ILLINOIS JOURNAL OF MATHEMATICS
Volume 24, Number 1, Spring 1980

ON A PROBLEM SUGGESTED BY OLGA TAUSSKY-TODD[1]

BY
MORRIS NEWMAN

Abstract

The problem considered is to characterize those integers m such that $m = \det(C)$, C an integral $n \times n$ circulant. It is shown that if $(m, n) = 1$ then such circulants always exist, and if $(m, n) > 1$ and p is a prime dividing (m, n) such that $p^t \| n$, then $p^{t+1} \mid m$. This implies for example, that n never occurs as the determinant of an integral $n \times n$ circulant, if $n > 1$.

The problem considered here was suggested by Olga Taussky-Todd at the meeting of the American Mathematical Society in Hayward, California (April, 1977): namely, to characterize the integers which can occur as the determinant of an integral circulant.

Let P be the $n \times n$ full cycle

$$\begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & & \cdots & \\ 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}.$$

Let J be the $n \times n$ matrix all of whose entries are 1, so that

$$J = I + P + P^2 + \cdots + P^{n-1}.$$

Let $a_0, a_1, \ldots, a_{n-1}$ be integers, and let C be the circulant

$$a_0 I + a_1 P + \cdots + a_{n-1} P^{n-1}.$$

Let $f(x)$ be the polynomial $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$. Then the eigenvalues of C are $f(\zeta_n^k)$, $1 \le k \le n$, $\zeta_n = \exp(2\pi i/n)$. Hence the determinant of C is given by $\det(C) = \prod_{k=1}^{n} f(\zeta_n^k)$.

The set of numbers $\{k\}$ coincides with the set $\{n\mu/d\}$. Here k runs over the integers $1, 2, \ldots, n$, d over the divisors of n (written $d \mid n$), and μ over the integers less than or equal to d and relatively prime to d (written $\mu : d$). It follows that

$$\det(C) = \prod_{d \mid n} \prod_{\mu : d} f(\zeta_n^{n\mu/d}) = \prod_{d \mid n} \prod_{\mu : d} f(\zeta_d^{\mu}) = \prod_{d \mid n} Nf(\zeta_d),$$

[1] This work was supported by a National Science Foundation grant, the Institute for Interdisciplinary Applications of Algebra and Combinatorics, and the Department of Mathematics of the University of California, Santa Barbara.

Received March 9, 1978.

where $Nf(\zeta_d)$ is the norm of $f(\zeta_d)$ in the cyclotomic field $Q(\zeta_d)$, and hence a rational integer. Thus we have a factorization of the determinant of C into $\sigma_0(n)$ rational integers. Some of these, of course, may be ± 1.

We are interested in those m such that an integral $n \times n$ circulant C exists for which

$$\det(C) = m. \tag{1}$$

We may assume that $m > 0$, since $\det(-P) = -1$, so that $\det(C) = m$ if and only if $\det(-PC) = -m$. We may also assume that $n > 1$.

We first prove:

THEOREM 1. *Suppose that $(m, n) = 1$. Then equation (1) always has solutions.*

Proof. Write $m = nq + r$, $0 \le r \le n - 1$. Then also $(n, r) = 1$. Put

$$C = qJ + I + P + \cdots + P^{r-1}.$$

Then the eigenvalues of C are

$$nq + r = m, \quad 1 + \zeta_n^k + \zeta_n^{2k} + \cdots + \zeta_n^{(r-1)k}, \quad 1 \le k \le n - 1.$$

It follows that the determinant of C is given by

$$\det(C) = m \prod_{k=1}^{n-1} \frac{1 - \zeta_n^{rk}}{1 - \zeta_n^k}.$$

Now ζ_n^k and ζ_n^{rk} simultaneously run over all nth roots of unity other than 1, since $(r, n) = 1$. Thus $\prod_{k=1}^{n-1} (1 - \zeta_n^{rk}) = \prod_{k=1}^{n-1} (1 - \zeta_n^k) = n$, and so $\det(C) = m$. This concludes the proof.

The next result provides a characterization of those numbers m for which (1) may have a solution, in the remaining case when $(m, n) > 1$.

Let $q = p^t$, p prime, $t \ge 1$. Then the number $1 - \zeta_q$ is a prime in $Q(\zeta_q)$ of norm p. We shall now prove:

THEOREM 2. *Suppose that $(m, n) > 1$. Let p be a prime which divides (m, n), and let $p^t \| n$ (i.e., p^t is the exact power of p dividing n). Then if (1) has solutions, $p^{t+1} \mid m$.*

Proof. Write $n = qk$, $q = p^t$, $(k, p) = 1$, and suppose that (1) has solutions. We have

$$m = \det(C) = \prod_{d \mid n} Nf(\zeta_d) = \prod_{\delta \mid k} \prod_{s=0}^{t} Nf(\zeta_{p^s\delta}), \tag{2}$$

since the divisors of n coincide with the numbers $p^s\delta$, $0 \le s \le t$, $\delta \mid k$.

Since $(\delta + p^s, p^s\delta) = 1$, $Nf(\zeta_{p^s\delta}) = Nf(\zeta_{p^s\delta}^{\delta+p^s}) = Nf(\zeta_{p^s}\zeta_\delta)$. Also $\zeta_{p^s} = \zeta_q^{p^{t-s}} \equiv 1 \bmod 1 - \zeta_q$. It follows that

$$\begin{aligned} Nf(\zeta_{p^s\delta}) &= \prod_{\mu : p^s\delta} f((\zeta_{p^s}\zeta_\delta)^\mu) \\ &= \prod_{\mu_1 : p^s,\, \mu_2 : \delta} f((\zeta_{p^s}\zeta_\delta)^{\delta\mu_1 + p^s\mu_2}) \equiv \prod_{\mu_1 : p^s,\, \mu_2 : \delta} f(\zeta_\delta^{p^s\mu_2}) \mod 1 - \zeta_q, \end{aligned}$$

$$Nf(\zeta_{p^s\delta}) \equiv Nf(\zeta_\delta)^{\phi(p^s)} \mod 1 - \zeta_q. \tag{3}$$

In the above, $\mu = \delta\mu_1 + p^s\mu_2$, where μ_1 runs over a reduced set of residues modulo p^s, and μ_2 over a reduced set of residues modulo δ. This is possible, of course, because $(\delta, p^s) = 1$.

Now both sides of (3) are rational integers, and $N(1 - \zeta_q) = p$. It follows that

$$Nf(\zeta_{p^s\delta}) \equiv Nf(\zeta_\delta)^{\phi(p^s)} \mod p. \tag{4}$$

Now suppose that for every $\delta \mid k$, $Nf(\zeta_\delta) \not\equiv 0 \bmod p$. Then (2) and (4) would imply that $m \not\equiv 0 \bmod p$, a contradiction. Hence for some divisor δ of k, $Nf(\zeta_\delta) \equiv 0 \bmod p$. But then (4) implies that $Nf(\zeta_{p^s\delta}) \equiv 0 \bmod p$ for all s with $0 \le s \le t$, which in turn implies that $m \equiv 0 \bmod p^{t+1}$, by (2). This completes the proof.

As a corollary, we obtain the answer to one of the problems suggested by Olga Taussky-Todd:

THEOREM 3. *Suppose that $n > 1$. Then there is no integral $n \times n$ circulant of determinant n.*

This result raises the following question: although n does not occur as the determinant of an integral $n \times n$ circulant, will some power of n occur as such a determinant? The answer to this is supplied by the theorem that follows.

THEOREM 4. *There is an integral $n \times n$ circulant of determinant qn^2, where q is any integer.*

Proof. Put $C = I - P + qJ$. Then the eigenvalues of C are qn, $1 - \zeta_n^k$ $(1 \le k \le n - 1)$. Since $\prod_{k=1}^{n-1} (1 - \zeta_n^k) = n$, $\det(C) = qn^2$ and the result follows.

It is easy to show by examples that the conditions on m and n imposed by Theorem 2 are only necessary, but not sufficient, to guarantee the existence of an integral $n \times n$ circulant of determinant m when $(m, n) > 1$. The general question remains open. However, we *have* determined necessary and sufficient conditions in the case when n is prime. We have:

THEOREM 5. *Suppose that n is prime and that $(m, n) > 1$. Then in order for $m = \det(C)$ to have solutions, it is necessary and sufficient that $n^2 \mid m$.*

Proof. The necessity is a consequence of Theorem 2, and the sufficiency of Theorem 4.