ON THE TWO-ADIC DENSITY OF REPRESENTATIONS BY QUADRATIC FORMS

IRMA REINER
1. Introduction. The problem of determining $A_q(S, T)$, the number of solutions of $X'SX \equiv T \pmod{q}$, where $S^\text{sym}$ and $T^\text{sym}$ are symmetric integral matrices, has been considered by C. L. Siegel [2, pp. 539-547]. He obtained explicit formulas for $A_q(S, T)$ when $q = p^n$, where $p$ is a prime not dividing $2|S||T|$. We wish to determine both $A_2(S, T)$ and $A_8(S, T)$ when $|S||T|$ is odd. Siegel has shown that the calculation of $A_8(S, T)$, for $|S||T|$ odd, is sufficient to give results when the modulus is replaced by a higher power of 2. Moreover, his work for composite moduli does not exclude a power of 2 as a factor.

We shall follow the pattern of Siegel's work, modifying it by the use of canonical forms established by B. W. Jones [1, pp. 715-727] and Gordon Pall for symmetric matrices in $G_2$, the ring of 2-adic integers. (Clearly, $A_q(S, T)$ depends only on the classes of $S$ and $T$ in $G_q$, the ring of $q$-adic integers). We shall calculate $A_2(S, T)$ combinatorially and $A_8(S, T)$ by the use of exponential sums.

2. Recursion formula. For convenience, we state here the following theorem of Jones:

Every quadratic form with matrix in $G_2$ and with unit determinant, $D$, is equivalent to one of the following:

(a) $x_1^2 + x_2^2 + \cdots + ax_r^2 + bx_{r-1}^2 + cx_r^2$,

where $a, b, c$ take one of the following sets of values:

(1, 1, 1) or (1, 3, 3) for $D \equiv 1 \pmod{8}$,
(1, 1, 5) or (1, 3, 7) for $D \equiv 5 \pmod{8}$,
(1, 1, 3) or (3, 3, 3) for $D \equiv 3 \pmod{8}$,
(1, 1, 7) or (3, 3, 7) for $D \equiv 7 \pmod{8}$,

while if $r=2$, $b$ and $c$ take one of the following sets of values:

(1, 1) or (3, 3) for $D \equiv 1 \pmod{8}$,
(1, 5) or (3, 7) for $D \equiv 5 \pmod{8}$,
(1, 3) for $D \equiv 3 \pmod{8}$,
(1, 7) for $D \equiv 7 \pmod{8}$.

(b) A sum of binary forms of the two types: $f = 2x_1^2 + 2x_2x_3 + 2x_2^2$. 

Received October 3, 1955. The author wishes to thank Professor Irving Reiner for helpful suggestions during the preparation of this paper.
Here, we may at will choose one of types $f$ and $g$ and require that all but at most one of the binary forms be of that type.

When (a) applies, we will call the matrix of the form \emph{even}; when (b) applies, we will call the matrix \emph{odd}.

We assume hereafter that $|S||T|$ is odd. Then we remark immediately, as in Siegel’s paper, that all representations of $T$ by $S$ modulo $2^a$, where $a=1$ or $3$, are primitive. Following the line of Siegel’s proof, we now obtain the recursion formula.

Taking $T=T_0^{(r)} + T_1^{(n-r)}$, from the canonical forms above, we let $\chi$ designate the first $r$ columns of $X$, where $X'SX\equiv T$ (mod $2^a$). Then

\begin{equation}
\chi'S\chi \equiv T_0 \pmod{2^a}.
\end{equation}

As remarked above, any solution $\alpha$ of (1) is primitive, and so can be completed to a unimodular matrix $U_1=\alpha A$ in $G_2$. We wish to alter $U_1$ so that

\begin{equation}
U_1SU_1 \equiv \begin{pmatrix} T_0 & N' \\ N & S_1 \end{pmatrix} \pmod{2^a},
\end{equation}

with $N$ designating an $m-r$ by $r$ null matrix. To do this, we call $E$ the matrix obtained from $U_1SU_1$ by deleting the first $r$ columns and the last $m-r$ rows. Then, noting that the determinant of $T_0$ is a 2-adic unit, we multiply $U_1$ by

\[
\begin{pmatrix} I^{(r)} & -T_0^{-1}E' \\ N & I^{(m-r)} \end{pmatrix}
\]

to achieve the desired form (2).

Now if there exists a $C$, with its first $r$ columns congruent to $\alpha$ (mod $2^a$), such that $C'SC\equiv T$ (mod $2^a$), we complete $C$ to a unimodular matrix in $G_2$, say $U_2=(CA_1)$. Since $U_1$ and $U_2$ are both completions of $\alpha$, consideration of $U_1^{-1}U_2$ shows us that

\begin{equation}
C \equiv U_1^r \begin{pmatrix} I^{(r)} & B \\ N & C_1 \end{pmatrix} \pmod{2^a},
\end{equation}

where $C_1$ and the $r$-rowed $B$ are in $G_2$. Using (2) and (3) in $C'SC\equiv T$ (mod $2^a$), we find that $B$ is null and that $C_1S_1C_1\equiv T_1$ (mod $2^a$). Thus, we obtain each different solution $X$ (mod $2^a$) exactly once by first determining all different solutions $\chi$ (mod $2^a$) of (1), then finding a $U_1$ as above for each such $\chi$, and finally determining for the corresponding $S_1$ all different solutions of $X'S_1X\equiv T_1$ (mod $2^a$). Thus

\[
A_{2a}(S, T) = \sum_\alpha A_{2a}(S_1, T_1).
\]

3. Combinatorial calculation of $A_{2a}(S, T)$. We use canonical forms,
taken modulo 2, in the following cases:

Case 1. We assume $T$ even and $S$ odd. Here we clearly have no solution.

Case 2. We assume both $S$ and $T$ even.

2.1. For $n=1$, $A_2(S, T)=2^{m-1}$.

Proof. We seek solutions $\{x_i\}$ such that
\[
\sum_{i=1}^{m} x_i^2 \equiv 1 \pmod{2}.
\]
Since a parity change in one $x_i$ changes the parity of the sum, we see that $A_2(S, T)$ is half of $2^m$.

2.2. For $n=2$, $A_2(S, T)=2^{m-1} \cdot 2^{m-2}$, for even $m$.

$A_2(S, T)=(2^{m-1}-1) \cdot 2^{m-2}$, for odd $m$.

Proof. We use Case 2.1 with the recursion formula. We wish to show that for every solution $\alpha$ of (4), except one where $m$ is odd and each component of $\alpha$ is 1, $A_2(S, T)>0$; that is, $S_i$ is even. Here we have the additional conditions:

\[
\sum_{i=1}^{m} y_i = 1 \pmod{2},
\]
\[
\sum_{i=1}^{m} x_i y_i = 0 \pmod{2}.
\]
But there is an obvious $\{y_i\}$ satisfying (5) and (6) with any solution $\{x_i\}$ of (4) which has a zero element; and clearly there is no such $\{y_i\}$ if all the elements of $\{x_i\}$ are 1. Hence, we have our result.

2.3. For general $m$ and $n$, ($n>1$),

$A_2(S, T)=F(m) \cdot F(m-1) \cdots F(m-n+2) \cdot 2^{m-n}$,

where $F(m)=2^{m-1}$ for even $m$ and $F(m)=2^{m-1}-1$ for odd $m$.

Proof. Now $S_i$ depends only on $\alpha$ and not on $n$, so that Case 2.2 tells us that $S_i$ is even except when $m$ is odd and each element of $\alpha$ is 1. Then the above result follows easily from the recursion formula.

Case 3. We assume both $S$ and $T$ odd.

3.1. For $n=2$, $A_2(S, T)=(2^m-1) \cdot 2^{m-1}$.

Proof. We want solutions, $\{x_i\}$ and $\{y_i\}$, of
\[
x_1 y_2 + x_2 y_1 + \cdots + x_{m-1} y_m + x_m y_{m-1} \equiv 1 \pmod{2}.
\]
Now \(\{x_i\}\) cannot be null if (7) is to hold; also there is an obvious \(\{y_i\}\) satisfying (7) for each non-null \(\{x_i\}\). Let us fix a non-null \(\{x_i\}\) and call any \(\{y_i\}\) satisfying (7) with our fixed \(\{x_i\}\) a "solution", otherwise a "non-solution". Then, since, modulo 2, the sum of two "solutions" is a "non-solution" and the sum of a "solution" with a "non-solution" is a "solution", we have our result.

3.2. For general \(m\) and \(n\),
\[
A_2(S, T) = (2^m - 1) \cdot 2^{m-1} (2^{m-2} - 1) \cdot 2^{m-3} \cdots (2^{m-n+2} - 1) \cdot 2^{m-n+1}.
\]

Proof. Equivalent matrices in \(G_2\) have the same parity, which is clearly unchanged when the matrices are taken modulo 2. Thus, from (2), since \(S\) is odd, so is
\[
S_i + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.
\]
Hence \(S_i\) is odd, and our result follows.

Case 4. We assume that \(S\) is even and \(T\) odd.

4.1. For \(n=2\),
\[
A_2(S, T) = (2^{m-1} - 1) 2^{m-2}, \text{ if } m \text{ is odd.}
\bar{A}_2(S, T) = (2^{m-1} - 2) 2^{m-2}, \text{ if } m \text{ is even.}
\]

Proof. We want solutions \(\{x_i\}\) and \(\{y_i\}\), of
\[
\sum_{i=1}^m x_i^2 = 0, \quad \sum_{i=1}^m y_i^2 = 0, \quad \sum_{i=1}^m x_i y_i = 1,
\]
all taken modulo 2. Let us fix \(\{x_i\}\) satisfying the first of these and consider the \(2^{m-1}\) incongruent \(\{y_i\}\) which satisfy the second. Of these \(\{y_i\}\), we call those satisfying the final congruence with our fixed \(\{x_i\}\) "solutions" and those not doing so "non-solutions". By an argument similar to that used in Case 3.1, we see that exactly half the \(2^{m-1}\) choices of \(\{y_i\}\) are "solutions", except when \(\{x_i\}\) is the null vector or, with \(m\) even, \((1, 1, \cdots, 1)\). There is no "solution" \(\{y_i\}\) corresponding to either of these exceptional \(\{x_i\}\).

4.2. For general \(m\) and \(n\),
\[
A_2(S, T) = (2^{m-1} - p) 2^{m-2} (2^{m-3} - p) 2^{m-4} \cdots (2^{m-n+1} - p) 2^{m-n},
\]
where \(p=1\) for odd \(m\) and \(p=2\) for even \(m\).

Proof. Using (2) again, we observe that \(S_i\) is even. (See Case 3.2.). Then the recursion formula implies our result.

4. Determination of \(A_2(S, T)\). We will assume throughout the fol-
lowing cases that $S$ and $T$ are in appropriate canonical forms as given in §2.

*Case 1.* We assume $T$ is even.

Clearly, $A_8(S, T)=0$ for $S$ odd and $T$ even; so we will also assume $S$ is even.

1.1. Let $n=1$. Here $T=(t)$. For $\omega$ a primitive 8th root of unity, we have

\begin{equation}
8A_8(S, T) = \sum_{h, \alpha \pmod{8}} \omega^\alpha, \quad Y = h(a_is_i^2 + \cdots + a_ms_m^2 - t),
\end{equation}

where $h$ and the elements $a_i, a_2, \cdots, a_m$ of the vector $a$ run through a complete residue system modulo 8, and where the diagonal elements of $S$ are the odd $s_1, s_2, \cdots, s_m$. Calling

$$
\sum_{\alpha \pmod{8}} \omega^{h\alpha^2} = [hs],
$$

we get

\begin{equation}
8A_8(S, T) = \sum_{h=1}^{7} [hs_1][hs_2] \cdots [hs_m] \omega^{-ht} + 8^m.
\end{equation}

We observe that $[hs_1]=4\omega^{h\alpha^2}$, for odd $h$; $[hs_1]=0$, for $h \equiv 4 \pmod{8}$; $[hs_1]=4\omega^{h\alpha^2}$, for $h \equiv 2 \pmod{8}$; and $[hs_1]=4\omega^{h\alpha^2}$, for $h \equiv 6 \pmod{8}$.

Then, let us call $u = \sum_{i=1}^{m} s_i - t \pmod{8}$, and define $f(u)=1$ for $u \equiv 0 \pmod{8}$, $f(u)=-1$ for $u \equiv 4 \pmod{8}$, and $f(u)=0$ for $u \equiv 0 \pmod{4}$. Also define

$$
K = (-1)^{(s_1-1)/2} + (-1)^{(s_2-1)/2} + \cdots + (-1)^{(s_m-1)/2} - 2t \pmod{8}.
$$

Then direct calculation gives from (9),

$$
8A_8(S, T) = 8^m + 4^{m+1}f(u) + 2(4\sqrt{2})^m \cos \frac{K\pi}{4}.
$$

1.2. Let $n=2$. We will (a) ascertain when $S$ is even and (b) show that two even $S_i$'s corresponding to different solutions $\alpha$ are equivalent in $G_2$. Then the result follows from the recursion formula.

(a) Let $T=t_1 + t_2$. Since parity is the same modulo 2 or modulo 8, we see from §3, Case 2.2, that of all solutions, $\alpha$, of $\chi'S_i \equiv t_1 \pmod{8}$, those and only those which reduce, modulo 2, to the vector $(1, 1, \cdots, 1)$ will yield odd $S_i$'s. For such an $\alpha$, $\sum_{i=1}^{m} a_is_i \equiv t_1 \pmod{8}$ implies $\sum_{i=1}^{m} s_i \equiv t_1 \pmod{8}$. But, equally well, if $S$ and $t_1$ are such that $\sum_{i=1}^{m} s_i \equiv t_1 \pmod{8}$,
then \( \sum_{i=1}^{m} a_i s_i = t_i \) (mod 8) holds for arbitrary odd \( a_i \). Thus, if \( \sum_{i=1}^{m} s_i = t_1 \) (mod 8), we get \( 4^m \) number of \( a_i \)'s, solutions of \( \chi S_t = t_1 \) (mod 8), which yield odd \( S_t \)'s; otherwise, none.

(b) Now let \( a \) be such that \( S_i \) is even. From [1], we see that two even matrices of odd determinant, which are congruent modulo 8, are in the same class in \( G_2 \). Thus, using (2), we obtain:

\[
t_{i_1} | S_i | = | S | \pmod{8} \quad \text{and} \quad \lambda (t_{i_1} + S_i) = \lambda (S),
\]

where \( \lambda (S) \) is the class invariant defined as 1 if \( 4j \) or \( 4j+1 \) of the diagonal elements of a diagonalized form of \( S \) are congruent to 3 modulo 4 and –1 if \( 4j+2 \) or \( 4j+3 \) are congruent to 3 modulo 4. These two conditions determine uniquely, independently of \( a \), the class of \( S_i \) in \( G_2 \).

**Example.** Let \( S \) be of type \((1, 3, 3)\) as given in \( \S \, 2, \, m \geq 3 \), and \( t_1 = 5 \). Then the determinantal relation gives an even \( S_1 \) of type \((1, 1, 5)\) or \((1, 3, 7)\). But the \( \lambda \)-condition admits only the second of the two, so any even \( S_1 \) is of type \((1, 3, 7)\).

Thus we have

\[
8^2 \cdot A_2 (S, T) = (8^m + 4^{m+1} f(u_0) + 2 (4 \sqrt{2})^m \cos (K_0 / 4) - 8 \cdot 4^m h(u_0))
\times (8^{m-1} + 4^m f(u_1) + 2 (4 \sqrt{2})^{m-1} \cos (K_1 / 4)),
\]

where \( u_0 \) and \( K_0 \) are arguments obtained from \( S \) and \( t_1 \) as above; \( u_1 \) and \( K_1 \) are arguments similarly obtained from \( S_1 \) and \( t_2 \); and \( h(u_0) \) is defined as 1 if \( u_0 \equiv 0 \pmod{8} \) and as 0 otherwise.

1.3. Let \( n \geq 2 \). Since the process of obtaining an \( S_i \) from a given pair, \( S \) and \( t_i \), is the same for \( n = 2 \) and for \( n > 2 \), we may use 1.2 above to obtain

\[
8^n A_n (S, T) = (8^{m-n+1} + 4^{m-n+2} f(u_{n-1}) + 2 (4 \sqrt{2})^{m-n+1} \cos (\pi K_{n-1} / 4))
\times \prod_{j=m-n+2}^{m} (8^j + 4^{j+1} f(u_{m-j}) + 2 (4 \sqrt{2})^{j} \cos (\pi K_{m-j} / 4) - 8 \cdot 4^{j} h(u_{m-j})),
\]

where, for each \( i \), \( u_i \) and \( K_i \) come from \( S_i \) and \( t_{i+1} \), as above.

(The process of finding successive \( S_i \) and \( t_i \), and hence of successive \( K_i, f(u_i) \), and \( h(u_i) \), is easy in practice, as evidenced by the example above. Explicit but complicated formulas could be given.)

**Case 2.** We assume \( S \) and \( T \) are both odd. We will first take \( n = 2 \).

2.1. We suppose that

\[
T = \begin{pmatrix} b & 1 \\ 1 & b \end{pmatrix} \quad \text{and} \quad S = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},
\]

\[
= \begin{pmatrix} 1 & b \\ b & 1 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \cdots + \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},
\]

then \( \sum_{i=1}^{m} a_i s_i = t_i \) (mod 8) holds for arbitrary odd \( a_i \). Thus, if \( \sum_{i=1}^{m} s_i = t_1 \) (mod 8), we get \( 4^m \) number of \( a_i \)'s, solutions of \( \chi S_t = t_1 \) (mod 8), which yield odd \( S_t \)'s; otherwise, none.
where \( b = 0 \) or 2. Then we seek solutions of:

\[
F(x) = 2(x_1 x_2 + x_3 x_4 + \cdots + x_{m-1} x_m) \equiv b \pmod{8}
\]

\[
G(y) = 2(y_1 y_2 + y_3 y_4 + \cdots + y_{m-1} y_m) \equiv b \pmod{8}
\]

\[
H(x, y) = x_1 y_2 + x_2 y_1 + x_3 y_3 + \cdots + x_{m-1} y_m + x_m y_{m-1} \equiv 1 \pmod{8}.
\]

Thus

\[
8^3 A_8(S, T) = \sum_{h, k, l} \omega^{F+b(h) + G+b(k) + H-l} \omega_{x_1, x_2, y_1, y_2}^{(S)},
\]

where \( \omega = e^{it/4} \) and \( h, k, l \), and the components of the vectors \( x \) and \( y \) all run through complete residue systems modulo 8. Then, letting

\[
R = \sum_{x_1, x_2, y_1, y_2} \omega_{x, y}^{(S)} EXP = 2x_1 x_2 h + 2y_1 y_2 k + (x_1 y_2 + x_2 y_1),
\]

we get

\[
8^3 A_8(S, T) = \sum_{h, k, l} R_{m/2}^{m/2} \omega^{-l-b} R_{m/2}^{m/2}.
\]

We note that, for \( l \) odd, replacement of \( h \) by \( lh \), of \( k \) by \( lk \), of \( x_1 \) by \( lx_1 \), and of \( y_1 \) by \( ly_1 \) in \( EXP \), the displayed exponent of (10), shows that \( \sum_{h, k} R_{m/2}^{m/2} \) is independent of \( l \). A similar argument works for \( l \equiv 2 \pmod{4} \).

For \( l \equiv 0 \pmod{8} \), we have

\[
R = 2^{l+r(h)} \cdot 2^{l+r(k)},
\]

where \( r(t) = 0 \) if \( t \equiv 1 \pmod{2} \), \( r(t) = 1 \) if \( t \equiv 2 \pmod{4} \), and \( r(t) = 2 \) if \( t \equiv 0 \pmod{4} \).

For \( l \equiv 4 \pmod{8} \) and \( h \) odd, we let \( z = x_1 h + 2y_1 \pmod{8} \), and replace \( y_1 \) by \( z \) as a variable in \( EXP \). Then, summing first on \( x_1 \), we get

\[
R = 2^{2+l+r(k)}.
\]

For \( l \equiv 4 \pmod{8} \) and \( h = 2h_1 \), we let \( z = x_1 h_1 + y_1 \pmod{8} \) and again replace \( y_1 \) by \( z \) as a variable in \( EXP \). Summing first on \( x_1 \) and \( z \), we readily get

\[
R = 2^l, \text{ for } h_1 k \equiv 1 \pmod{2}\]

\[
R = 2^m, \text{ for } h_1 k \equiv 0 \pmod{4} \text{ or } h_1 k \equiv 2 \pmod{4} \text{ and } k \equiv 1 \pmod{2}\]

\[
R = 2^{2l}, \text{ for } h_1 k \equiv 2 \pmod{4} \text{ and } k \equiv 0 \pmod{2}.
\]

Summing first on \( l \) in (11), we get by straightforward calculation:

\[
A_8(S, T) = 2^{m-7}(2^m + 2^{m/2} - 2), \quad \text{for } b = 0.
\]

\[
A_8(S, T) = 2^{m-7}(2^m - 3 \cdot 2^{m/2} + 2), \quad \text{for } b = 2.
\]

2.2. We suppose that
Then, using the same $R$ as before and letting

$$v = \sum_{x,y,u,\nu} (8)$$

where $P = 2(xy + x^2 + y^2)h + 2(uv + u^2 + v^2)k + (uy + vx + 2ua + 2vy)l$, we get

$$8^3 A_3(S, T) = \sum_{h,k,l (8)} R^{(m-2)/2} V \omega^{-1-bh-bk}.$$ 

To evaluate $V$, we use repeatedly:

$$\sum_{u (8)} \omega^{2au + d} = 0, \text{ if } d \equiv 2 \pmod{4} \text{ or if } d \equiv 1 \pmod{2}$$

$$= -4\omega^{2a} + 4, \text{ if } d \equiv 4 \pmod{8}$$

$$= 4\omega^{2a} + 4, \text{ if } d \equiv 0 \pmod{8}.$$

We obtain:

(i) For $l$ odd, $V = 64$.

(ii) $V$ is the same for $l = 2$ and $l \equiv 6 \pmod{8}$.

(iii) For $l \equiv 0 \pmod{8}$, $V = g(h)g(k)$, where we define $g(t) = 64$ for $t \equiv 0 \pmod{4}$, $g(t) = 16$ for $t \equiv 1 \pmod{2}$, and $g(t) = -32$ for $t \equiv 2 \pmod{4}$.

(iv) For $l \equiv 4 \pmod{8}$, we have:

(a) When $h$ is odd, $V = 16g(k)$.
(b) When $h$ or $k \equiv 0 \pmod{4}$, $V = 2^0$.
(c) When $h \equiv 2 \pmod{4}$, $V = -2$, when $k$ is odd, and $V = -2^{11}$, when $k \equiv 2 \pmod{4}$.

We sum first on $l$ in (12), using our results for $R$ and considering only $l \equiv 0 \pmod{4}$. We get

$$A_3(S, T) = 2^4 \left(2 \cdot 2^8(n-2) - 2^{11}(m-2)/2 - 2^{5}(m-2)\right), \quad \text{for } b = 0.$$ 

$$A_3(S, T) = 2^4 \left(2 \cdot 2^8(n-2) + 3 \cdot 2^{11}(m-2)/2 - 2^{5}(m-2)\right), \quad \text{for } b = 2.$$ 

For $n > 2$, when $S$ and $T$ are odd, we will use our results for $n = 2$, along with the recursion formula. The successive canonical forms of $T, T_1, \cdots$ are clear; that is, $T_i$ is obtained from $T$ by removing the initial binary block, etc. $T_1$ is thus odd and known. From

$$S_1 \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \equiv U_1SU_1, \quad \text{(mod 8)},$$

we deduce $-|S_1| = |S|$ (mod 8) and the oddness of $S_1$. Thus $S_i$ is easily determined classwise uniquely. The same holds true, of course, for successive $S_i$.

**Case 3.** We assume $S$ is even and $T$ is odd. Considering first
\( n=2 \), we let \( s_1, s_2, \ldots, s_m \) be the diagonal elements in the canonical form of \( S \), and let \( T \) be

\[
\begin{pmatrix}
  b & 1 \\
  1 & b
\end{pmatrix},
\]

where \( b=0 \) or 2. Then we seek solutions of:

\[
\begin{align*}
  u &= x_1^2s_1 + x_2^2s_2 + \cdots + x_m^2s_m \equiv b \pmod{8} \\
  v &= y_1^2s_1 + y_2^2s_2 + \cdots + y_m^2s_m \equiv b_m \pmod{8} \\
  r &= x_1y_1s_1 + x_2y_2s_2 + \cdots + x_my_ms_m \equiv 1 \pmod{8}.
\end{align*}
\]

Here

\[
8^3A_8(S, T) = \sum_{h, k, l \in \mathbb{Z}} \omega^{h(u-b)+k(v-b)+l(r-1)}.
\]

Let \( \omega^i = \omega_i \) and call

\[
f_i(h, k, l) = \sum_{x, y \in \mathbb{Z}} \omega^{hx^2+txy+ky^2}.
\]

Then

\[
(13) \quad 8^3A_8(S, T) = \sum_{h, k, l} f_1 f_2 \cdots f_m \omega^{-hb-kb-l}.
\]

We calculate \( f_i \), considering the value of \( l \pmod{8} \), and note that as before we need consider only \( l \equiv 0 \pmod{4} \). We get:

<table>
<thead>
<tr>
<th>( h )</th>
<th>( k )</th>
<th>( l \pmod{8} )</th>
<th>( f_i )</th>
</tr>
</thead>
<tbody>
<tr>
<td>odd</td>
<td>odd</td>
<td>0</td>
<td>( c = 16\omega_i^{h+k} )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>( -c = -16\omega_i^{h+k} )</td>
</tr>
<tr>
<td>odd</td>
<td>even</td>
<td>0</td>
<td>( d = 16\omega_i^{h+k} + 16\omega_i^h )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>( e = -16\omega_i^{h+k} + 16\omega_i^h )</td>
</tr>
<tr>
<td>even</td>
<td>even</td>
<td>0</td>
<td>( p = 16(\omega_i^{h+k} + \omega_i^h + \omega_i^k + 1) )</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>( q = 16(-\omega_i^{h+k} + \omega_i^h + \omega_i^k + 1) )</td>
</tr>
</tbody>
</table>

Then from (13), we get

\[
8^3A_8(S, T) = 2 \sum_{h \text{ odd \atop k \text{ even}}} \left( \prod_{i=1}^{m} d_i - \prod_{i=1}^{m} e_i \right) \omega^{-hb-kb} + (1 - (-1)^m) \left( \sum_{h, k \text{ odd}} \left( \prod_{i=1}^{m} c_i \right) \omega^{-hb-kb} \right)
\]

\[
+ \sum_{h, k \text{ even}} \left( \prod_{i=1}^{m} p_i - \prod_{i=1}^{m} q_i \right) \omega^{-hb-kb},
\]

where all the sum indices are taken modulo 8. Replacement of \( k \) by \( k+4 \) in the first summand merely changes the sign of the expression, so the first sum is zero. The second sum is easily seen to be \( 16^{m+1} \cdot \alpha(1-(-1)^m) \), where \( \alpha = 1 \) if \( \sum s_i \equiv b \pmod{4} \) and \( \alpha = 0 \) otherwise.
We consider particular contributions to the third sum, using $\omega_1^{sk} = i^sj^k$ and adjusting so that $h$ and $k$ run through a complete residue system modulo 4.

(a) For $h \equiv 2 \pmod{4}$ and all $k \pmod{4}$, we have contributed $-4\alpha(32)^m$.

(b) For $h \equiv k \equiv 2 \pmod{4}$, we get $-(-32)^m$.

(c) For $h \equiv 0 \pmod{4}$ and $k \equiv 1, 3 \pmod{4}$, we obtain

$$16^m \cdot 2^{m+1} \cdot i^{-h}(2^{m/2} \cos (\pi B/4) - 1),$$

where $B = \sum_{j=1}^{m} (i)^{j-1}$.

(d) For $h$ and $k$ odd, with $h \equiv k \pmod{4}$, we get

$$16^m(-2^{m+1}2^{m/2} \cos (\pi B/4) + 2^{m+1} \cos (\pi B/2)).$$

(e) For $h$ and $k$ odd, with $h \equiv -k \pmod{4}$, we get $2(32)^m$.

(f) For $h \equiv k \equiv 0 \pmod{4}$, we have $16^m(2^{2m} - 2^m)$.

Thus, here

$$8^3 A_8(S, T) = 16^{m+1}\alpha(1 - (-1)^m) + 32^m(-8\alpha + (-1)^m + 4i^{-b}(2^{m/2} \cos (\pi B/4) - 1)) + 32^m(2 \cos (\pi B/2) - 2^{1+(m/2)} \cos (\pi B/4) + 2 + 2^m - 1).$$

For $n > 2$, where $S$ is even and $T$ odd, we use the recursion formula with the results for $n=2$. The successive diagonal forms of $T$ are clear. From

$$S_1 \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = U_iSU_1 \quad \pmod{8},$$

we see firstly that $S_1$ is even and secondly, that its determinant is determined modulo 8. Again, using (14) and the remarks of §4, 1.2 b, we see from the following transformations that the number of 3's, modulo 4, in a diagonal form of $S_i$ is one less than the number of 3's modulo 4, in a diagonal form of $S$; hence, $\lambda(S_i)$ is known:

$$ax^2 + 2yz \rightarrow a(x+y)^2 + 2yz = ax^2 + ay^2 + 2y(ax + z) \rightarrow$$

$$ax^2 + ay^2 + 2yz \equiv ax^2 + a(y + az)^2 - az^2 \rightarrow ax^2 + ay^2 - az^2,$$

where $a$ is odd, the congruence is taken modulo 8, and $\rightarrow$ indicates $2$-adic equivalence. Thus $S_1$ is classwise unique and easily determined.

**REFERENCES**

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any of the editors. Manuscripts intended for the outgoing editors should be sent to their successors. All other communications to the editors should be addressed to the managing editor, E. G. Straus at the University of California, Los Angeles 24, California.

50 reprints of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is $12.00; single issues, $3.50. Back numbers are available. Special price to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues, $1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 2120 Oxford Street, Berkeley 4, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 10, 1-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seymour Ginsburg</td>
<td>On mappings from the family of well ordered subsets of a set</td>
<td>583</td>
</tr>
<tr>
<td>Leon Ehrenpreis</td>
<td>Some properties of distributions on Lie groups</td>
<td>591</td>
</tr>
<tr>
<td>Marion K. Fort, Jr.</td>
<td>A geometric problem of Sherman Stein</td>
<td>607</td>
</tr>
<tr>
<td>Paul R. Garabedian</td>
<td>Calculation of axially symmetric cavities and jets</td>
<td>611</td>
</tr>
<tr>
<td>Walter Mossman Gilbert</td>
<td>Completely monotonic functions on cones</td>
<td>685</td>
</tr>
<tr>
<td>William L. Hart and T. S. Motzkin</td>
<td>A composite Newton-Raphson gradient method for the solution of systems of equations</td>
<td>691</td>
</tr>
<tr>
<td>C. W. Mendel and I. A. Barnett</td>
<td>A functional independence theorem for square matrices</td>
<td>709</td>
</tr>
<tr>
<td>Howard Ashley Osborn</td>
<td>The problem of continuous programs</td>
<td>721</td>
</tr>
<tr>
<td>William T. Reid</td>
<td>Oscillation criteria for linear differential systems with complex coefficients</td>
<td>733</td>
</tr>
<tr>
<td>Irma Reiner</td>
<td>On the two-adic density of representations by quadratic forms</td>
<td>753</td>
</tr>
<tr>
<td>Shoichiro Sakai</td>
<td>A characterization of $W^*$-algebras</td>
<td>763</td>
</tr>
<tr>
<td>Robert Steinberg</td>
<td>Note on a theorem of Hadwiger</td>
<td>775</td>
</tr>
<tr>
<td>J. Eldon Whitesitt</td>
<td>Construction of the lattice of complemented ideals within the unit group</td>
<td>779</td>
</tr>
<tr>
<td>Paul Civin</td>
<td>Correction to “Some ergodic theorems involving two operators”</td>
<td>795</td>
</tr>
</tbody>
</table>