SKEW CIRCULANTS AND THE THEORY OF NUMBERS

I. J. GOOD
Virginia Polytechnic Institute and State University, Blacksburg, VA 24061

(Submitted March 1984)

1. SKEW CIRCULICES AND SKEW DISCRETE FOURIER TRANSFORMS

The matrices

$$\begin{bmatrix} x & y \\ -y & x \end{bmatrix}$$

provide a familiar representation of complex numbers $x + iy$. Let us consider the more general matrix

$$X = \begin{bmatrix} x_0 & x_1 & x_2 & \cdots & x_{t-1} \\ -x_{t-1} & x_0 & x_1 & \cdots & x_{t-2} \\ -x_{t-2} & -x_{t-1} & x_0 & \cdots & x_{t-3} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ -x_2 & -x_3 & -x_4 & \cdots & x_1 \\ -x_1 & -x_2 & -x_3 & \cdots & x_0 \end{bmatrix}, \tag{1}$$

where t is a positive integer, and $x_0, x_1, \ldots, x_{t-1}$ are real numbers. The determinant of X is called a *skew circulant* by Muir [7, p. 442] and by Davis [1, pp. 83-85], and we call X a *skew circulix*. We can write X in the form

$$X = x_0I + x_1J + \cdots + x_{t-1}J^{t-1}, \tag{2}$$

where I is the $t \times t$ unit matrix and

$$J = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 \\ -1 & 0 & 0 & 0 & \cdots & 0 & 0 \end{bmatrix}. \tag{3}$$

Since $J^t = -I$, it follows that all polynomials in J can be expressed as polynomials of degree at most $t - 1$, and every such polynomial is a skew circulix. Hence, all skew circulices commute with each other.

On a point of terminology, a skew circulix is not in general a skew-symmetric matrix although it can be. For example, J^2 is both a skew circulix and a skew-symmetric matrix when $t = 4$.

The eigenvalues of X are

$$x_s^\dagger = \sum_{r=0}^{t-1} x_r j^{r(2s+1)} \qquad (s = 0, 1, \ldots, t-1), \tag{4}$$

where $j = e^{\pi i/t}$. By analogy with the discrete Fourier transform, we may call the sequence $(x_0^\dagger, x_1^\dagger, \ldots, x_{t-1}^\dagger)$ the skew discrete Fourier transform (skew DFT) of $(x_0, x_1, \ldots, x_{t-1})$. The eigenvectors of all skew circulices are the columns of the matrix

$$\{j^{r(2s+1)}\} \qquad (r, s = 0, 1, \ldots, t-1).$$

We now list a few further properties of skew circulices to emphasize their mathematical respectability. See also Section 4.

Just as the ordinary discrete Fourier transform is associated with sequences of period t, the skew DFT is associated with sequences of antiperiod t; that is, doubly infinite sequences such that $x_{r+t} = -x_r$ for all integers r. This is so in the sense that, if (x_r) has antiperiod t, then the sum (4) is unchanged if r runs through any complete set of residues modulo t, not necessarily from 0 to $t - 1$. Antiperiodicity is a natural concept because, if a sequence has period $2t$, it can be readily expressed as the sum of two sequences, one with period t and one with antiperiod t.

The skew DFT has the inversion formula

$$x_r = \frac{1}{t}\sum_{s=0}^{t-1} x_s^\dagger j^{-r(2s+1)}, \tag{5}$$

an application of which is mentioned in Section 4. The skew DFT also has the convolution property that, if

$$z_q = \sum_{r=0}^{t-1} x_r y_{q-r} \qquad (q = 0, 1, \ldots, t-1),$$

where either (x_r) or (y_r) has antiperiod t, then

$$z_s^\dagger = x_s^\dagger y_s^\dagger \qquad (s = 0, 1, \ldots, t-1). \tag{6}$$

Under the same circumstances, and if (x_r) is real, the skew DFT of $\sum_r x_r y_{q+r}$ is $\bar{x}_s^\dagger y_s^\dagger$, where the bar denotes complex conjugacy. In particular, the skew DFT of $\sum_q x_q x_{q+r}$ is $|x_s^\dagger|^2$ so that, by the inversion formula, we have a "Parseval" formula,

$$\sum x_q^2 = \frac{1}{t}\sum |x_s^\dagger|^2. \tag{7}$$

Exercise: The skew circulant with top row $(1, x, x^2, \ldots, x^{t-1})$ is equal to $(x^t + 1)^{t-1}$.

2. CYCLOTOMOUS INTEGERS

A *cyclotomic integer* is defined (for example, by Edwards [2, pp. 81-88]) as a number of the form

$$\sum_{r=0}^{m-1} c_r \omega^r \qquad (\omega = e^{2\pi i/m}), \tag{8}$$

where $c_0, c_1, \ldots, c_{m-1}$ are ordinary integers, positive, negative, or zero, and where m is prime. However, if we generalize the definition by allowing m to be even, and write $m = 2t$, then (8) becomes

$$\sum_{r=0}^{t-1}(c_r - c_{r+t})j^r \qquad (j = e^{\pi i/t}).$$

Accordingly, for any positive integer t,

$$\sum_{r=0}^{t-1} a_r j^r = \sum_{r=0}^{t-1} a_r e^{\pi i r/t}, \tag{9}$$

where each a_r is an integer, will be called a *cyclotomous integer* (with respect to t). It is cyclotomic with respect to $2t$, under the generalized use of the expression "cyclotomic."

When $t = 1$, the cyclotomous integers are the ordinary integers, and when $t = 2$ they are the Gaussian integers (for example, LeVeque [6, pp. 129-131]).

Definition: We say that t is *ausgezeichnet* if the corresponding cyclotomous integers are "unique," that is, if the equation

$$\sum_{r=0}^{t-1} a_r j^r = \sum_{r=0}^{t-1} b_r j^r$$

implies that $a_r = b_r$ $(r = 0, 1, \ldots, t - 1)$; or, in other words, if

$$\sum_{r=0}^{t-1} a_r j^r = 0 \tag{10}$$

only if $a_r = 0$ $(r = 0, 1, \ldots, t - 1)$.

Theorem 1: The ausgezeichnet integers are the powers of 2, namely 1, 2, 4, 8, ... The others are unausgezeichnet.

Proof: If t is not a power of 2, then it has an odd factor $k > 1$. Write $t = ck$, where $1 \leqslant c < t$. Then

$$0 = 1 + j^t = (1 + j^c)(1 - j^c + j^{2c} - \cdots + j^{(k-1)c}).$$

Therefore, $1 - j^c + j^{2c} - \cdots + j^{(k-1)c}$ is a cyclotomous integer that vanishes, so t is unausgezeichnet.

To prove the theorem for $t = 2^n$ $(n = 0, 1, 2, \ldots)$, we note first that the result is obvious when $n = 0$ or 1 (and very easily proved when $n = 2$), and we shall proceed by mathematical induction, assuming $n \geqslant 2$, so that $t \geqslant 4$. Our inductive assumption is that $\frac{1}{2}t$ is ausgezeichnet.

Suppose that equation (10) is satisfied for some "vector" (a_r). Then

$$a_0 + (a_1 - a_{t-1})\cos\frac{\pi}{t} + (a_2 - a_{t-2})\cos\frac{2\pi}{t} + \cdots$$
$$+ (a_{\frac{1}{2}t-1} - a_{\frac{1}{2}t+1})\cos\frac{(\frac{1}{2}t - 1)\pi}{t} = 0 \tag{11}$$

and

$$(a_1 + a_{t-1})\sin\frac{\pi}{t} + (a_2 + a_{t-2})\sin\frac{2\pi}{t} + \cdots$$
$$+ (a_{\frac{1}{2}t-1} + a_{\frac{1}{2}t+1})\sin\frac{(\frac{1}{2}t - 1)\pi}{t} = 0. \tag{12}$$

Equation (11) can be rewritten as

$$\left[a_0 + (a_2 - a_{t-2})\cos\frac{2\pi}{t} + (a_4 - a_{t-4})\cos\frac{4\pi}{t} + \cdots\right]$$
$$+ \left[(a_1 - a_{t-1})\cos\frac{\pi}{t} + (a_3 - a_{t-3})\cos\frac{3\pi}{t} + \cdots\right] = 0. \tag{13}$$

Now, if m is any positive integer, $\cos(2m\pi/t)$ is a polynomial in $\cos(2\pi/t)$ with integer coefficients, while $\cos[(2m + 1)\pi/t]$ is of the form

$$\cos\frac{(2m + 1)\pi}{t} = R\left[\cos\frac{2\pi}{t}\right]\cos\frac{\pi}{t}, \tag{14}$$

where R, with or without a subscript, denotes a rational function (with rational coefficients), not necessarily the same function on each occasion. Equation (14) can be deduced, for example, from Hobson [5, p. 106, formula (6)], where in fact the rational function is a polynomial with integral coefficients. It then follows from (13) that either both bracketed expressions vanish or else $\cos(\pi/t)$ is a rational function of $\cos(2\pi/t)$. Therefore, if we can rule out the latter possibility, we see from our inductive hypothesis that

$$a_0 = a_1 - a_{t-1} = a_2 - a_{t-2} = \cdots = 0. \tag{15}$$

Similarly, on rewriting (12) as

$$(a_1 + a_{t-1})\cos\frac{(\frac{1}{2}t - 1)\pi}{t} + \cdots + (a_{\frac{1}{2}t-1} + a_{\frac{1}{2}t+1})\cos\frac{\pi}{t} = 0, \tag{16}$$

we infer that

$$a_1 + a_{t-1} = a_2 + a_{t-2} = \cdots = 0 \tag{17}$$

provided, once again, that, when $t = 4, 8, 16, \ldots,$

$$\cos(\pi/t) \text{ is not a rational function of } \cos(2\pi/t). \tag{18}$$

Thus, if we can prove (18), it will follow that (15) and (17) are both true and, therefore, $a_0 = a_1 = a_2 = \cdots = a_{t-1} = 0$, which would complete the inductive proof of our theorem. It remains to prove statement (18). To do so, we formulate a slightly more general result because the increased generality enables the method of induction to work.

Theorem 2: When $t = 2^n$ $(n = 2, 3, 4, \ldots)$ neither $\cos(\pi/t)$ nor $\sin(\pi/t)$ is of the form $R[\cos(2\pi/t)]$.

For its historical interest, we mention in passing that the product of all the cosines is $2/\pi$, as François Viète or Franciscus Vieta, an eminent mathematician, lawyer, and cryptanalyst, discovered in the seventeenth century. (See Hobson [5, p. 128] for its proof.) Vieta's formula is often expressed in the form

$$\frac{2}{\pi} = \frac{\sqrt{2}}{2}\cdot\frac{\sqrt{2 + \sqrt{2}}}{2}\cdot\frac{\sqrt{2 + \sqrt{2 + \sqrt{2}}}}{2}\cdot\ \cdots\ .$$

Proof of Theorem 2: When $t = 4$, the result is obvious, so we take $n > 2$ and proceed by induction. Suppose that $\cos(\pi/t) = R[\cos(2\pi/t)]$ and try to arrive at a contradiction. The rational function of $\cos(2\pi/t)$ is of the form

$$\frac{c_0 + c_1 \cos(2\pi/t) + \cdots + c_p \cos^p(2\pi/t)}{d_0 + d_1 \cos(2\pi/t) + \cdots + d_q \cos^q(2\pi/t)}$$

$$= \frac{P_1[\cos(4\pi/t)] + \cos(2\pi/t)P_2[\cos(4\pi/t)]}{P_3[\cos(4\pi/t)] + \cos(2\pi/t)P_4[\cos(4\pi/t)]},$$

where $P_1, \ldots, P_4$ are polynomials with integer coefficients. [See the remarks following equation (14).] Multiply the numerator and denominator by

$$P_3[\cos(4\pi/t)] - \cos(2\pi/t)P_4[\cos(4\pi/t)]$$

which, by the inductive hypothesis, does not vanish, and we obtain an equation of the form

$$\cos(\pi/t) = R_1[\cos(4\pi/t)] + \cos(2\pi/t)R_2[\cos(4\pi/t)].$$

Squaring both sides gives, after dropping the arguments of R_1 and R_2 for the sake of brevity,

$$\tfrac{1}{2} + \tfrac{1}{2}\cos(2\pi/t) = R_1^2 + [\tfrac{1}{2} + \tfrac{1}{2}\cos(4\pi/t)]R_2^2 + 2\cos(2\pi/t)R_1R_2.$$

However, by the inductive hypothesis, $\cos(2\pi/t)$ is not a rational function of $\cos(4\pi/t)$, so

$$\tfrac{1}{2} = R_1^2 + \cos^2(2\pi/t)R_2^2$$

and

$$1 = 4R_1R_2.$$

Therefore,

$$\tfrac{1}{2} = R_1^2 + \frac{\cos^2(2\pi/t)}{16R_1^2}.$$

Therefore,

$$R_1^4 - \tfrac{1}{2}R_1^2 + \frac{1}{16}\cos^2(2\pi/t) = 0.$$

Therefore,

$$R_1^2 = \tfrac{1}{2} \pm \sqrt{[\tfrac{1}{4} - \tfrac{1}{4}\cos^2(2\pi/t)} = \tfrac{1}{2}[1 \pm \sin(2\pi/t)].$$

Therefore, $\sin(2\pi/t)$ is a rational function of $\cos(4\pi/t)$, which is false by the inductive hypothesis. So $\cos(\pi/t)$ is not a rational function of $\cos(2\pi/t)$.

Similarly, if $\sin(\pi/t)$ is a rational function of $\cos(2\pi/t)$, we have, as before, in turn,

$$\sin(\pi/t) = R_3[\cos(4\pi/t)] + \cos(2\pi/t)R_4[\cos(4\pi/t)],$$

$$\tfrac{1}{2} - \tfrac{1}{2}\cos(2\pi/t) = R_3^2 + [\tfrac{1}{2} + \tfrac{1}{2}\cos(4\pi/t)]R_4^2 + 2\cos(2\pi/t)R_3R_4,$$

$$\tfrac{1}{2} = R_3^2 + \cos^2(2\pi/t)R_4^2,$$

$$-1 = 4R_3R_4,$$

and

$$\tfrac{1}{2} = R_3^2 + \frac{\cos^2(2\pi/t)}{16R_3^2},$$

and, just as before, we deduce that $\sin(\pi/t)$ cannot be a rational function of $\cos(2\pi/t)$. This completes the proof of Theorem 2 and hence of Theorem 1.

Theorem 3: When t is ausgezeichnet, that is, a power of 2, the degree of the algebraic integer j is t.

Proof: By Theorem 1 we know that 0 cannot be expressed as a cyclotomous integer other than in the obvious manner; that is, j cannot satisfy an equation of degree $t - 1$ or less having integral coefficients. But j does satisfy an equation of degree t, namely $j^t + 1 = 0$, so j is an algebraic integer of degree (precisely) t.

Theorem 4: If j is replaced by j^{2s+1} in (10), where s is a positive integer, then Theorem 1 remains valid.

To see this, note first that the sequence of complex numbers

$$1,\ j^{2s+1},\ j^{2(2s+1)},\ \ldots,\ j^{(t-1)(2s+1)}$$

is merely a permutation of the same sequence with s replaced by 0. Hence, the substitution leaves the class of cyclotomous numbers invariant. The remaining details of the proofs of Theorems 1 and 2 go through with only trivial changes.

Theorem 4 shows that the eigenvalues of the integral skew circulix A with top row $(a_0, a_1, \ldots, a_{t-1})$, where the a's are integers, are all uniquely expressible as cyclotomous integers, when t is a power of 2. These cyclotomous integers are called *associates* of one another and their product is det A, the determinant of A. This determinant is also known as the *norm* of any one of these cyclotomous integers.

When $t = 2$, the cyclotomous integers are the Gaussian integers $a + ib$. The associate of $a + ib$ is $a - ib$ and the norm is $a^2 + b^2$. The so-called *units* of the ring of Gaussian integers are those whose reciprocals are also Gaussian integers, that is, those with norm 1. These units are ±1 and $\pm i$. It is familiar that in the ring of Gaussian integers the "fundamental theorem of arithmetic" is true, that is, each Gaussian integer has a unique decomposition into prime Gaussian integers, apart from units. For a rigorous statement of this property, and for its proof, see, for example, Hardy and Wright [4, pp. 184-186].

3. THE CYCLOTOMOUS INTEGERS WHEN $t = 4$

Hardy and Wright [4, l.c., pp. 280-281] state the fundamental theorem for the algebraic integers $\alpha + \beta i + \gamma\sqrt{2} + \delta i\sqrt{2}$, where α and β are integers and γ and δ are either both integers or both halves of odd integers. It is readily seen that these are the same as the cyclotomous integers corresponding to $t = 4$, namely $a + bj + cj^2 + dj^3$, where $j = e^{\pi i/4} = (1 + i)/\sqrt{2}$. These again are the same as the cyclotomic integers corresponding to $m = 8$, but the cyclotomous form has the merit of unique representation. The proof of the fundamental theorem in this case can be obtained along the lines of the proof given in [4, §12.8] for the Gaussian integers, which is the case $m = 4$. But when $m = 2t = 16$, or any higher power of 2, this proof does not work, and presumably in these cases the decomposition into cyclotomous primes in not unique.

In the remainder of this section, we assume that $t = 4$. Let a, b, c, and d be integers, and let

$$A = \begin{bmatrix} a & b & c & d \\ -d & a & b & c \\ -c & -d & a & b \\ -b & -c & -d & a \end{bmatrix}. \tag{19}$$

Then

$$\det A = \prod_{s=0}^{3} [a + bj^{2s+1} + cj^{2(2s+1)} + dj^{3(2s+1)}]. \tag{20}$$

By pairing off the complex conjugate pair of factors with $s = 0$ and $s = 3$, and the pair with $s = 1$ and $s = 2$, we see that

$$\det A \geqslant 0. \tag{21}$$

The determinant $\det A$ is also called the norm of $a + bj + cj^2 + dj^3$ and will be denoted by $N(a, b, c, d)$.

The three ways of pairing off the four factors a of (20) ($s = 0, 1, 2, 3$), lead naturally to three ways of writing the norm. Thus:

$$\begin{aligned} a_0^\dagger a_1^\dagger &= (a + bj + cj^2 + dj^3)(a + bj^3 + cj^6 + dj^9) \\ &= a^2 - b^2 + c^2 - d^2 + (j + j^3)(ad + ab - bc + cd) \\ &= a^2 - b^2 + c^2 - d^2 + i\sqrt{2}(ad + ab - bc + cd). \end{aligned}$$

But $a_3^\dagger = \bar{a}_0^\dagger$, $a_2^\dagger = \bar{a}_1^\dagger$, so $a_2^\dagger a_3^\dagger$ is the complex conjugate of $a_0^\dagger a_1^\dagger$ and

$$N(a, b, c, d) = (a^2 - b^2 + c^2 - d^2)^2 + 2(ad + ab - bc + cd)^2. \tag{22}$$

Again

$$\begin{aligned} a_0^\dagger a_3^\dagger = |a_0^\dagger|^2 &= \left| a + \frac{b - d}{\sqrt{2}} + i\left(c + \frac{b + d}{\sqrt{2}}\right)\right|^2 \\ &= \left(a + \frac{b - d}{\sqrt{2}}\right)^2 + \left(c + \frac{b + d}{\sqrt{2}}\right)^2 \\ &= a^2 + b^2 + c^2 + d^2 + \sqrt{2}(-ad + ab + bc + cd), \end{aligned}$$

and

$$N(a, b, c, d) = (a^2 + b^2 + c^2 + d^2)^2 - 2(ad - ab - bc - ca)^2. \tag{23}$$

Finally,

$$\begin{aligned} a_0^\dagger a_2^\dagger &= (a + bj + cj^2 + dj^3)(a + bj^5 + cj^{10} + dj^{15}) \\ &= [a + ci + j(b + di)][a + ci - j(b + di)] = (a + ci)^2 - i(b + di)^2 \\ &= a^2 - c^2 + 2bd - i(b^2 - d^2 - 2ac). \end{aligned}$$

So

$$N(a,\ b,\ c,\ d) = (a^2 - c^2 + 2bd)^2 + (b^2 - d^2 - 2ac)^2. \tag{24}$$

Exercises:

(i) $N(a, b, c, d) = N(-a, -b, -c, -d) = N(d, c, b, a)$.

(ii) $N(-1, x-1, x, x+1) = (x^2+1)^2$. [Form $N(x, 0, 1, 0)N(0, 1, 1, 1)$.]

(iii) The product of the skew circulices whose top rows are $(x, 1, 0, 0)$, $(x, -1, 0, 0)$, $(x, 0, 0, 1)$, and $(x, 0, 0, -1)$ is $(x^4 + 1)I$.

(iv) $N(x, x, x+2, x+3) = N(x+2, x+3, x+1, x+1)$.

(v) $N(1, b, b, 0) - 1$, where b is an integer, is eight times the square of the triangular number $b(b-1)/2$.

(vi) If a positive integer ν is not of the form $\alpha^2 + 2\beta^2$, then ν^2 is of the form $h^2 + k^2 + 2\ell^2$, where not more than one of the three terms can vanish. (Hint: Use the equality of (23) and (24) combined with Bachet's theorem that every positive integer is the sum of four squares.]

Theorem 5: $N(a, b, c, d)$ vanishes only if $a = b = c = d = 0$.

For, from (23), $N(a, b, c, d) = 0$ implies that

$$a^2 + b^2 + c^2 + d^2 = \pm\sqrt{2}(ad - ab - bc - cd).$$

Therefore, $a^2 + b^2 + c^2 + d^2$, being rational, must vanish, and the result follows. (**Exercise:** The *rational* skew circulices form a field.)

Thus, (21) can be sharpened to

$$\det A \geqslant 1. \tag{25}$$

The units of the ring of cyclotomous integers (with $t = 4$) are the solutions of the Diophantine equation

$$N(a,\ b,\ c,\ d) = 1. \tag{26}$$

We shall adopt the abbreviation (a, b, c, d) for the number

$$a + bj + cj^2 + dj^3.$$

Theorem 6: The units of the ring of cyclotomous integers (with $t = 4$) are:

$$\pm 1,\ \pm j,\ \pm i,\ \pm j^3$$

and

$$(\varepsilon q_n,\ \pm p_n,\ \varepsilon q_n,\ 0),\ (0,\ \varepsilon q_n,\ \pm p_n,\ \varepsilon q_n),\ (-\varepsilon q_n,\ 0,\ \varepsilon q_n,\ \pm p_n)$$

and

$$(\pm p_n,\ -\varepsilon q_n,\ 0,\ \varepsilon q_n)$$

where $\varepsilon = 1$ or $\varepsilon = -1$, and p_n/q_n is the n^{th} convergent in the continued fraction for $\sqrt{2}$; that is,

$$p_n = \frac{(1+\sqrt{2})^n + (1-\sqrt{2})^n}{2},\quad q_n = \frac{(1+\sqrt{2})^n - (1-\sqrt{2})^n}{2\sqrt{2}}. \tag{27}$$

These units are all of the form

$$j^r(1 + j + j^2)^s, \tag{28}$$

where r and s are integers (positive, negative, or zero).

Recall first that the sequences of p_n's and q_n's begin with the values 1, 3, 7, 17, 41, 99, etc., and 1, 2, 5, 12, 29, 70, ..., and satisfy the recurrence relations $p_{n+1} = 2p_n + p_{n-1}$, $q_{n+1} = 2q_n + q_{n-1}$. Moreover, (p_n, q_n) provides the general solutions of the (Fermat-)Pell equations $r^2 = 2s^2 \pm 1$ (see, for example, LeVeque [6, pp. 139-144]). In fact

$$p_{2n}^2 = 2q_{2n}^2 + 1 \quad \text{and} \quad p_{2n-1}^2 = 2q_{2n-1}^2 - 1, \tag{29}$$

which is true even when $n = 0$ if we write $p_0 = 1$, $q_0 = 0$ (as we must if we want to satisfy the recurrence relations when $n = 1$).

To prove Theorem 6 we note, for example, that $N(a, b, a, 0) = (2a^2 - b^2)^2$, from (22), and hence $N(q_n, p_n, q_n, 0) = 1$, from (29). Or we can simply check that (1, 1, 1, 0) is a unit, that its inverse is (1, 0, -1, 1), and then show that all the units defined in (28) are of the forms mentioned in the rest of the statement of the theorem.

That there are no units other than those mentioned in the theorem follows from a deep theorem due to Dirichlet, concerning units in general; see, for example, LeVeque [6, p. 75]. In particular, therefore, $N(a, b, c, d) = 1$ implies $abcd = 0$.

As an example of Theorem 6, we have

$$N(29, 41, 29, 0) = \begin{vmatrix} 29 & 41 & 29 & 0 \\ 0 & 29 & 41 & 29 \\ -29 & 0 & 29 & 41 \\ -41 & -29 & 0 & 29 \end{vmatrix} = 1.$$

Although $N(\varepsilon q_n, \pm p_n, \varepsilon q_n, 0) = 1$, we have $N(q_n, p_n, -q_n, 0) = p_{2n}^2$, so the signs can have a big effect.

By (23), (29), and Theorem 6, we see that the only solutions of the simultaneous Diophantine equations

$$\begin{aligned} a^2 + b^2 + c^2 + d^2 &= p_{2n}, \\ ad - ab - bc - cd &= \pm q_{2n} \end{aligned} \tag{30}$$

are given by $a = c = \pm q_n$, $b = \pm p_n$, $d = 0$, and the "antirotations" of these solutions listed in the statement of Theorem 6. In particular, there is no solution with $abcd \neq 0$.

An allied question is what integers, and especially what primes, are expressible as integral skew circulants, not necessarily of order 4. For order 2, the problem is the familiar solved one of expressing integers as the sum of two squares. Since the product of two integral skew circulices is a third one, we know that the products of "expressible" numbers are also expressible (as skew circulants of order 4).

If $N(a, b, c, d)$ is prime, then, by (24) it must either be 2, for example, $N(1, 1, 0, 0) = 2$, or it is of the form $4q + 1$. In the latter case, r and s are of opposite parity, where $r = a^2 - c^2 + 2bd$ and $s = b^2 - d^2 - 2ac$. Suppose that r is odd and s is even. Then $a \not\equiv c \pmod 2$ and $b \equiv d \pmod 2$. By trying the four possibilities for the parities of (a, b, c, d) we see that $r^2 + s^2 \equiv 1 \pmod 8$, and the same conclusion is reached if r is even and s is odd. Thus, the only odd primes that $N(a, b, c, d)$ can equal are of the form $8n + 1$. I conjecture that every prime of this form is expressible as $N(a, b, c, d)$, that is, as an integral skew circulant, having found that this is true up to 1033, as shown in Table 1. Call this Conjecture 1.

Table 1. Values of (a, b, c, d) for which $p = N(a, b, c, d)$ where p is prime and $p \equiv 1 \pmod 8$, for all $p \leqslant 1033$. Solutions are given for which a, b, c, and d are all nonnegative.

p	a	b	c	d	p	a	b	c	d	p	a	b	c	d
17	2	1	0	0	337	4	3	0	0	641	5	2	0	0
41	2	1	1	1	353	4	1	1	1	673	3	3	2	3
73	2	2	0	1	401	3	3	1	2	761	4	7	8	2
89	3	1	1	0	409	4	2	0	1	769	4	0	2	3
97	3	2	0	0	433	4	0	2	1	809	4	3	0	2
113	3	0	1	1	449	4	2	3	0	857	1	6	3	1
137	3	3	2	1	457	3	1	3	2	881	5	4	0	0
193	3	1	2	1	521	3	2	1	3	929	5	1	2	1
233	1	4	1	1	569	6	8	7	0	937	5	0	1	3
241	4	2	1	0	577	5	3	1	0	953	5	1	1	2
257	4	1	0	0	593	4	2	1	2	977	5	5	2	1
281	5	5	3	0	601	8	11	9	1	1009	8	9	6	0
313	3	3	3	2	617	4	1	2	2	1033	7	9	8	1

Given a solution of $N(a, b, c, d) = 1$, we can multiply each of a, b, c, d by any number and thus show that all squares are expressible. So Conjecture 1 implies that all numbers of the form $2^q S p_1 p_2 \ldots$, where S is a square and p_1, p_2, ... are primes of the form $8n + 1$, are expressible, and I suspect that no other numbers are. (Conjecture 2.) This conjecture is based on well over one hundred numerical examples.

It is familiar that primes of the form $4n + 1$, and *a fortiori* those of the form $8n + 1$, are expressible in essentially only one way as the sum of two squares. Suppose that a prime $p \equiv 1 \pmod 8$ is $r^2 + s^2$, where we can take $r > 0$ and $s > 0$. Then, if Conjecture 1 is right, integers a, b, c, d exist, so that the two terms in (24) satisfy

$$\begin{aligned} &|a^2 - c^2 + 2bd| = r \text{ or } s \\ \text{and} \quad & \\ &|b^2 - d^2 - 2ac| = s \text{ or } r. \end{aligned} \tag{31}$$

Researches by Gauss, Lagrange, Cauchy, Eisenstein, Jacobi, and Stern (see Smith [9, p. 269] included the remarkable result that a prime p of the form $8n + 1$ is also uniquely expressible in the form $h^2 + 2k^2$, where

$$\pm 2h \equiv \binom{5n}{n} \pmod p. \tag{32}$$

Conjecture 1 would then imply, from (22), that h and k can be written (by no means uniquely) in the forms

$$h = |a^2 - b^2 + c^2 - d^2| \quad \text{and} \quad k = |ad + ab - bc + cd|. \tag{33}$$

We also know, by a theorem due to Gauss (see Smith [9, p. 268]), that $p = r^2 + s^2$, where

$$2r \equiv \binom{4n}{2n} \pmod{p}. \tag{34}$$

Formulas (31)-(34) can be helpful in finding values for a, b, c, d, that is, in expressing a prime of the form $8n + 1$ as a skew circulant.

Table 1 can be used for writing down, for a given prime $p \equiv 1 \pmod{8}$, the essentially unique solutions of $p = r^2 + s^2$ and $p = h^2 + 2k^2$ when $p \leqslant 1033$. We can also use the table (up to $p = 1033$), combined with (23), to obtain arbitrarily many solutions of $p = \alpha^2 - 2\beta^2$, because we can multiply (a, b, c, d) by any unit. For example,

$$\begin{aligned}(a, b, c, d) \times (1, 1, 1, 0) &= (a-c-d,\ a+b-d,\ a+b+c,\ b+c+d)\\ &= (a', b', c', d')\end{aligned}$$

say; and we see, by elementary algebra, that

$$a'^2 + b'^2 + c'^2 + d'^2 = 3(a^2+b^2+c^2+d^2) - 4(ad-ab-bc-cd),$$

while

$$a'd' - a'b' - b'c' - c'd' = 3(ad-ab-bc-cd) - 2(a^2+b^2+c^2+d^2).$$

This forces us to notice that if (α_n, β_n) is a solution of $p = \alpha^2 - 2\beta^2$, then another one is $(\alpha_{n-1}, \beta_{n-1})$, where we have the "backward" recursion

$$\alpha_{n-1} = 3\alpha_n - 4\beta_n,\ \beta_{n-1} = 3\beta_n - 2\alpha_n. \tag{35}$$

Likewise, by forming $(a, b, c, d)(1, 0, -1, 1)$, or from (35), we are led to the "forward" recursion

$$\alpha_n = 3\alpha_{n-1} + 4\beta_{n-1},\ \beta_n = 2\alpha_{n-1} + 3\beta_{n-1}. \tag{36}$$

Thus, given one solution, we can generate an unlimited supply (compare LeVeque [6, p. 146], for example), by climbing up and down a ladder infinite in both directions.

One can verify that equations (36) are equivalent to

$$\begin{aligned}\alpha_n &= [\ell\sqrt{8} - 4m)\lambda^{n+1} + (\ell\sqrt{8} + 4m)\mu^{n+1}](32)^{-\frac{1}{2}}\\ \beta_n &= [(2\ell - m\sqrt{8})\lambda^{n+1} - (2\ell + m\sqrt{8})\mu^{n+1}](32)^{-\frac{1}{2}},\end{aligned} \tag{37}$$

where n is *any* integer, $\lambda = 3 + \sqrt{8}$, $\mu = 3 - \sqrt{8} = \lambda^{-1}$, $\ell^2 - 2m^2 = p$. Indeed, using only the fact that $\lambda\mu = 1$, one can verify directly that if $\ell^2 - 2m^2 = x$, for any x, then $\alpha_n^2 - 2\beta_n^2 = x$ also. For example, when $p = 17$, we can take $\ell = 7$, $m = 4$, giving $\ldots\alpha_{-2} = 37$, $\alpha_{-1} = 7$, $\alpha_0 = 5$, $\alpha_1 = 23$, $\alpha_2 = 133$, $\ldots$, $\beta_{-2} = -26$, $\beta_{-1} = -4$, $\beta_0 = 2$, $\beta_1 = 16$, $\beta_2 = 94$, $\ldots$.

Equations (37), in their turn, are equivalent to

$$\alpha_{n+1} = 6\alpha_n - \alpha_{n-1},\ \beta_{n+1} = 6\beta_n - \beta_{n-1}, \tag{38}$$

which can be used both forward and backward. Equations (37) and (38) are decidedly Fibonaccian, so it is not surprising that the α's and β's have further nice properties. For example,

$$\alpha_n\alpha_{n+k} - 2\beta_n\beta_{n+k} = p\gamma_k,$$

where $\gamma_0 = 1$, $\gamma_1 = 3$, $\gamma_{n+1} = 6\gamma_n - \gamma_{n-1}$. The even-numbered numerators of the simple continued fraction for $\sqrt{2}$ are $\gamma_1, \gamma_2, \gamma_3, \ldots$.

To conclude this section, consider one more conjecture, Conjecture 3: Let $p \equiv 1 \pmod 8$ be prime. Then *all* solutions of $p = \alpha^2 - 2\beta^2$ can be obtained from (37), or recursively from (38), by starting with a single solution. That there *is* a solution would be a consequence of Conjecture 1. The two conjectures combined imply that all solutions are of the form shown in formula (23). (See Table 2.)

Table 2. Some solutions of $p = \alpha^2 - 2\beta^2$ where $p \equiv 1 \pmod 8$, and the top rows of the corresponding skew circulices. The signs preserve the recurrences $\alpha_{n+1} = 6\alpha_n - \alpha_{n-1}$, $\beta_{n+1} = 6\beta_n - \beta_{n-1}$. In each case, $\alpha = a^2 + b^2 + c^2 + d^2$ and $\beta = ad - ab - bc - cd$ as in formula (23).

$p = 17$						$p = 41$					
α	β	a	b	c	d	α	β	a	b	c	d
37	26	-2	4	-4	1	71	50	-1	5	-6	2
7	4	1	1	-2	1	13	8	2	1	-2	2
5	-2	2	1	0	0	7	-2	2	1	1	1
23	-16	2	3	3	1	29	-20	0	2	4	3
133	-94	-2	4	8	7	167	-118	-7	-1	6	9
775	-548	-17	-5	10	19	973	-688	-22	-17	-2	14

4. DISCUSSION OF ALLIED MATTERS

Complicated Numbers

In an unpublished paper, the author called the skew circulix (1) a representation of a "complicated number"

$$x_0 + j_1x_1 + \cdots + j_{t-1}x_{t-1}$$

and developed a theory of functions of a complicated variable (see Good [3]). The theory contained, for example, an easy generalization of the Cauchy-Riemann equations, and a more difficult generalization of Cauchy's residue theorem for integrals over contours encircling flat manifolds of dimension $t - 2$. These manifolds generalize the poles in the usual theory. Generalizations of Liouville's theorem and analytic continuation were also given. The following discussion is extracted from that document to which it was, however, somewhat incidental.

Generalized Trigonometry

The skew DFT is related to the following generalization of trigonometry.

Consider the differential equations

$$D^ty = k^ty, \tag{39}$$

$$D^ty = -k^ty, \tag{40}$$

where k is a positive number and D means d/du. (The case $t = 4$ occurs in the theory of a vibrating elastic bar; see Webster [11, p. 139].) A fundamental set of solutions (39) is given by the generalized hyperbolic functions of Ungar [10]:

$$f_r(u) = \frac{u^r}{r!} + \frac{u^{r+t}}{(r+t)!} + \frac{u^{r+2t}}{(r+2t)!} + \cdots \quad (r = 0, 1, \ldots, t-1), \tag{41}$$

while, for (40), a fundamental set contains the generalized trigonometric functions

$$g_r(u) = \frac{u^r}{r!} - \frac{u^{r+t}}{(r+t)!} + \frac{u^{r+2t}}{(r+2t)!} - \cdots \quad (r = 0, 1, \ldots, t-1). \tag{42}$$

(Compare to Muir [7, pp. 443-444], where the corresponding definitions contain minor errors; and Ramanujan [8].) The solution of (39), with initial values $c_0, c_1, c_2, \ldots, c_{t-1}$ for $y, Dy, \ldots, D^{t-1}y$ at $u = 0$, is $\Sigma c_r f_r(ku)$, while that of (40), with the same initial values, is $\Sigma c_r g_r(ku)$. Let us list some formulas that are satisfied by these generalized trigonometric functions. The reader should mentally consider what they state for the case $t = 2$. We omit most of the similar formulas for the functions $f_r(u)$. The reader might like to verify, however, that

$$\sum_r [f_r(u)]^2 = t^{-1}\sum_{s=0}^{t-1} \exp[2u \cos(2\pi s/t)]. \tag{43}$$

When $t \to \infty$, this gives a familiar formula for the Bessel function $I_0(2u)$ as an integral.

The formula

$$\exp(uj^{2s+1}) = \sum_{r=0}^{t-1} g_r(u)j^{r(2s+1)} \tag{44}$$

[which is true also when j is replaced by j^{2p+1} $(p = 0, 1, 2, \ldots)$], is a direct generalization of "de Moivre's formula," which is the case $t = 2$. As in ordinary trigonometry we can obtain an addition formula by first deducing an expression for $\exp[(u + y)j^{2s+1}]$ from (44), and then taking the inverse skew DRT. Another method, which is closely related, is to note that

$$e^{uJ} = g_0(u)I + g_1(u)J + \cdots + g_{t-1}(u)J^{t-1} \tag{45}$$

is a skew circulix whose eigenvalues are $\exp(uj^{2s+1})$ $(s = 0, 1, \ldots, t - 1)$. Hence,

$$g_r(u + y) = \sum_{s=0}^{t-1} \varepsilon_{r,s} g_s(u) g_{r+s}(y) \quad (r, s = 0, 1, \ldots, t-1), \tag{46}$$

where $\varepsilon_{r,s} = 1$ if $r \geqslant s$ and $\varepsilon_{r,s} = -1$ if $r < s$. These identities generalize the usual formulas for $\cos(u + y)$ and $\sin(u + y)$. It follows, for example, that $g_r(nu)$ is a homogeneous polynomial in $g_0(u), \ldots, g_{t-1}(u)$ $(n = 1, 2, 3, \ldots)$.

It seems fair to conclude that the skew circulix has not previously been given the attention that it merits.

REFERENCES

1. Philip J. Davis. *Circulant Matrices*. New York: Wiley, 1979.
2. Harold M. Edwards. *Fermat's Last Theorem*. New York: Springer, 1977.
3. I. J. Good. "A Simple Generalization of Analytic Function Theory." Unpublished paper, 1982.
4. G. H. Hardy & E. M. Wright. *An Introduction to the Theory of Numbers*. Oxford: Clarendon Press, 1938.
5. E. W. Hobson. *A Treatise on Plane and Advanced Trigonometry*. 7th ed. Cambridge: Cambridge University Press, 1928; rpt. New York: Dover, 1957.
6. W. J. LeVeque. *Topics in Number Theory*. Vol. I. Reading, Mass.: Addison-Wesley, 1956.
7. Thomas Muir. *A Treatise on the Theory of Determinants*. London: Constable, 1933; rpt. New York: Dover, 1960.
8. S. Ramanujan. "Some Properties of Bernoulli's Numbers." *J. London Math. Soc.* **3** (1911):219-234. Also in *Collected Papers of Srinivasa Ramanujan*, Cambridge: Cambridge University Press, 1927; New York: Dover, 1962, pp. 1-14.
9. H. J. S. Smith. *Report on the Theory of Numbers*. New York: Chelsea, n.d. Also in Vol. I of *The Collected Mathematical Papers of Henry John Stephen Smith*.
10. A. Ungar. "Generalized Hyperbolic Functions." *Amer. Math. Monthly* **89** (1982):688-691.
11. A. G. Webster. *Partial Differential Equations of Mathematical Physics*. 2nd ed. New York: Hafner, 1947.

◆◇◆◇◆