JOURNAL OF NUMBER THEORY 4, 557–572 (1972)

Skew Circulant Quadratic Forms

DENNIS GARBANATI AND ROBERT C. THOMPSON*

Department of Mathematics, University of California Santa Barbara, Santa Barbara, California 93106

Communicated by O. Taussky Todd

Received December 22, 1970

This paper investigates positive definite unimodular quadratic forms in n variables with rational integer coefficients and a skew circulant as the coefficient matrix. It is shown for $n \leqslant 13$ that every such form is in the principal class, but that this no longer holds for $n = 14$. It is also shown that such forms can never be even. This behaviour is opposite to that for forms with a circulant as the coefficient matrix.

1. INTRODUCTION

It is the purpose of this paper to study positive definite quadratic forms with rational integer coefficients and a unimodular skew circulant as the matrix of coefficients. Note that a skew circulant is not a skew symmetric matrix and can in fact be symmetric and even positive definite symmetric.

Let A and B be $n \times n$ positive definite symmetric unimodular matrices with rational integers as entries. We say A and B are congruent if an integral unimodular C exists (i.e., $\det C = \pm 1$) such that $B = CAC^{\tau}$ (the superscript τ denotes transposition). Congruence is an equivalence relation on the set of $n \times n$ positive definite integral unimodular matrices and the number of equivalence classes is finite [5]. In fact, the number of such congruence classes [4] is one for $n \leqslant 7$, two for $n = 8, 9, 10, 11$, three for $n = 12, 13$, four for $n = 14$, five for $n = 15$, eight for $n = 16$.

There have been a number of investigations, some unpublished, of the possible presence of circulants in the $n \times n$ congruence classes. For $n = 8$, Taussky and Newman [7] showed that each of the two classes contained circulants. Other results on the presence of circulants in the $n \times n$ congruence classes are due to Kneser ($n = 9$ [unpublished]), Newman

* Both authors are supported in part by the U.S. Air Force Office of Scientific Research, under Grant 698-67.

($n = 12$ [unpublished]), Thompson ($n \leqslant 13$ [10]), Dade and Taussky (all prime $n \leqslant 100$ [unpublished]). See also [1]. Further recent results for a large number of prime n appear in an unpublished thesis by Davis [2].

A type of matrix possesing properties similar to those possessed by circulants is the skew circulant. It is the purpose of this paper to study the presence of definite skew circulants in the congruence classes described above. Our main result may be stated as follows: For $n \leqslant 13$, only the principal class contains skew circulants, but for $n = 14$ one of the non-principal classes also contains skew circulants. We shall also show that the congruence class of an even definite integral unimodular A (i.e., each diagonal element of A is even) cannot contain a skew circulant. That is, an integral skew circulant cannot be the coefficient matrix of an even definite unimodular quadratic form. It is known [7] that a corresponding assertion for circulants cannot be made.

2. Basic Properties of Skew Circulants

Let P_n be the companion matrix of the polynomial $\lambda^n + 1$. (We take the stripe of one's to be in the diagonal immediately above the main diagonal.). Then $P_n{}^n = -I_n$ where I_n is the n-square identity matrix. By definition, a skew circulant C is a polynomial in P_n, i.e., it has the form

$$C = \sum_{t=1}^{n} a_{t-1} P_n^{t-1}. \tag{1}$$

The top row of C is $(a_0, \ldots, a_{n-1})$ and each row below the top is obtained by shifting the elements of the preceding row to the right one place, and returning the negative of the last element to the initial position. Let ω be primitive root of unity of order $2n$ and set

$$U = n^{-1/2}(\omega^{(i-1)(2j-1)})_{1 \leqslant i,j \leqslant n}.$$

The matrix U is unitary and

$$U^* P_n U = \operatorname{diag}(\omega, \omega^3, \ldots, \omega^{2n-1}). \tag{2}$$

(Here U^* is the complex conjugate transpose of U.)
Thus

$$U^* C U = \operatorname{diag}(\lambda_1, \ldots, \lambda_n), \tag{3}$$

where

$$\lambda_j = \sum_{t=1}^{n} \omega^{(2j-1)(t-1)} a_{t-1}, \qquad 1 \leqslant j \leqslant n. \tag{4}$$

We may rewrite (4) as

$$(\lambda_1, \ldots, \lambda_n) = n^{1/2}(a_0, \ldots, a_{n-1})\, U. \tag{5}$$

It is not difficult to see that sums, products, transposes, and inverses (when they exist) of skew circulants are again skew circulants. A matrix M satisfies $MP_n = P_nM$ if and only if M is a skew circulant. A skew circulant is always a normal matrix.

3. The Existence of Nontrivial Integral Unimodular Skew Circulants

We say an integral unimodular skew circulant is trivial if it is a generalized permutation matrix, that is, if it is $\pm P_n^{\alpha}$ for some exponent α. Otherwise, we say a skew circulant is nontrivial. It is natural to ask whether nontrivial integral unimodular skew circulants actually exist.

THEOREM 1. *Nontrivial integral unimodular $n \times n$ skew circulants exist if and only if $n \geqslant 4$.*

Proof. Let C be an $n \times n$ integral unimodular skew circulant, with $n \leqslant 3$. Each eigenvalue of C must then be a unit in the algebraic integer ring $Z[\omega]$, where Z denotes the rational integers. If $n \leqslant 3$, the only units in $Z[\omega]$ are roots of unity, and hence $|\lambda_i| = 1$ for $1 \leqslant i \leqslant n \leqslant 3$. From this fact, (5), and the fact that U is unitary, we get

$$n = |\lambda_1|^2 + \cdots + |\lambda_n|^2 = n(a_0^2 + \cdots + a_{n-1}^2). \tag{6}$$

Therefore $a_0^2 + \cdots + a_{n-1}^2 = 1$, and this forces all but one of $a_0, \ldots, a_{n-1}$ to be zero, and the remaining $a_i = \pm 1$. Thus C is trivial.

Conversely, suppoe $n \geqslant 4$. Let $k = n - 1$ if n is even, and $k = n - 2$ if n is odd. Then $(k, 2n) = 1$ and hence a positive integer β exists such that $\beta k \equiv 1 \pmod{2n}$. Let

$$C = \sum_{t=0}^{k-1} P_n^{\,t} = (I - P_n^{\,k})(I - P_n)^{-1}. \tag{7}$$

Then

$$\begin{aligned} C^{-1} &= (I - P_n)(I - P_n^{\,k})^{-1} = (I - P_n^{\beta k})(I - P_n^{\,k})^{-1} \\ &= \sum_{t=0}^{\beta-1} P_n^{tk}. \end{aligned}$$

Thus both C and C^{-1} are integral matrices. Since $k \geqslant 3$, C is a unimodular nontrivial integral skew circulant.

COROLLARY. *For $n \leqslant 3$, the only $n \times n$ positive definite symmetric integral unimodular skew circulant is the identity. For $n \geqslant 4$, nontrivial positive definite symmetric integral unimodular skew circulants exist.*

Proof. For $n \leqslant 3$, the result follows from Theorem 1. Let $n \geqslant 4$, and let C be a nontrivial integral unimodular skew circulant. Then CC^{τ} is a positive definite integral unimodular skew circulant and cannot be the identity since the main diagonal entry of CC^{τ} equals the sum of the squares of the entries of any row of C.

4. Skew Circulants in the Principal Class

The following theorem is directly analogous to a corresponding theorem for circulants. The proof closely follows the proof of Theorem 4 in [8] and so will not be given.

THEOREM 2. *Let C be a positive definite symmetric integral unimodular skew circulant, and suppose $C = AA^{\tau}$ where A is an integral matrix. Then $A = C_1R$ where C_1 is an integral skew circulant and R is a generalized permutation matrix. Furthermore $C = C_1C_1^{\tau}$.*

5. Congruence Classes Not Containing Skew Circulants

THEOREM 3. *Let A be an m-square positive definite integral unimodular matrix such that the associated quadratic form*

$$x^{\tau}Ax, \qquad x = (x_1, \ldots, x_m)^{\tau},$$

does not represent one, that is, $x^{\tau}Ax > 1$ for each nonzero integral x. Let

$$B = A \dotplus \operatorname{diag}(1, 1, \ldots, 1) = A \dotplus I_t$$

be $n = m + t$-square, with $t > 0$. Then B is not congruent to any skew circulant.

Proof. It is easy to check that the number of integral column n-tuples x such that $x^{\tau}Bx = 1$ is exactly $2t$. If C, a skew circulant, were congruent to B then the number of integral vectors x such that $x^{\tau}Cx = 1$ would also

be $2t$. However, we will show that $x^\tau Cx = 1$ has more than $2t$ integral solutions and hence it follows that C cannot be congruent to B.

Let y be a fixed integral column n-tuple such that $y^\tau Cy = 1$. Then, since $P_n{}^\tau CP_n = C$, we find that

$$(P_n{}^i y)^\tau C(P_n{}^i y) = 1,$$

where $i = 0, 1, 2, \ldots, n-1$. Therefore, each of the following integral vectors represents one:

$$\pm y, \pm P_n y, \ldots, \pm P_n^{n-1} y. \tag{8}$$

We wish to show that these vectors are distinct. If not, let i be minimal such that

$$P_n{}^i y = \pm y, \qquad n > i > 0, \tag{9}$$

for some choice of the $\pm$ sign. Then, necessarily, the $\pm$ sign must be minus. For if

$$P_n{}^i y = y, \tag{10}$$

then from $-y = P_n{}^n y$ and (10), we get

$$-y = P_n{}^r y, \tag{11}$$

where r is remainder obtained on dividing n by i. Plainly $r \neq 0$ in (11), consequently (11) defeats the minimality of i. Hence we have

$$P_n{}^i y = -y. \tag{12}$$

We next show that $i \mid n$. Let $d = (i, n)$, so that $d = \alpha i + \beta n$ for certain integers α, β. Then $P_n{}^d y = P_n^{\alpha i + \beta n} y = (-1)^{\alpha+\beta} y = \pm y$. The minimality of i implies $d \geqslant i$, hence $d = i$ and therefore $i \mid n$. Let $n = ki$. We claim that k is odd. For there exists an odd a, $1 \leqslant a < 2n$, such that $(\omega^a)^i = -1$. This is because (12) shows that -1 is an eigenvalue of $P_n{}^i$, hence -1 is the i-th power of some eigenvalue ω^a (a odd) of P_n. From $(\omega^a)^i = -1$ we get $\omega^{2ai} = 1$, hence $(2n) \mid (2ai)$, hence $k \mid a$. Therefore k is odd.

The dimension of the eigenspace of $P_n{}^i$ belonging to eigenvalue -1 is just the multiplicity of -1 as an eigenvalue of $P_n{}^i$. The eigenvalue -1 of $P_n{}^i$ appears exactly as the i-th power of the following eigenvalues of P_n:

$$\omega^k, \omega^{3k}, \omega^{5k}, \ldots, \omega^{(2i-1)k}.$$

Thus the multiplicity of -1 as an eigenvalue of $P_n{}^i$ is i.

Let $u = (u_1, \ldots, u_i)$ be a row i-tuple, and let $v = (u, -u, u, -u, \ldots, -u, u)$

be a row n-tuple. There are k appearances of u and $-u$ in v. Then $P_n{}^i v^\tau = -v^\tau$. Since the vectors v of this type span an i-dimensional space, we see that every eigenvector of $P_n{}^i$ beloning to eigenvalue -1 has the form of v. Thus $y = v^\tau$ for some choice of integers $u_1, \ldots, u_i$.

Now observe that $P_n{}^j y = (w, -w, w, \ldots, -w, w)^\tau$ where w is an integral vector. Hence $y^\tau P_n{}^j y = (u, -u, \ldots, u)(w, -w, \ldots, w)^\tau = kuw^\tau$. Because C is an integral linear combination of the $P_n{}^j$, $j = 0, 1, 2, \ldots, n-1$, we deduce that

$$y^\tau C y = kz,$$

where z is some integer. Since $y^\tau C y = 1$, we find that $k \mid 1$; hence $k = 1$. But this forces $i = n$, a contradiction. Therefore the $2n$ vectors (8) are distinct. Thus the number of vectors representing one is at least $2n > 2t$. Thus we obtain the contradiction announced near the beginning of the proof. The proof is complete.

Before giving the next theorem we prepare the way with a lemma.

LEMMA. *Let ξ be a primitive 2^k root of unity and let*

$$u = a_0 + a_1\xi + \cdots + a_{m-1}\xi^{m-1}, \qquad m = 2^{k-1},$$

be a real unit in $Z[\xi]$ where $a_0, \ldots, a_{m-1}$ are rational integers. Then a_0 is odd.

Proof. The proof is an induction on k. When $k = 1$ or 2 we have $u = a_0$, hence $a_0 = \pm 1$. Let $k \geqslant 3$.

Suppose the result established for real units in the ring $Z[\xi^2]$ based upon the primitive root of unity ξ^2 of order 2^{k-1}, and let u be as stated above. Since u is real we have $u = \bar{u}$. Using $\xi^m = -1$ it follows that $a_1 = -a_{m-1}$, $a_2 = -a_{m-2}, \ldots$, and hence

$$u = a_0 + \sum_{t=1}^{m/2-1} a_t(\xi^t - \xi^{m-t})$$

$$= a_0 + \sum_{t=1}^{m/4-1} a_{2t}(\xi^{2t} - \xi^{m-2t})$$

$$+ \sum_{t=1}^{m/4} a_{2t-1}(\xi^{2t-1} - \xi^{m-2t+1}). \tag{13}$$

The map σ defined by $\sigma(\xi) = \xi^{m-1}$ defines an automorphism of $Z[\xi]$, for which

$$u^\sigma = a_0 + \sum_{t-1}^{m/4-1} a_{2t}(\xi^{2t} - \xi^{m-2t}) - \sum_{t=1}^{m/4} a_{2t-1}(\xi^{2t-1} - \xi^{m-2t+1}).$$

Thus

$$uu^\sigma = \Big[a_0 + \sum_{t=1}^{m/4-1} a_{2t}(\xi^{2t} - \xi^{m-2t})\Big]^2 - \Big[\sum_{t=1}^{m/4} a_{2t-1}(\xi^{2t-1} - \xi^{m-2t+1})\Big]^2. \tag{14}$$

Let $0 < t \leqslant s < m/4$. *Then*

$$(\xi^{2t} - \xi^{m-2t})(\xi^{2s} - \xi^{m-2s}) = (\xi^{2(s-t)} - \xi^{m-2(s-t)}) + \epsilon(\xi^{2\alpha} - \xi^{m-2\alpha}), \qquad 0 < \alpha < m/4,$$

where $\epsilon = 1$, $\alpha = s + t$ if $s + t < m/4$; $\epsilon = 0$ if $s + t = m/4$; and $\epsilon = -1$, $\alpha = m/2 - s - t$ if $m/4 < s + t < m/2$. Furthermore, if $0 < t \leqslant s \leqslant m/4$, then

$$(\xi^{2t-1} - \xi^{m-2t+1})(\xi^{2s-1} - \xi^{m-2s+1}) = (\xi^{2(s-t)} - \xi^{m-2(s-t)}) + \epsilon'(\xi^{2\alpha} - \xi^{m-2\alpha}), \qquad 0 < \alpha < m/4,$$

where $\epsilon' = 1$, $\alpha = t + s - 1$ if $t + s \leqslant m/4$; $\epsilon' = 0$ if $t + s = m/4 + 1$; $\epsilon' = -1$, $\alpha = m/2 - t - s + 1$ if $m/4 < t + s - 1 < m/2$. Combining these facts we obtain from (14) that

$$uu^\sigma = \sum_{t=0}^{m/2-1} A_t(\xi^2)^t, \qquad A_t \in Z,$$

where

$$A_0 = a_0{}^2 + \sum_{t=1}^{m/2-1} \pm 2a_t{}^2.$$

Since $\bar{u}^\sigma = \overline{u^\sigma}$ (because the Galois group of a cyclotomic field is abelian), we deduce that uu^σ is a real unit in $Z[\xi^2]$. Our inductive hypothesis now implies that A_0 is odd and hence a_0 is odd.

We use the lemma to prove the following theorem.

THEOREM 4. *Let C be an n-square symmetric unimodular integral skew circulant, with main diagonal element a_0. Then a_0 is odd.*

Proof. Let $(a_0, a_1, \ldots, a_{n-1})$ be the top row of C. Let $n = 2^{k-1}r$, where r is odd, and let ω be the primitive $2n$-th root of unity. Set $\xi = \omega^r$. Then ξ is a primitive root of unity of order 2^k.

By (4), the eigenvalue $\lambda_{(r+1)/2}$ of C is given by

$$\lambda_{(r+1)/2} = \sum_{t=1}^{n} (\omega^r)^{t-1} a_{t-1}$$

$$= \sum_{t=1}^{m} A_{t-1}\xi^{t-1}, \qquad m = 2^{k-1}, \tag{15}$$

where

$$A_0 = a_0 + \sum_{t=1}^{r-1} (-1)^t a_{tm} = a_0 + \sum_{t=1}^{(r-1)/2} (-1)^t (a_{tm} - a_{(r-t)m}).$$

Since C is unimodular and symmetric, $\lambda_{(r+1)/2}$ is a real unit in $Z[\xi]$. By the lemma we see that A_0 is odd. Since C is symmetric we have $a_i = -a_{n-i}$, $1 \leqslant i < n$, and hence $a_{tm} = -a_{(r-t)m}$, for $1 \leqslant t \leqslant (r-1)/2$. Therefore

$$A_0 = a_0 + 2 \sum_{t=1}^{(r-1)/2} (-1)^t a_{tm}.$$

Thus a_0 must be odd.

An $n \times n$ positive definite symmetric integral unimodular matrix A is said to be even if each main diagonal element of A is even. Thus A is even if and only if the associated quadratic form x^tAx represents only even integers for integral vectors x. It is known [5] that even matrices exist if and only if $n \equiv 0 \pmod 8$. It is known [7] that definite integral unimodular circulants may be even. It is natural to ask the same question for definite integral unimodular skew circulants. The answer, somewhat surprisingly, is opposite to that for circulants.

THEOREM 5. *There exist no even positive definite integral unimodular skew circulants.*

Proof. The main diagonal element of every symmetric unimodular skew circulant must be odd.

For completeness we state the following counterpart to Theorem 5.

THEOREM 6. *For each $n \equiv 0 \pmod 8$ there exists an even integral positive definite unimodular circulant.*

Proof. Let M be the 8×8 circulant described in [7]. Then M is positive definite, integral, unimodular, and even. Let $n = 8k$. Then $I_k \otimes M$ (the $\otimes$ denotes Kronecker product) is an $n \times n$ positive definite symmetric, integral, unimodular, even circulant.

6. Congruence Classes Containing Skew Circulants

THEOREM 7. *Let $n = 2p$ where p is a prime such that $p \equiv 7 \pmod 8$. Then a positive definite integral unimodular skew circulant C exists which is not in the congruence class of I_n.*

Proof. Let ω be a primitive root of unity of order $4p$. The irreducible polynomial for ω is

$$\varphi_{4p}(x) = \sum_{t=0}^{p-1} (-1)^t x^{2t}. \tag{16}$$

Thus, letting $i = (-1)^{1/2}$, we have

$$\varphi_{4p}(i) = p. \tag{17}$$

The multiplicative order m of 2 (mod p) is well known to be odd when $p \equiv 7 \pmod 8$. Let $m = 2s + 1$ and define polynomial $d(x)$ by

$$d(x) = (1 - x^2)^s(1 - x).$$

Let $D = d(P_n)$ and set $B = DD^T$. Then

$$B = b(P_n),$$

where $b(x)$ is an integral polynomial of degree not exceeding $n - 1$. The eigenvalues of B are then $d(\omega^{2j-1})\,\overline{d(\omega^{2j-1})}$, for $j = 1,\ldots, n$. In particular, $b(\omega) = |d(\omega)|^2$ and $b(i) = |d(i)|^2$. Now

$$d(\omega) = (1 - \omega^2)^s(1 - \omega)$$

is a unit in the ring $Z[\omega]$. This follows from the facts that both $(1 - \omega)$, $(1 - \omega^2)$ are units in this ring; see [see [3, 11]. In fact,

$$(1 - \omega)(\omega^2 + \omega^3 + \omega^6 + \omega^7 + \omega^{10} + \omega^{11} + \cdots + \omega^{2p-4} + \omega^{2p-3}) = 1,$$
$$(1 + \omega)(\omega^2 - \omega^3 + \omega^6 - \omega^7 + \omega^{10} - \omega^{11} + \cdots + \omega^{2p-4} - \omega^{2p-3}) = 1.$$

Thus $b(\omega) = d(\omega)\,\overline{d(\omega)}$ is also a unit. Furthermore, $b(i) = d(i)\,\overline{d(i)}$, therefore

$$b(i) = 2^{2s+1} \equiv 1 \pmod p.$$

Thus

$$b(i) = 1 + tp$$

for some integer t. Define polynomial $c(x)$ by

$$c(x) = b(x) - t\varphi_{4p}(x),$$

and let

$$C = c(P_n).$$

Plainly C is an integral skew circulant. We shall investigate the eigenvalues of C. To within an isomorphism, the eigenvalues of C are completely determined by the eigenvalues λ_1, $\lambda_{(p+1)/2}$. Thus is so because of (4) and the existence of isomorphisms from a primitive root of unity of given degree onto all other primitive roots of unity of the same degree. For C we find that λ_1 is $c(\omega) = b(\omega) = d(\omega)\,\overline{d(\omega)} > 0$ and hence for each automorphism σ of the cyclotomic field generated by ω, we have

$$c(\omega^\sigma) = c(\omega)^\sigma = d(\omega^\sigma)\,\overline{d(\omega^\sigma)} > 0.$$

(The abelian nature of the Galois group of a cyclotomic field is used here.) Thus $c(\omega^\sigma)$ is a positive real unit for each σ. The eigenvalue $\lambda_{(p+1)/2}$ for C is $c(i) = 1$, and hence it and its conjugates are also positive reals. This means each eigenvalue of the normal matrix C is a positive real unit, and therefore C is a positive definite symmetric integral unimodular skew circulant.

We complete the proof by showing that C is not congruent to the I_n. For if C were congruent to I_n, then by Theorem 2 $C = D_0 D_0^\tau$ when D_0 is an integral unimodular skew circulant. Let $D_0 = d_0(P_n)$ where $d_0(x)$ is an integral polynomial. Then

$$c(\omega) = d_0(\omega)\,\overline{d_0(\omega)} = d(\omega)\,\overline{d(\omega)}.$$

Thus $d_0(\omega)$, $d(\omega)$ are units, so let $d(\omega) = d_0(\omega)\,u$ where u is a unit in $Z[\omega]$. Then $u\bar{u} = 1$. Since the Galois group of the cyclotomic field generated by ω is abelian, we get $u^\sigma(\overline{u^\sigma}) = 1$ for every σ in this Galois group. Thus each conjugate of u has modulus one, and this implies [9] that u is a root of unity. Hence [11] $u = \omega^\beta$ for some nonnegative integral exponent β. Therefore,

$$d(\omega) = \omega^\beta\, d_0(\omega).$$

Thus $d(x) - x^\beta\, d_0(x)$ is divisible by $\varphi_{4p}(x)$, say

$$d(x) = x^\beta\, d_0(x) + f(x)\,\varphi_{4p}(x),$$

where $f(x)$ has integral coefficients. Therefore (see (17))

$$d(i) \equiv i^{\beta} d_0(i) \pmod{p}.$$

Now $d_0(i)$ must be a unit in $Z[i]$, hence $d_0(i) = \pm 1$, or $\pm i$. But also $d(i) = 2^s(1 - i)$. Since

$$2^s(1 - i) \not\equiv \pm 1 \quad \text{or} \quad \pm i \pmod{p},$$

we cannot have $d(i) \equiv i^{\beta} d_0(i) \pmod{p}$. Therefore C cannot be in the congruence class of I_n. This finishes the proof of Theorem 7.

7. 12×12 Skew Circulants

The purpose of this section is to establish the following theorem.

THEOREM 8. *Let C be an integral unimodular positive definite 12×12 skew circulant. Then an integral unimodular 12×12 skew circulant A exists such that*

$$C = AA^{\tau}.$$

If X, Y, Z are 12×12 integral skew circulants then an equation like $Z = XY$ holds if and only if $\lambda_i(Z) = \lambda_i(X)\lambda_i(Y)$, for $1 \leqslant i \leqslant 12$. Because of isomorphisms mapping primitive roots of unity of a given degree to all other primitive roots of unity of the same degree, the equations $\lambda_i(Z) = \lambda_i(X)\lambda_i(Y)$ will be valid for all i if they are valid for $i = 1, 2$. Here, for example, $\lambda_i(C)$ denotes the eigenvalues of C as given by (4), where now in (4) ω is a primitive root of unity of order 24.

The eigenvalues of a 12×12 integral unimodular C will be units in the ring $Z[\omega]$. Before giving the proof of Theorem 8 we must locate the basis units in the maximal real subring $Z[\omega + \omega^{-1}]$ of $Z[\omega]$. It is not hard to verify that

$$Q(\omega + \omega^{-1}) = Q(2^{1/2}, 3^{1/2}).$$

(Q denotes the rational numbers.) Note that

$$\omega = \frac{1}{2}\left[\frac{6^{1/2} + 2^{1/2}}{2} + i\,\frac{6^{1/2} - 2^{1/2}}{2}\right].$$

The subfields of $Q(2^{1/2}, 3^{1/2})$ are $Q(2^{1/2})$, $Q(3^{1/2})$, $Q(6^{1/2})$, and the fundamental units in the algebraic integer subrings of these fields are, respectively, $1 + 2^{1/2}$, $2 + 3^{1/2}$, $5 + 2 \cdot 6^{1/2}$.

The nonidentity automorphisms of $Q(2^{1/2}, 3^{1/2})$ are σ, τ, $\rho = \sigma\tau$, where their actions on $2^{1/2}$, $3^{1/2}$ are described by

$$\begin{aligned} \sigma &: 2^{1/2} \to 2^{1/2}, \qquad 3^{1/2} \to -3^{1/2}, \\ \tau &: 2^{1/2} \to -2^{1/2}, \qquad 3^{1/2} \to 3^{1/2}, \\ \rho &: 2^{1/2} \to -2^{1/2}, \qquad 3^{1/2} \to -3^{1/2}. \end{aligned}$$

For national simplicity, let

$$u_1 = 1 + 2^{1/2}, \qquad u_2 = \tfrac{1}{2}(2^{1/2} + 6^{1/2}), \qquad u_3 = 2^{1/2} + 3^{1/2}. \tag{18}$$

Then $u_2^2 = 2 + 3^{1/2}$, $u_3^2 = 5 + 2 \cdot 6^{1/2}$. Thus u_1, u_2^2, u_3^2 are, respectively, the fundamental units in the rings $Z[2^{1/2}]$, $Z[3^{1/2}]$, $Z[6^{1/2}]$.

Let u be a unit in the algebraic integer ring of $Q(2^{1/2}, 3^{1/2})$. Then uu^σ is fixed by σ, hence uu^σ is in $Q(2^{1/2})$, and thus

$$uu^\sigma = \pm u_1^\alpha, \qquad \alpha \in Z. \tag{19.1}$$

Similarly

$$uu^\tau = \pm u_2^{2\beta}, \qquad \beta \in Z, \tag{19.2}$$

$$uu^\rho = \pm u_3^{2\gamma}, \qquad \gamma \in Z. \tag{19.3}$$

Furthermore,

$$uu^\sigma u^\tau u^\rho = \pm 1,$$

since this product is the norm of u. Multiplying together (19.1), (19.2), (19.3) and using (20), we get

$$u^2 = \pm u_1^\alpha u_2^{2\beta} u_3^{2\gamma}.$$

Since u^2, u_1, u_2, u_3 are all positive reals, we have

$$u^2 = u_1^\alpha u_2^{2\beta} u_3^{2\gamma}. \tag{21}$$

We claim that α is even, for we have

$$(u^\sigma)^2 = (u_1^\sigma)^\alpha (u_2^\sigma)^{2\beta} (u_3^\sigma)^{2\gamma}. \tag{22}$$

Here $(u^\sigma)^2$, $(u_2^\sigma)^2$, $(u_3^\sigma)^2$ are positive reals, and u_1^σ is a negative real. Consequently, (22) is contradictory if α is odd; hence α is even. Let $\alpha = 2\alpha'$. Then

$$u = \pm u_1^{\alpha'} u_2^\beta u_3^\gamma.$$

Thus the unit group in the algebraic integer ring of $Q(2^{1/2}, 3^{1/2})$ is generated by -1, u_1, u_2, u_3. Consequently, these are the fundamental units.

LEMMA 1. *The basis units in the algebraic integer ring of* $Q(2^{1/2}, 3^{1/2})$ *are* $-1, u_1, u_2, u_3$.

LEMMA 2. *Let* $\alpha_0, \ldots, \alpha_7, \beta_0, \ldots, \beta_3 \in Z$. *If*

$$\begin{aligned} &\beta_0 \equiv \alpha_0 - \alpha_4, \quad \beta_1 \equiv \alpha_1 - \alpha_5, \\ &\beta_2 \equiv \alpha_2 - \alpha_6, \quad \beta_3 \equiv \alpha_3 - \alpha_7 \pmod 3, \end{aligned} \tag{23}$$

then $a_0, a_1, \ldots, a_{11} \in Z$ *exist such that*

$$\begin{aligned} &\alpha_0 = a_0 - a_8, \quad \alpha_4 = a_4 + a_8, \quad \beta_0 = a_0 - a_4 + a_8, \\ &\alpha_1 = a_1 - a_9, \quad \alpha_5 = a_5 + a_9, \quad \beta_1 = a_1 - a_5 + a_9, \\ &\alpha_2 = a_2 - a_{10}, \quad \alpha_6 = a_6 + a_{10}, \quad \beta_2 = a_2 - a_6 + a_{10}, \\ &\alpha_3 = a_3 - a_{11}, \quad \alpha_7 = a_7 + a_{11}, \quad \beta_3 = a_3 - a_7 + a_{11}. \end{aligned} \tag{24}$$

Conversely, if $a_0, \ldots, a_{11}$ *are given, and* $\alpha_0, \ldots, \alpha_7, \beta_0, \ldots, \beta_3$ *are defined by* (24) *then* (23) *holds.*

Proof. By (23) there exists a_{8+i} such that $\beta_i - \alpha_i + \alpha_{4-i} = 3a_{8+i}$, $i = 0, 1, 2, 3$. Let

$$\begin{aligned} &a_0 = \alpha_0 + a_8, \quad a_1 = \alpha_1 + a_9, \quad a_2 = \alpha_2 + a_{10}, \quad a_3 = \alpha_3 + a_{11}, \\ &a_4 = \alpha_4 - a_8, \quad a_5 = \alpha_5 - a_9, \quad a_6 = \alpha_6 - a_{10}, \quad a_7 = \alpha_7 - a_{11}. \end{aligned}$$

Then $a_0, \ldots, a_{11}$ satisfy (24). The converse is direct.

LEMMA 3. *Let integers* $\alpha_0, \ldots, \alpha_7, \beta_0, \ldots, \beta_3$ *be given. Then an integral* 12×12 *skew circulant* A *exists such that*

$$\lambda_1(A) = \alpha_0 + \alpha_1\omega + \alpha_2\omega^2 + \alpha_3\omega^3 + \cdots + \alpha_7\omega^7, \tag{25.1}$$

$$\lambda_2(A) = \beta_0 + \beta_1\zeta + \beta_2\zeta^2 + \beta_3\zeta^3 \tag{25.2}$$

(*where* $\zeta = \omega^3$) *if and only if* (23) *is satisfied.*

Proof. Let the first row of A be $(a_0, \ldots, a_{11})$. Using $\omega^8 = \omega^4 - 1$, $\zeta^4 = -1$, we find that

$$\begin{aligned} \lambda_1(A) = {} & (a_0 - a_8) + (a_1 - a_9)\,\omega + (a_2 - a_{10})\,\omega^2 + (a_3 - a_{11})\,\omega^3 \\ & + (a_4 + a_8)\,\omega^4 + (a_5 + a_9)\,\omega^5 + (a_6 + a_{10})\,\omega^6 + (a_7 + a_{11})\,\omega^7, \end{aligned} \tag{26}$$

$$\begin{aligned} \lambda_2(A) = {} & (a_0 - a_4 + a_8) + (a_1 - a_5 + a_9)\,\zeta \\ & + (a_2 - a_6 + a_{10})\,\zeta^2 + (a_3 - a_7 + a_{11})\,\zeta^3. \end{aligned} \tag{26.2}$$

Because $1, \omega, \ldots, \omega^7$ are independent over Q, as are $1, \zeta, \zeta^2, \zeta^3$, (25) and (26) agree if and only if (24) holds, and for this (23) is the necessary and sufficient condition.

LEMMA 4. *There exist* 12×12 *integral unimodular skew circulants* A *for which* $\lambda_1(A)$ *and* $\lambda_2(A)$ *are as stated below*:

(i) $\lambda_1(A) = u_1, \quad \lambda_2(A) = u_1^3;$
(ii) $\lambda_1(A) = u_2, \quad \lambda_2(A) = -u_1^2;$
(iii) $\lambda_1(A) = u_3, \quad \lambda_2(A) = u_1^2;$
(iv) $\lambda_1(A) = 1, \quad \lambda_2(A) = -u_1^4.$

Proof. In each case (i)-(iv), express the proposed $\lambda_1(A)$, $\lambda_2(A)$ in the form appearing on the right hand side of (25). Then the conditions (23) are satisfied and hence an integral skew circulant A exists, using Lemma 3 with $\lambda_1(A)$, $\lambda_2(A)$ as described in each case. In each case the eigenvalues $\lambda_1(A)$, $\lambda_2(A)$ are units, and hence all eigenvalues of A are units since the remaining eigenvalues are obtained as images of $\lambda_1(A)$, $\lambda_2(A)$ under isomorphisms. Therefore, each eigenvalue of A is a unit, hence so is $\det A$. Therefore $\det A = \pm 1$, as required.

LEMMA 5. *Let* C *be a positive definite integral unimodular skew circulant. Then an integral skew circulant* C_1 *exists such that, if* $D = C_1 C C_1^{\tau}$, *then*

$$\lambda_1(D) = u_1^{\alpha} u_2^{\beta} u_3^{\gamma}, \quad \lambda_2(D) = u_1^{\delta}, \tag{27}$$

where

$$\alpha = 0 \text{ or } 1, \quad \beta = 0 \text{ or } 1, \quad \gamma = 0 \text{ or } 1, \quad 0 \leqslant \delta \leqslant 7. \tag{28}$$

Proof. The eigenvalues $\lambda_1(C)$, $\lambda_2(C)$ must be units. These eigenvalues lie in $Q(\omega)$, and $Q(\zeta)$, and are positive reals. Therefore $\lambda_1(C)$ and $\lambda_2(C)$ have the form

$$\lambda_1(C) = u_1^{\alpha} u_2^{\beta} u_3^{\gamma}, \qquad \lambda_2(C) = u_1^{\delta},$$

where $\alpha, \beta, \gamma, \delta \in Z$. By Lemma 4 we can find an integral unimodular skew circulant A such that in $\lambda_1(ACA^{\tau})$ we adjust the exponents α, β, γ, δ as follows: α, β, γ are first adjusted up or down by arbitrary multiples of 2, then leaving α, β, γ fixed, δ is adjusted up or down by arbitrary multiples of 8. Thus a congruence of C by an integral unimodular skew circulant may be found to bring the exponents α, β, γ, δ to the range described by (28).

LEMMA 6. *Let D be a positive definite integral unimodular skew circulant, for which $\lambda_1(D)$, $\lambda_2(D)$ are given by* (27) *and* (28). *Then $D = I_{12}$.*

Proof. Not only must the eigenvalues $\lambda_1(D)$, $\lambda_2(D)$ of D be positive units, but so must $\lambda_1(D)^\sigma$, $\lambda_1(D)^\tau$, $\lambda_1(D)^\rho$, $\lambda_2(D)^\sigma$, since these are also eigenvalues of D. However, for any choice of the triple (α, β, γ) of exponents (except (0, 0, 0) and (1, 1, 1)), we find that one of

$$\lambda_1(D)^\sigma, \qquad \lambda_1(D)^\tau, \quad \lambda_1(D)^\rho$$

is negative. Thus either $\lambda_1(D) = 1$ or $\lambda_1(D) = u_1u_2u_3$. If δ is odd then the eigenvalue $(u_1^\sigma)^\delta$ of D is negative. Therefore δ is even.

Case (i) $\lambda_1(D) = 1$, $\lambda_2(D) = u_1^\delta$, $\delta = 0, 2, 4,$ or 6. For $\delta = 0, 2, 4,$ or 6, if we express $\lambda_1(D)$ and $\lambda_2(D)$ in the form appearing on the right hand side of (25) (thus $\alpha_0 = 1$, $\alpha_1 = \cdots = \alpha_7 = 0$), then we see that the conditions (23) are satisfied only when $\delta = 0$.

Case (ii) $\lambda_1(D) = u_1u_2u_3$, $\lambda_2(D) = u_1^\delta$, $\delta = 0, 2, 4, 6$. Express $\lambda_1(D)$, $\lambda_2(D)$ in the forms appearing on the right hand side of (25). Then, by direct computation in each case, we see that for no choice of $\delta = 0, 2, 4, 6$ is (23) satisfied.

Hence all cases other than $\lambda_1(D) = \lambda_2(D) = 1$ are excluded. Therefore $D = I_{12}$.

Theorem 8 is now fully proved.

8. $n \times n$ SKEW CIRCULANT CONGRUENCE CLASSES FOR $n \leqslant 14$

Our results may now be combined to establish the following result.

THEOREM 9. *Let C be an $n \times n$ positive definite integral unimodular skew circulant. If $n \leqslant 13$ then C is in the congruence class of I_n. There exists a 14×14 positive definite integral unimodular skew circulant which is not in the congruence class of I_{14}.*

Proof. For $1 \leqslant n \leqslant 13$, representatives of the different congruence classes of positive definite integral unimodular matrices are

$$I_n, \qquad 1 \leqslant n \leqslant 13, \tag{28.1}$$

$$\Phi_8 \dotplus I_{n-8}, \qquad 8 \leqslant n \leqslant 13, \tag{28.2}$$

$$\Phi_{12} \dotplus I_{n-12}, \qquad 12 \leqslant n \leqslant 13. \tag{28.3}$$

Here, for $t \equiv 0 \pmod 4$, the matrix Φ_t is described on p. 331 of [5]. The

matrix Φ_t does not represent one [5], and Φ_8 is also even. By Theorem 5, the congruence class represented by Φ_8 does not contain any skew circulant. By Theorem 3, the congruence classes represented by $\Phi_8 \dot{+} I_{n-8}$, for $8 < n \leqslant 13$ cannot contain a skew circulant. For the same reason the class represented by $\Phi_{12} \dot{+} I_1$ does not contain a skew circulant. By Theorem 8 no 12×12 class (other than the class of I_{12}) can contain a skew circulant. This completes the proof of the first assertion. To prove the second assertion apply Theorem 7 with $p = 7$.

REFERENCES

1. R. AUSTING, Groups of unimodular circulants, *J. Res. Nat. Bur. Stand. B* **65** (1965), 313–318.
2. D. L. DAVIS, "On the Distribution of the Signs of the Conjugates of the Cyclotomic Units in the Maximal Real Subfield of the qth Cyclotomic Field, q a Prime," thesis, California Institute of Technology, 1969.
3. D. HILBERT, "Gesammelte Abhandlungen," Chelsea, Vol. 1, p. 203, New York, 1965.
4. M. KNESER, Klassenzahlen definiter Quadratischen Formen, *Arch. Math.* **8** (1957), 241–250.
5. O. T. O'MEARA, "Introduction to Quadratic Forms," Academic Press, New York, 1963.
6. M. NEWMAN, "Circulant Quadratic Forms," Report of the Institute in the Theory of Numbers, pp. 189–193, Boulder, CO, 1959.
7. M. NEWMAN AND O. TAUSSKY, Classes of definite unimodular circulants, *Canad. Math. J.* **9** (1956), 71–73.
8. M. NEWMAN AND O. TAUSSKY, A generalization of the normal basis in abelian number fields, *Comm. Pure Appl. Math.* **9** (1956), 85–91.
9. M. POLLARD, "The Theory of Algebraic Numbers," Carus Monograph No. 9, The Mathematical Association of America, 1950.
10. R. C. THOMPSON, Classes of definite group matrices, *Pacific J. Math.* **17** (1966), 175–190.
11. E. WEISS, "Algebraic Number Theory," McGraw-Hill, New York, 1963.