!c
ight]\Big\}=(-1)^n$$

where  $n = \frac{c-1}{2} \cdot \frac{d-1}{2} + \frac{\operatorname{sgn} c - 1}{2} \cdot \frac{\operatorname{sgn} d - 1}{2}$ . This agrees with Hasse [4] and Hecke [5].

We also note that when  $C_0 = 2U$  and C = V for unimodular U and V,

$$(\mathit{V/D}, 2\mathit{U}) = e \Big\{ rac{1}{4} \left[ \operatorname{sgn} \mathit{D}^{\iota}(\mathit{VU}) - \operatorname{sgn_4} \! \mathit{D}^{\iota}(\mathit{VU}) 
ight] - \left[ \operatorname{sgn} \mathit{D}^{\iota}\mathit{U} - \operatorname{sgn_4} \! \mathit{D}^{\iota}\mathit{U} 
ight] \Big\} \,.$$

If C = 2V, replace  $\operatorname{sgn}_4$  by  $\operatorname{sgn}_8$ . These correspond to the classical supplementary laws. Unfortunately, there are also choices for C which require the complicated criterion of Theorem 6, and we will not pursue the matter further.

16 ROBERT STYER

## § 4. Transformations of multivariable theta functions

Stark [10] uses symplectic Gauss sums to explicitly evaluate transformation formulas for theta functions defined over algebraic number fields. He embeds these theta functions into the symplectic theta function, then uses Theorem 2 to determine the explicit multiplier system of the symplectic theta function. He evaluates the symplectic multiplier system in terms of the original algebraic numbers whenever the lower right corner of the transformation matrix is essentially a first degree odd prime ideal. In this section, we will consider more general cases, in particular the case when even prime factors occur.

The theta functions considered by Stark are defined for a field K of degree n with ring of integers  $\mathcal{O}(K)$ , different  $\mathfrak{D}$ , and any (fractional) ideal  $\mathfrak{m}$ . In particular,

$$\theta_{\scriptscriptstyle K}(z,\,\mathfrak{m}) = \sum_{\mu\in\mathfrak{m}} e\{\operatorname{tr}(x\mu^2 + iy|\mu|^2)\}$$
.

Stark actually defines a more general theta function; its transformation formula, however, is essentially the same as this one. One of his extra variables does allow us to change ideals within ideal classes, so we will assume that m is an odd integral ideal.

These theta functions transform under certain subsets of SL(2,K). The transformation formula, however, only depends on the lower row  $(\Upsilon,\delta)$ . Here for given ideals  $\mathfrak{m}_1$  and  $\mathfrak{m}_2$ ,  $(\Upsilon,\delta)$  satisfy  $\Upsilon\in\mathfrak{Dm}_1\mathfrak{m}_2$ ,  $\delta\in\mathfrak{m}_1\mathfrak{m}_2^{-1}$ ,  $\Upsilon\delta\in2\mathfrak{Dm}_1^2$  and if  $(\Upsilon)=\mathfrak{cDm}_1\mathfrak{m}_2$  and  $(\delta)=\mathfrak{bm}_1\mathfrak{m}_2^{-1}$  then  $(\mathfrak{c},\delta)=1$ .

For any ideal  $\mathfrak{m}$ , let  $[\mu_1, \mu_2, \dots, \mu_n]$  be an integral basis for  $\mathfrak{m}$ . Let  $\mu^{(i)}$  be the  $i^{\text{th}}$  conjugate of  $\mu \in K$ . Define the  $n \times n$  matrix M associated to the ideal  $\mathfrak{m}$  by  $M = (\mu_j^{(i)})_{1 \leq i,j \leq n}$ . Consider the ideals  $\mathfrak{m}_1$  and  $\mathfrak{m}_2$  above and their associated matrices  $M_1$  and  $M_2$ . Let  $\operatorname{diag}(\lambda) = \operatorname{diag}(\lambda^{(i)})_{1 \leq i \leq n}$  for any  $\lambda \in K$ . Then Stark defines the symplectic embedding (C, D) of the pair  $(7, \delta)$  by  $C = M_1^{-1} \operatorname{diag}(7)^i M_2^{-1}$  and  $D = M_1^{-1} \operatorname{diag}(\delta) M_2$ .

Stark shows the following results.

THEOREM 10. (a) (C, D) is CESD. If  $(\delta) = \mathfrak{bm}_1\mathfrak{m}_2^{-1}$ , then  $|\det D| = N(\delta)$ . The results are independent of the choice of bases for  $\mathfrak{m}_1$  and  $\mathfrak{m}_2$ . Also,  $\operatorname{sgn} D^t C = \operatorname{sgn} \delta \Upsilon$ .

(b)  $\theta_{\rm K}(z, \, {\rm I}{\rm I}_{\rm I})$  transforms under certain matrices with bottom row  $(\Upsilon, \, \delta)$ . Finding the particular transformation formula reduces to evaluating the symplectic Gauss sum  $G_{\rm D}(C)$ .

(c) If  $(\delta) = \mathfrak{pm}_1\mathfrak{m}_2^{-1}$  where  $\mathfrak{p}$  is a first degree prime ideal of norm p with  $(\mathfrak{p}, 2\mathfrak{Dm}_1\mathfrak{m}_2) = 1$ , then

$$rac{G_{\scriptscriptstyle D}(C)}{|\det D|^{\scriptscriptstyle 1/2}} = arepsilon_{\scriptscriptstyle p}\!\!\left(rac{2p\delta^{\scriptscriptstyle -1}\gamma}{\mathfrak{p}}
ight).$$

Stark could easily have shown the following.

Theorem 11. The Gauss sum  $G_D(C)$  obtained by Stark's embedding of  $(7, \delta)$  has the same value as the Gauss sum  $C(2\delta^{-1}7)$  defined by Hecke [5] whenever  $(5, 2\mathfrak{D}\mathfrak{m}_1\mathfrak{m}_2) = 1$ .

*Proof.* Hecke defines a Gauss sum for an algebraic number  $\omega$  by  $C(\omega) = \sum_{\mu \bmod a} e(2\mathrm{tr}(\omega\mu^2))$  where  $(\omega) = \mathfrak{b}/(\mathfrak{a}\mathfrak{D})$  with  $(\mathfrak{a},\mathfrak{b}) = 1$ . Whenever  $\mathfrak{b}, 2\mathfrak{Dm}_2) = 1$ ,

$$C(2\delta^{-1}\varUpsilon) = \sum_{\mu \bmod \mathfrak{b}} e(2\mathrm{tr}(2\delta^{-1}\varUpsilon\mu^2)) = \sum_{\mu \bmod \mathfrak{b}} e({}^t m^* \operatorname{diag}(\delta^{-1}\varUpsilon\mu^2) m^*)$$

where  ${}^{t}m^{*}=(1,1,\cdots,1).$ 

Then

$$C(\omega) = \sum_{\mu \bmod b} e({}^{t}m(\mu)D^{-1}Cm(\mu))$$

where  $m(\mu) = {}^{\iota}(M_2^{-1}\operatorname{diag}(\mu)M_2){}^{\iota}M_2m^*$  is an integral column vector. This ast sum will be Stark's  $G_D(C)$  once we show that  $\mu \equiv 0 \mod \mathfrak{d}$  iff  $m(\mu) \equiv 0 \mod {}^{\iota}D$ . Assume that  $m(\mu) \equiv 0 \mod {}^{\iota}D$  so  $m(\mu) = {}^{\iota}Dm_0$  for  $m_0 \in \mathbb{Z}^n$ . Then

$${}^{t}M_{2}\operatorname{diag}(\mu)m^{*}={}^{t}M_{2}\operatorname{diag}(\delta){}^{t}M_{1}^{-1}m_{0}$$

and thus

$$\operatorname{diag}(\mu N(\mathfrak{m}_1)\delta^{-1})m^* = N(\mathfrak{m}_1)^t M_1^{-1} m_0.$$

The right hand vector is integral over K, so the left side is integral over K. When  $(\mathfrak{d}, \mathfrak{m}_1) = 1$ , this means that  $\mu \delta^{-1}$  is integral in K, hence  $\mu \equiv 0$  mod  $\mathfrak{d}$ . The converse is similar, which concludes the proof.

COROLLARY 1. Let  $\Upsilon \in \mathcal{O}(K)$ ,  $\Upsilon_0 \in 2\mathfrak{D}\mathfrak{m}_1\mathfrak{m}_2$ , and  $(\delta) = \mathfrak{b}\mathfrak{m}_1\mathfrak{m}_2^{-1}$  with  $(\mathfrak{b}, 2\Upsilon \Upsilon_0)$  = 1. Let  $C = M_1^{-1}\operatorname{diag}(\Upsilon)M_1$  and let  $(C_0, D)$  be Stark's symplectic embedding of  $(\Upsilon_0, \delta)$ . Then  $(C/D, C_0) = (\Upsilon/\delta)$ .

We could use the reciprocity law in Theorem 9 to obtain a reciprocity law for algebraic integers extending that of Hecke [5]. We will not do this, but only note that Hecke's "primär" requirement essentially eliminates the 4 signatures of the matrices. For the more general reciprocity law, one requires 4- and 8-signatures of algebraic integers.

Our goal is to evaluate  $G_D(C)$  in cases where b may involve even ideals. Therefore, we also will be forced to consider the concept of a 4-signature of an algebraic integer.

DEFINITION. Fix a fractional ideal  $\mathfrak{m}$ . Let  $\Delta \in \mathfrak{Dm}^2$  be chosen such that for each prime ideal  $\mathfrak{p}|(2)$ , if  $(\Delta) = \mathfrak{Dp}^r\mathfrak{qm}^2$  with  $(\mathfrak{p},\mathfrak{q}) = 1$ , then r = 0 or  $r \geq 2$ . Define the 4-signature of  $\Delta$  with respect to  $\mathfrak{m}$  by

$$\operatorname{sgn}_4(\Delta, \mathfrak{m}) = \operatorname{sgn}_4[(M^{-1}\operatorname{diag}(\Delta)^t M^{-1})]$$

where the sgn4 on the right was defined just before Theorem 5.

If  $\Delta \in \mathfrak{Dm}^{-1}$  with  $\mathfrak{m}$  an integral odd ideal, define  $\operatorname{sgn}_{4}(\Delta) = \operatorname{sgn}_{4}(N(\mathfrak{m})^{2}\Delta, \mathcal{O}(K))$ . That this is defined independently of  $\mathfrak{m}$  is apparent from the following theorem.

Theorem 12. Assume that  $\Delta$  is always chosen with the appropriate "evenness" conditions so the symbols below are defined.

(a) Let  $\mathfrak{m}_1$  and  $\mathfrak{m}_2$  have the same "even part", that is,  $\mathfrak{m}_1=\mathfrak{q}_1\mathfrak{q}_2$  and  $\mathfrak{m}_2=\mathfrak{q}_3\mathfrak{q}_2$  with  $\mathfrak{q}_1$  and  $\mathfrak{q}_3$  odd ideals.

If  $\Delta \in \mathfrak{Dm}_1$  and  $\Delta \in \mathfrak{Dm}_2$ , then

$$\operatorname{sgn}_4(\Delta, \mathfrak{m}_1) = \operatorname{sgn}_4(\Delta, \mathfrak{m}_2).$$

- (b) Let  $\sigma \in \mathfrak{Dm}^2$ . Then  $\operatorname{sgn}_4(\Delta + 4\sigma, \mathfrak{m}) = \operatorname{sgn}_4(\Delta, \mathfrak{m})$ . Let  $\sigma \in K$ . Then  $\operatorname{sgn}_4(\sigma^2\Delta, \sigma\mathfrak{m}) = \operatorname{sgn}_4(\Delta, \mathfrak{m})$ . In particular, if  $\sigma$  is odd, then  $\operatorname{sgn}_4(\sigma^2\Delta) = \operatorname{sgn}_4(\Delta)$ .
- (c) Suppose that K is a normal field with odd discriminant, and that there exists a first degree prime ideal  $\mathfrak{p}|(2)$ . Then

$$\operatorname{sgn}_4(\Delta) = \sum_{j=1}^n \left(\frac{\Delta^{(j)}}{\mathfrak{p}^2}\right)$$

where  $(\lambda/\mathfrak{p}^2)$  equals 1 when  $\lambda \equiv 1 \mod \mathfrak{p}^2$ , equals -1 when  $\lambda \equiv -1 \mod \mathfrak{p}^2$ , and equals 0 when  $\lambda \equiv 0 \mod \mathfrak{p}^2$ .

Proof of (a). Since  $\mathfrak{m}_1$  and  $\mathfrak{m}_2$  have the same "even part", we can choose an odd integer  $a \in \mathfrak{m}_1\mathfrak{m}_2^{-1}$ . Define  $T = aM_1^{-1}M_2$ ; T is integral and has odd determinant, hence is invertible mod 4. Thus,

$$\begin{split} \mathrm{sgn}_4 &((M_1^{-1}\operatorname{diag}(\varDelta)^t M_1^{-1})) = \mathrm{sgn}_4 &((TM_2^{-1}\mathrm{diag}(\varDelta)^t M_2^{-1t}T)) \\ &= \mathrm{sgn}_4 &((M_2^{-1}\operatorname{diag}(\varDelta)^t M_2^{-1})) \end{split}$$

which is the desired result.

The proof of b) is easy. Note that the matrix associated to  $\sigma m$  is  $\operatorname{liag}(\sigma)M$ .

To justify c), we modify the idea behind Stark's proof of Theorem 10c). Since  $\mathfrak p$  is a first degree prime dividing (2),  $\mathcal O(K)/\mathfrak p^2$  is isomorphic to  $\mathbb Z/4\mathbb Z$ . The matrix M associated to the ideal  $\mathcal O(K)$  has non-zero determinant mod  $\mathfrak p^2$  when the discriminant is odd. (Indeed,  $|\det M^t M|$  is the discriminant; see Lang [6]). By hypothesis on  $\mathcal A$ ,  $\mathcal A^{(j)} \not\equiv 2 \mod \mathfrak p^2$  for any  $1 \leq j \leq n$ , and clearly  $\operatorname{diag}(\mathcal A) \equiv \operatorname{diag}((\mathcal A^{(j)}/\mathfrak p^2)) \mod \mathfrak p^2$ . If we let N be an integral matrix with  $N \equiv M \mod \mathfrak p^2$ , then  $\operatorname{sgn}_4(\mathcal A) = \operatorname{sgn}_4((M^{-1}\operatorname{diag}(\mathcal A)^tM^{-1})) = \operatorname{sgn}_4((N^{-1}\operatorname{diag}(\mathcal A)^t)^tN^{-1})) = \sum_{j=1}^n (\mathcal A^{(j)}/\mathfrak p^2)^t$ . This concludes the proof of Theorem 12.

We are now ready to evaluate the Gauss sum factor of the theta transformation formula of Stark's theta functions. Since even translations do not affect the multiplier system, we may replace the pair  $(7, \delta)$  by  $(7, 27\sigma + \delta)$  with  $\sigma \in \mathbb{D}^{-1}\mathfrak{m}_2^{-2}$ . In particular, with an appropriate  $\sigma$ , we may assume that  $(\delta) = \delta_1 \delta_2 \mathfrak{m}_1 \mathfrak{m}_2^{-1}$  with  $(\delta_1, 2\mathfrak{D}\mathfrak{m}_1 \mathfrak{m}_2) = 1$  and  $\delta_2 | (2)$ . There exist ideals  $\mathfrak{m}_3$  with  $(\mathfrak{m}_3, 2\delta_1) = 1$  and  $\mathfrak{m}_4 = \mathfrak{m}_1 \mathfrak{m}_2 \mathfrak{m}_3^{-1}$  such that  $\delta = \delta_1 \delta_2$  with  $(\delta_1) = \delta_1 \mathfrak{m}_1 \mathfrak{m}_3^{-1} = \delta_1 \mathfrak{m}_4 \mathfrak{m}_2^{-1}$  and  $(\delta_2) = \delta_2 \mathfrak{m}_3 \mathfrak{m}_2^{-1} = \delta_2 \mathfrak{m}_1 \mathfrak{m}_4^{-1}$ . Finally, choose  $\nu \in \mathfrak{D}\mathfrak{m}_1 \mathfrak{m}_3$  such that  $(\nu) = \mathfrak{p} \mathfrak{D}\mathfrak{m}_1 \mathfrak{m}_3$  with  $\mathfrak{p}$  a first degree prime ideal of norm  $\mathfrak{p}$  with  $(p, 2\mathfrak{D}\mathfrak{m}_1 \mathfrak{m}_3) = 1$ . Let  $(\infty)$  denote the product of all the real infinite primes of K.

Theorem 13. Let  $(\Upsilon, \delta)$ ,  $\delta_1$ ,  $\delta_2$  and  $\nu$  be as above. Then

$$rac{G_{\it D}(\it C)}{|\det D|^{1/2}} = e \Big\{rac{1}{4}\, {
m sgn_4}(2\delta^{-1}\gamma)\Big\} \cdot \Big(rac{2\gamma\delta_2}{\mathfrak{d}_1}\Big) \! arepsilon(\delta_1 
u) \cdot arepsilon_p^{-1} \! \chi(\delta_1) \; .$$

Here  $\varepsilon(\delta_1\nu) = e\{(1/4)(\operatorname{sgn}\delta_1\nu - \operatorname{sgn}_4\delta_1\nu)\}$  and  $\chi(\delta_1) = (\nu/\delta_1)(\delta_1/\mathfrak{p})(p\nu^{-1}/\mathfrak{p})$  is a quadratic character defined modulo  $4\mathfrak{Dm}_1\mathfrak{m}_3^{-1}(\infty)$ . If  $\delta_1$  is a first degree prime ideal of norm  $\delta$ , then  $\chi(\delta_1) = \varepsilon_a \varepsilon_p \varepsilon(-\delta_1\nu) \cdot (d\delta_1^{-1}/\delta_1)$ .

*Proof.* Let  $D_1 = M_1^{-1} \operatorname{diag}(\delta_1) M_3$ ,  $D_1' = M_4^{-1} \operatorname{diag}(\delta_1) M_2$ ,  $D_2 = M_3^{-1} \operatorname{diag}(\delta_2) M_2$ , and  $D_2' = M_1^{-1} \operatorname{diag}(\delta_2) M_4$ . Then  $D = D_1 D_2 = D_2' D_1'$ . Since  $(\delta_1, \delta_2) = 1$ , one can easily construct matrices which satisfy the hypotheses of Theorem 3a). Thus,

$$rac{G_{\scriptscriptstyle D}(C)}{|\det D|^{\scriptscriptstyle 1/2}} = rac{G_{\scriptscriptstyle D_1}\!(C^{\scriptscriptstyle t}D_2)}{|\det D_1|^{\scriptscriptstyle 1/2}} \cdot rac{G_{\scriptscriptstyle D_2}\!(C^{\scriptscriptstyle t}D_1')}{|\det D_2'|^{\scriptscriptstyle 1/2}} \,.$$

Now level  $D_2'=2$  and  $|\det D_2'|= extbf{N}(\mathfrak{d}_2)$  so we may apply Theorem 5 and

Theorem 12 to evaluate the last Gauss sum factor as  $e\{1/4 \operatorname{sgn}_4(2\delta^{-1}\gamma)\}$ .

Let 
$$\lambda = rac{\gamma \delta_2}{2}$$
 and  $L = M_1^{-1} \operatorname{diag}(\lambda)^\iota M_2^{-1}$  .

Let  $N_1 = M_1^{-1} \operatorname{diag}(\nu) M_1$  and  $N_3 = {}^{\iota} M_3 \operatorname{diag}(\nu) {}^{\iota} M_3^{-1}$ . One can verify the hypotheses of Theorem 4a) to obtain

$$rac{G_{\scriptscriptstyle D_1}\!(2L)}{|\det D_{\scriptscriptstyle 1}|^{1/2}} = rac{G_{\scriptscriptstyle D_1}\!(2N_{\scriptscriptstyle 1}\!LN_{\scriptscriptstyle 3})}{|\det D_{\scriptscriptstyle 1}|^{1/2}} = (C'/D_{\scriptscriptstyle 1},\,2C_{\scriptscriptstyle 0})rac{G_{\scriptscriptstyle D_1}\!(2C_{\scriptscriptstyle 0})}{|\det D_{\scriptscriptstyle 1}|^{1/2}}$$

where  $C'=M_1^{-1}(\lambda\nu)M_1$  and  $C_0=M_1^{-1}(\nu)^tM_3^{-1}$ . By Corollary 1,  $(C'/D_1,2C_0)(\lambda\nu/b_1)$ .

Choose an ideal  $\mathfrak{m}_5$  with  $(\mathfrak{m}_5,2\mathfrak{p})=1$  such that  $\nu=\nu_1\nu_2$  with  $(\nu_1)=\mathfrak{p}\mathfrak{m}_1\mathfrak{m}_5^{-1}$  and  $(\nu_2)=\mathfrak{D}\mathfrak{m}_5\mathfrak{m}_3$ . Let  $C_0=C_1C_2$  with  $C_1=M_1^{-1}\operatorname{diag}(\nu_1)M_5$  and  $C_2=M_5^{-1}\operatorname{diag}(\nu_2)^tM_3^{-1}$ . Note that  $|\det C_1|=p$  and  $C_2$  is unimodular. Using Theorems 3, 5, and 2,

$$egin{aligned} rac{G_{D_1}\!(2C_0)}{|\det D_1|^{1/2}} &= e\!\left\{rac{1}{4}\operatorname{sgn}D_1^tC_0\!
ight\}\!rac{G_{2C_0}\!(-D_1)}{|\det 2C_1|^{1/2}} \ &= e\!\left\{rac{1}{4}\operatorname{sgn}\delta_1\!
u
ight\}\!rac{G_2\!(-D_1^tC_0)}{2^{n/2}}\!\cdot\!rac{G_{C_1}\!(-2D_1^tC_2)}{p^{1/2}} \ &= e\!\left\{rac{1}{4}\operatorname{sgn}\delta_1\!
u
ight\}\!e\!\left\{rac{1}{4}\operatorname{sgn}_4\!(-D_1^tC_0)\!
ight\}\!arepsilon_p\!\left(rac{-p
u_1^{-1}\delta_1
u_2}{\mathfrak{p}}
ight) \ &= e\!\left\{rac{1}{4}\left[\operatorname{sgn}\delta_1
u - \operatorname{sgn}_4\delta_1
u
ight]\!
ight\}\!arepsilon_p^{-1}\!\left(rac{p
u^{-1}\delta_1}{\mathfrak{p}}
ight). \end{aligned}$$

Here we used  $\lambda = r \delta_2/2$  but we could also have set  $\lambda = 2\beta^2$  for  $\beta \in \mathfrak{Dm}_1\mathfrak{m}_3$ , say  $(\beta) = \mathfrak{Dm}_1\mathfrak{m}_3\mathfrak{b}$ , with  $(\mathfrak{b}, 2\mathfrak{p}) = 1$ . Since  $(2\lambda/\mathfrak{b}_1) = 1$  for this  $\lambda$ , we have shown that

$$rac{G_{\scriptscriptstyle D_1}\!(2L)}{\left|\det D_1
ight|^{1/2}} = e \Big\{rac{1}{4} \left[\operatorname{sgn}\delta_{\scriptscriptstyle 1}\!
u - \operatorname{sgn}_{\scriptscriptstyle 4}\delta_{\scriptscriptstyle 1}\!
u
ight] \Big\} arepsilon_{\scriptscriptstyle 1}^{-1}\!\!\chi(\delta_{\scriptscriptstyle 1}) \,.$$

Let  $\delta_1' = \delta_1 + \alpha$  with  $\alpha \in 4\mathfrak{D}\mathfrak{m}_1^2\mathfrak{b}^2$  and  $(\delta_1', \mathfrak{p}) = 1$ . Let  $\delta_1' \equiv \delta_1 \operatorname{mod}(\infty)$ . Set  $D_1' = M_1^{-1}\operatorname{diag}(\delta_1')M_3 = D_1 + (2L)A$  where  $A = {}^tM_3\operatorname{diag}(\alpha/(2\lambda))M_3$  is an integral even symmetric matrix. Applying Theorem 1 and the periodicity of the Gauss sum,

$$egin{aligned} rac{G_{{\scriptscriptstyle D}_1}\!(2L)}{|\det D_1|^{1/2}} &= e\!\left\{rac{1}{4}\,\mathrm{sgn}\,\delta_1\!\lambda
ight\}\!rac{G_{{\scriptscriptstyle 2}{\scriptscriptstyle L}}\!(-D_1)}{|\det 2L|^{1/2}} \ &= e\!\left\{rac{1}{4}\,\mathrm{sgn}\,\delta_1'\!\lambda
ight\}\!rac{G_{{\scriptscriptstyle 2}{\scriptscriptstyle L}}\!(-D_1')}{|\det 2L|^{1/2}} &= rac{G_{{\scriptscriptstyle D}_1'}\!(2L)}{|\det D_1'|^{1/2}}\,. \end{aligned}$$

This implies that  $\chi(\delta_1) = \chi(\delta_1')$  whenever  $\delta_1 \equiv \delta_1' \mod 4\mathfrak{Dm}_1^2 \delta_1^2(\infty)$  and  $(\delta_1', \mathfrak{p}) = 1$ . If  $(\delta_1', \mathfrak{p}) \neq 1$ , define  $\chi(\delta_1')$  to be  $\chi(\delta_1)$ .

Clearly  $\chi(\delta_1) = \chi(\delta_1\mu^2)$  for any  $\mu \in \mathfrak{m}_1\mathfrak{m}_3\mathfrak{b}$  with  $(\mu, 2\mathfrak{p}) = 1$ . Choose any  $\alpha \in 4\mathfrak{D}\mathfrak{m}_1\mathfrak{m}_3^{-1}$ ; thus,  $\alpha\mu^2 \in 4\mathfrak{D}\mathfrak{m}_1^2\mathfrak{b}^2$ . Suppose that  $\delta_1 + \alpha \equiv \delta_1 \operatorname{mod}(\infty)$ . Then  $\chi(\delta_1) = \chi(\delta_1\mu^2) = \chi(\delta_1\mu^2 + \alpha\mu^2) = \chi(\delta_1 + \alpha)$ . We conclude that  $\chi$  is a character  $\operatorname{mod} 4\mathfrak{D}\mathfrak{m}_1\mathfrak{m}_3^{-1}(\infty)$ , which proves the theorem.

The proof of this theorem illustrates how the theorems regarding symplectic Gauss sums and Jacobi symbols can be used. These methods also apply to a theorem of Andrianov and Maloletkin [1]. They define a theta function involving a quadratic form of m variables, embed it into the symplectic theta function, and thus calculate the transformation formula when m is even. The author [11] has already extended their theorem to include m odd by using an analogy of Dirichlet's theorem concerning primes in an arithmetic progression. This is actually stronger than we need. Without reproducing the arguments of [1] and [11], we only note that the problem reduces to evaluation of a Gauss sum  $G_{\tilde{\rho}}(\tilde{C})$  $|\det ilde{D}|^{1/2}$ . Here  $ilde{D}=I_m \otimes D$  and  $ilde{C}=F^{-1} \otimes C$ . F is an integral even symmetric  $m \times m$  matrix with level q,  $C \equiv 0 \mod q$ , and after a suitable translation we may assume that  $(\det D, 2 \det C) = 1$ . Replacing C by  $4q^2C$  does not change the Gauss sum, so we assume that  $(q^{-1}C, D)$  is CESD. Let  $qF^{-1} = \left(\frac{a_1}{b_1}\Big|^{\iota} \frac{b_1}{F_1}\right)$  where  $F_1$  is an integral even symmetric  $(m-1) \times (m-1)$  matrix. Using Lemma 1a),

$$rac{G_{I_m}(qF^{-1} igotimes q^{-1}C)}{|\det D|^{m/2}} = rac{G_{\scriptscriptstyle D}([a_{\scriptscriptstyle 1} - {}^tb_{\scriptscriptstyle 1}F_{\scriptscriptstyle 1}^{-1}b_{\scriptscriptstyle 1}]q^{-1}C)}{|\det D|^{1/2}} \cdot rac{G_{I_{m-1} igotimes D}(F_{\scriptscriptstyle 1} igotimes q^{-1}C)}{|\det D|^{(m-1)/2}}$$

The first factor on the right becomes

$$([a_{\scriptscriptstyle 1}-{}^{\iota}b_{\scriptscriptstyle 1}F_{\scriptscriptstyle 1}^{\scriptscriptstyle -1}b_{\scriptscriptstyle 1}]qI/D,\,C)\!\cdot\!rac{G_{\scriptscriptstyle D}(C)}{|\det D|^{\scriptscriptstyle 1/2}}\,.$$

Continuing this procedure with the obvious definitions and using Theorem 7b) to multiply the Jacobi symbols, we finally get

$$\left(\prod_{i=1}^m (a_i - {}^tb_iF_i^{-1}b_i)qI/D, \ C\right) \cdot \left[rac{G_D(C)}{|\det D|^{1/2}}
ight]^m.$$

Now  $\prod_{i=1}^m (a_i - {}^tb_iF_i^{-1}b_i)q = \det(q^2F^{-1})$  and so using Theorem 8b), one obtains

$$\frac{G_{\scriptscriptstyle \tilde{D}}(\tilde{C})}{|\det \tilde{D}|^{1/2}} = \Big(\frac{\det F}{\det D}\Big) \Big[\frac{G_{\scriptscriptstyle D}(C)}{|\det D|^{1/2}}\Big]^{\scriptscriptstyle m}\,.$$

22 ROBERT STYER

The Gauss sum on the right can be evaluated using Theorems 3, 4, and 2 for any known (C, D), In particular, if det D is odd squarefree, then the Gauss sum on the left equals  $(2^m \det F/\det D)$ .  $\prod_{p|\det D} \varepsilon_p^m(c^m/p)$  where each c is a diagonal element of  $pD^{-1}C$  with (c, p) = 1. This gives an alternate way to calculate the transformation formula when the quadratic form has an odd number of variables, and illustrates again the usefulness of the symplectic Gauss sum and symplectic Jacobi symbol.

# **BIBLIOGRAPHY**

- [1] Andrianov, A. N. and Maloletkin, G. N., Behavior of theta series of degree n under modular substitutions, Math USSR-Izv., 9 (1975), No. 2, 227-241.
- [2] Eichler, Martin, Introduction to the Theory of Algebraic Numbers and Functions, Academic Press, New York, 1966, 46-52.
- [3] Friedberg, Solomon, Theta series, the Weil representation, and the corresponding eighth root of unity, preprint.
- [4] Hasse, Helmut, Number Theory, Springer-Verlag, Berlin, 1980, p. 86.
- [5] Hecke, Erich, Vorlesungen über die Theorie der algebraischen Zahlen, Chelsea, New York, 1948, 218-249.
- [6] Lang, Serge, Algebraic Number Theory, Addison-Wesley, Reading, Mass. 1970, p. 64.
- [7] Maass, Hans, Siegel's Modular Forms and Dirichlet Series, Lecture Notes in Mathematics, 216, Springer-Verlag, Berlin, 1971, 155-164.
- [8] Newman, Morris, Integral Matrices, Pure and Applied Mathematics, 45, Academic Press, New York, 1972.
- [9] Stark, H. M., On the transformation formula for the symplectic theta function and applications, J. Fac. Sci., Univ. of Tokyo, 29 (1982), No. 1, 1-12.
- [10] Stark, H. M., Some examples of modular forms over number fields. I. to appear.
- [11] Styer, Robert, Prime determinant matrices and the symplectic theta function, Amer. J. Math., 106 #3 (1983), 645-665.
- [12] Weber, H., Ueber die mehrfachen Gaussischen Summen, J. Reine Angew. Math., 74 (1872), 14-56.

Department of Mathematics Villanova University Villanova, PA 19085 USA