PROGRESS ON OLGA TAUSSKY-TODD'S CIRCULANT PROBLEM

NORBERT KAIBLINGER

Abstract. Determining the possible values of integer circulant determinants is an open problem proposed by Taussky-Todd. Recent interest in this question comes from studying the Lehmer constant of finite cyclic groups. By refining the approach by Laquer and Newman we contribute to the circulant determinant problem in the case that the order is a power of two.

1. Introduction and main result

An integer circulant matrix is a matrix of the form

$$C_v = \begin{pmatrix} a_0 & a_1 & \dots & & a_{n-1} \\ a_{n-1} & a_0 & a_1 & & \\ & \ddots & \ddots & \ddots & \\ & & \ddots & \ddots & a_1 \\ a_1 & \dots & & a_{n-1} & a_0 \end{pmatrix}, \qquad v = (a_0, a_1, \dots, a_{n-1}) \in \mathbb{Z}^n.$$

Let $\mathscr{D}(n) \subseteq \mathbb{Z}$ denote the set of all possible values of $n \times n$ integer circulant determinants,

$$\mathscr{D}(n) = \{\det C_v \colon v \in \mathbb{Z}^n\}, \qquad n \geq 1.$$

Determining $\mathscr{D}(n)$ for an arbitrary positive integer n is an open problem, suggested by Taussky-Todd, see [15], and with implications for the Lehmer constant of finite cyclic groups [7, 12].

It is known that the set $\mathbb{Z}_n^* = \{d \in \mathbb{Z} \colon \gcd(d, n) = 1\}$ is always contained in $\mathscr{D}(n)$. In fact, Laquer [10] and Newman [15] showed that

$$\mathbb{Z}_n^* \cup n^2\mathbb{Z} \subseteq \mathscr{D}(n), \qquad n \geq 1. \tag{1}$$

See [13] for viewing this result in a more general context. In some cases the inclusion (1) is an identity. For example, the classical Diophantine result on the difference of two perfect squares implies

$$\mathscr{D}(2) = \{a_0^2 - a_1^2 \colon a_0, a_1 \in \mathbb{Z}\} = \mathbb{Z} \setminus 2\mathbb{Z}_2^* = \mathbb{Z}_2^* \cup 4\mathbb{Z}.$$

More generally, for $n = p$ prime, Laquer [10] and Newman [15] proved that

$$\mathscr{D}(p) = \mathbb{Z} \setminus p\mathbb{Z}_p^* = \mathbb{Z}_p^* \cup p^2\mathbb{Z}, \qquad p \text{ prime}.$$

2010 *Mathematics Subject Classification.* 11C08, 11C20, 11T22, 15A15, 15B05, 15B36.
Key words and phrases. Integer circulant matrix, determinant, resultant, cyclotomy.
Supported by the Austrian Science Fund FWF grant P 21339.

For $n = 2p$, twice an odd prime number, Laquer [10] also showed that

$$\begin{aligned} \mathscr{D}(2p) &= \mathscr{D}(2) \cap \mathscr{D}(p) \\ &= \mathbb{Z} \setminus (2\mathbb{Z}_2^* \cup p\mathbb{Z}_p^*) \qquad\qquad p \geq 3 \text{ prime.} \\ &= \mathbb{Z}_{2p}^* \cup 4\mathbb{Z}_p^* \cup p^2\mathbb{Z}_2^* \cup 4p^2\mathbb{Z}, \end{aligned} \tag{2}$$

For $n = p^2$, the square of an odd prime, Newman showed in [16] that

$$\mathscr{D}(p^2) = \mathbb{Z}_p^* \cup \begin{cases} 27\mathbb{Z}, & p = 3, \\ p^4\mathbb{Z}, & p \geq 5 \text{ prime.} \end{cases}$$

For $n = p^k$, a prime power, Newman [15, 16] has proved the inclusions

$$\mathbb{Z}_p^* \cup p^{2k}\mathbb{Z} \subseteq \mathscr{D}(p^k) \subseteq \mathbb{Z}_p^* \cup \begin{cases} p^{k+1}\mathbb{Z}, & p = 2, 3, \\ p^{k+2}\mathbb{Z}, & p \geq 5 \text{ prime,} \end{cases} \qquad k \geq 2. \tag{3}$$

By the next theorem, our main result, we improve these inclusions, for $p = 2$. In particular, we obtain $\mathscr{D}(4)$ and $\mathscr{D}(8)$.

Theorem 1.1. *We have* $\mathscr{D}(4) = \mathbb{Z}_2^* \cup 16\mathbb{Z}$, $\mathscr{D}(8) = \mathbb{Z}_2^* \cup 32\mathbb{Z}$, *and*

$$\mathbb{Z}_2^* \cup 2^{2k-1}\mathbb{Z} \subseteq \mathscr{D}(2^k) \subseteq \mathbb{Z}_2^* \cup 2^{k+2}\mathbb{Z}, \quad k \geq 4.$$

Proof. We apply the new lower bound derived in Section 4 (Theorem 4.4), and the new upper bound derived in Section 5 (Theorem 5.8).

First, by (3) we have $\mathbb{Z}_2^* \cup 16\mathbb{Z} \subseteq \mathscr{D}(4)$, and by Theorem 5.8 with $q = 1$ and $k = 2$ we have $\mathscr{D}(4) \subseteq \mathbb{Z}_2^* \cup 16\mathbb{Z}$.

Next, by Theorem 4.4(i) with $q = 2^{k-3}$ we have $\mathbb{Z}_2^* \cup 2^{2k-1}\mathbb{Z} \subseteq \mathscr{D}(2^k)$, for $k \geq 3$; and by Theorem 5.8 with $q = 1$ we have $\mathscr{D}(2^k) \subseteq \mathbb{Z}_2^* \cup 2^{k+2}\mathbb{Z}$, for $k \geq 3$. □

Example 1.2. By Theorem 1.1 there exists an integer circulant 16×16 matrix with determinant 128 and no such matrix exists with determinant 32. We do not know whether such a matrix exists with determinant 64.

Remark 1.3. The power 2^{k+2} in Theorem 1.1 is best possible in the sense that

$$\mathscr{D}(2^k) \not\subseteq \mathbb{Z}_2^* \cup 2^{k+3}\mathbb{Z}, \qquad k \geq 1,$$

see Example 3.3 below.

Open question: Determine $\mathscr{D}(n)$ in the presently unknown cases $n = 12, 15, 16, 18, \ldots$

The Section 2 contains preliminary results. In Section 4 we derive the lower bound for Theorem 1.1, and in Section 5 we derive the upper bound for Theorem 1.1.

2. Preliminary results

Denote by $\operatorname{Res}(f, g)$ the resultant of two polynomials $f, g \in \mathbb{Z}[x]$, expressed by a simplified product notation that we will use below. For non-constant g,

$$\operatorname{Res}(g, f) = c^{\deg f} \underbrace{\prod_{g(x)=0} f(x)}_{f(x_1)\cdots f(x_n),} \qquad \begin{array}{l} \text{for } c \in \mathbb{Z} \text{ and } x_1, \ldots, x_n \in \mathbb{C} \text{ such that} \\ g(x) = c \cdot (x - x_1) \cdots (x - x_n); \end{array}$$

and for constant g,

$$\mathrm{Res}(g,f)=\begin{cases}c^{\deg f}, & g=c\neq 0,\ f\neq 0,\\ 0, & g=0 \text{ or } f=0.\end{cases}$$

For the properties of the resultant we refer to [3, Section 4], [4, Chapter 12]. We will frequently use the following property.

Lemma 2.1. *Let $f_1,f_2,g\in\mathbb{Z}[x]$ and suppose g is monic and non-constant. Then the assumption $f_1\equiv f_2 \pmod g$ implies $\mathrm{Res}(g,f_1)=\mathrm{Res}(g,f_2)$.*

Proof. Apply [3, Lemma 4.1(i)]. Explicitly, if g is monic and non-constant, then for $f_2=f_1+h\cdot g$, with $h\in\mathbb{Z}[x]$,

$$\mathrm{Res}(g,f_2)=\prod_{g(x)=0}\big(f_1(x)+h(x)\cdot\underbrace{g(x)}_{=0}\big)=\prod_{g(x)=0}f_1(x)=\mathrm{Res}(g,f_1).$$

□

Remark 2.2. In Lemma 2.1 the condition that g is non-constant cannot be omitted, since for example, $\mathrm{Res}(1,0)=0$ is not equal to $\mathrm{Res}(1,1)=1$.

The next lemma lists several resultant formulas for later use.

Lemma 2.3. *Let $k,n\geq 1$ and let $\alpha=\gcd(k,n)$.*

(i)
$$\mathrm{Res}(1+\cdots+x^{n-1},1+\cdots+x^{k-1})=\begin{cases}1, & \alpha=1,\\ 0, & \alpha\geq 2.\end{cases}$$

(ii)
$$\mathrm{Res}(x^n-1,1+\cdots+x^{k-1})=\begin{cases}k, & \alpha=1,\\ 0, & \alpha\geq 2.\end{cases}$$

(iii)
$$\mathrm{Res}(1+\cdots+x^{n-1},1-x^k)=\begin{cases}n, & \alpha=1,\\ 0, & \alpha\geq 2.\end{cases}$$

(iv)
$$\mathrm{Res}(x^n+1,1+\cdots+x^{k-1})=\begin{cases}2^{\alpha-1}, & k/\alpha \textit{ odd},\\ 0, & k/\alpha \textit{ even}.\end{cases}$$

(v)
$$\mathrm{Res}(1+\cdots+x^{n-1},1+x^k)=\begin{cases}2^{\alpha-1}, & n/\alpha \textit{ odd},\\ 0, & n/\alpha \textit{ even}.\end{cases}$$

(vi)
$$\mathrm{Res}(x^n+1,1-x^k)=\begin{cases}2^{\alpha}, & k/\alpha \textit{ odd},\\ 0, & k/\alpha \textit{ even}.\end{cases}$$

(vii)
$$\mathrm{Res}(x^n-1,1+x^k)=\begin{cases}2^{\alpha}, & n/\alpha \textit{ odd},\\ 0, & n/\alpha \textit{ even}.\end{cases}$$

(viii)
$$\mathrm{Res}(x^n+1,1+x^k)=\begin{cases}2^{\alpha}, & n/\alpha \textit{ even or } k/\alpha \textit{ even},\\ 0, & n/\alpha, k/\alpha \textit{ odd}.\end{cases}$$

(ix)
$$\mathrm{Res}(x^n-1,1-x^k)=0.$$

Proof. (i) First, suppose $\alpha = 1$. Applying the usual Euclidean algorithm to the pair of integers $(n_1, k_1) = (n, k)$ yields $(n_2, k_2), \dots (n_r, k_r)$ such that for each $j = 1, \dots, r-1$,

$$n_{j+1} \equiv n_j (\mathrm{mod}\ k_j), \quad k_{j+1} = k_j \qquad \text{or} \qquad n_{j+1} = n_j, \quad k_{j+1} \equiv k_j (\mathrm{mod}\ n_j), \tag{4}$$

and since $\alpha = \gcd(n, k) = 1$,

$$n_r = 1, \quad k_r \geq 1 \qquad \text{or} \qquad n_r \geq 1, \quad k_r = 1. \tag{5}$$

For $\rho_{n,k} = \mathrm{Res}(1 + \cdots + x^{n-1}, 1 + \cdots + x^{k-1})$, we observe by using Lemma 2.1 that (4) implies $\rho_{n_{j+1},k_{j+1}} = \rho_{n_j,k_j}$, for $j = 1, \dots, r-1$, and (5) implies $\rho_{n_r,k_r} = 1$. Hence,

$$\mathrm{Res}(1 + \cdots + x^{n-1}, 1 + \cdots + x^{k-1}) = \rho_{n,k} = \rho_{n_2,k_2} = \cdots = \rho_{n_r,k_r} = 1.$$

Secondly, suppose $\alpha \geq 2$. Then the polynomial $1 + \cdots + x^{\alpha-1}$ divides both arguments of the resultant, whence the resultant vanishes. Thus (i) is verified for all $\alpha \geq 1$.
(ii) First, for $n = 1$, we have $\mathrm{Res}(x - 1, 1 + \cdots + x^{k-1}) = (1 + \cdots + x^{k-1})_{x=1} = k$. Hence, for general $n \geq 1$, by also using (i),

$$\begin{aligned}
&\mathrm{Res}(x^n - 1, 1 + \cdots + x^{k-1}) \\
&= \mathrm{Res}(x - 1, 1 + \cdots + x^{k-1})\ \mathrm{Res}(1 + \cdots + x^{n-1}, 1 + \cdots + x^{k-1}) \\
&= \begin{cases} k \cdot 1 = k, & \alpha = 1, \\ k \cdot 0 = 0, & \alpha \geq 2. \end{cases}
\end{aligned}$$

(iii) From (ii) we obtain, since $\alpha = 1$ implies $(-1)^{(n-1)(k+1)} = 1$,

$$\begin{aligned}
&\mathrm{Res}(1 + \cdots + x^{n-1}, 1 - x^k) \\
&= (-1)^{(n-1)k}\,\mathrm{Res}(1 - x^k, 1 + \cdots + x^{n-1}) \\
&= (-1)^{(n-1)k}(-1)^{n-1}\,\mathrm{Res}(x^k - 1, 1 + \cdots + x^{n-1}) \\
&= (-1)^{(n-1)(k+1)}\,\mathrm{Res}(x^k - 1, 1 + \cdots + x^{n-1}) \\
&= \begin{cases} 1 \cdot n = n, & \alpha = 1, \\ (-1)^{(n-1)(k+1)} \cdot 0 = 0, & \alpha \geq 2. \end{cases}
\end{aligned}$$

(iv)-(ix) Step I. (Preparatory computations). Suppose that $\alpha = 1$.
Then by using (ii) we have

$$\begin{aligned}
&\mathrm{Res}(x^n + 1, 1 + \cdots + x^{k-1}) \\
&= \frac{\mathrm{Res}(x^{2n} - 1, 1 + \cdots + x^{k-1})}{\mathrm{Res}(x^n - 1, 1 + \cdots + x^{k-1})} = \begin{cases} k/k = 1, & k \text{ odd}, \\ 0/k = 0, & k \text{ even}, \end{cases} \qquad (\alpha = 1).
\end{aligned} \tag{6}$$

From (6) we obtain

$$\begin{aligned}
&\mathrm{Res}(1 + \cdots + x^{n-1}, 1 + x^k) \\
&= (-1)^{(n-1)k}\,\mathrm{Res}(x^k + 1, 1 + \cdots + x^{n-1}) \\
&= \begin{cases} 1 \cdot 1 = 1, & n \text{ odd}, \\ (-1)^k \cdot 0 = 0, & n \text{ even}, \end{cases} \qquad (\alpha = 1).
\end{aligned} \tag{7}$$

Next, since

$$\begin{aligned}&\operatorname{Res}(x^n+1,1-x)\\&=(-1)^n\operatorname{Res}(1-x,x^n+1)\\&=(-1)^n(-1)^n\operatorname{Res}(x-1,x^n+1)\\&=1\cdot(x^n+1)_{x=1}=1\cdot 2=2,\end{aligned}\qquad(\alpha=1),$$

we have by using (6),

$$\begin{aligned}&\operatorname{Res}(x^n+1,1-x^k)\\&=\operatorname{Res}(x^n+1,1-x)\,\operatorname{Res}(x^n+1,1+\cdots+x^{k-1})\\&=\begin{cases}2\cdot 1=2, & k \text{ odd},\\ 2\cdot 0=0, & k \text{ even},\end{cases}\end{aligned}\qquad(\alpha=1).\tag{8}$$

From (8) we obtain

$$\begin{aligned}&\operatorname{Res}(x^n-1,1+x^k)\\&=(-1)^{nk}\operatorname{Res}(x^k+1,x^n-1)\\&=(-1)^{nk}(-1)^k\operatorname{Res}(x^k+1,1-x^n)\\&=\begin{cases}1^k\cdot 2=2, & n \text{ odd},\\ (-1)^k\cdot 0=0, & n \text{ even},\end{cases}\end{aligned}\qquad(\alpha=1).\tag{9}$$

From (8) and (9) we obtain, since $\operatorname{Res}\big(f(-x),g(-x)\big)=\operatorname{Res}\big(f(x),g(x)\big)$,

$$\begin{aligned}&\operatorname{Res}(x^n+1,1+x^k)\\&=\operatorname{Res}\big((-x)^n+1,1+(-x)^k\big)\\&=\begin{cases}\operatorname{Res}(x^n+1,1-x^k)=2, & n \text{ even},\\ \operatorname{Res}(-x^n+1,1+x^k) & \\ =(-1)^k\operatorname{Res}(x^n-1,1+x^k)=1\cdot 2, & k \text{ even},\end{cases}\end{aligned}\qquad(\alpha=1).\tag{10}$$

We also note that

$$\operatorname{Res}(x^n+1,1+x^k)=0,\quad n,k \text{ odd},\qquad(\alpha=1),\tag{11}$$

since the polynomial $x+1$ divides both arguments of the resultant.

Step II (Proof of (iv)-(ix)).
Since by the chain rule for resultants [14] we have

$$\operatorname{Res}\big(f(x^\alpha),g(x^\alpha)\big)=\operatorname{Res}(f,g)^\alpha,$$

we observe that (vi) follows from (8); that (vii) follows from (9); and that (viii) follows from (10) combined with (11).

Next, (iv) is obtained from (vi) by computing

$$\begin{aligned}&\operatorname{Res}(x^n+1,1+\cdots+x^{k-1})\\&=\frac{\operatorname{Res}(x^n+1,1-x^k)}{\operatorname{Res}(x^n+1,1-x)}=\begin{cases}2^\alpha/2=2^{\alpha-1}, & k/\alpha \text{ odd},\\ 0/2=0, & k/\alpha \text{ even}.\end{cases}\end{aligned}$$

and (v) is obtained from (vii) in an analogous way.

Finally, the resultant in (ix) vanishes indeed, since the polynomial $x-1$ divides both arguments of the resultant. □

3. Resultants and the structure of $\mathscr{D}(n)$

In the first lemma we list some basic properties of $\mathscr{D}(n)$, for $n \geq 1$.

Lemma 3.1. *Let $n \geq 1$.*
(i) *$\mathscr{D}(n)$ is a submonoid of $\mathbb{Z}$ with multiplication.*
(ii) *$d \in \mathscr{D}(n) \Leftrightarrow -d \in \mathscr{D}(n)$.*

Proof. (i) First, the integer circulant $n \times n$ matrices form an (abelian) submonoid of the (non-commutative) monoid of all $n \times n$ integer matrices, with matrix multiplication. Secondly, the determinant function is multiplicative.
(ii) Notice that $\det C_v = -1$, for $v = (0, -1, 0, \ldots, 0) \in \mathbb{Z}^n$, and use (i). □

The next lemma is concerned with the relation between circulant determinants and polynomial resultants discussed in [2, p. 76], used, e.g., in [1, 6, 7, 19]. The lemma includes both directions of this relation.

Lemma 3.2. (i) *For $v = (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$, let $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$. Then $\det C_v = \operatorname{Res}(x^n - 1, f)$.*
(ii) *Conversely, for $f \in \mathbb{Z}[x]$, let $v = (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$ such that $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \equiv f(x) \bmod (x^n - 1)$. Then $\operatorname{Res}(x^n - 1, f) = \det C_v$.*
(iii) *In particular,*

$$\mathscr{D}(n) = \{\operatorname{Res}(x^n - 1, f) \colon f \in \mathbb{Z}[x]\}.$$

Proof. (i) See [2, p. 76]. Explicitly, the usual formula expressing the determinant of a circulant matrix as the product of its eigenvalues [2, p. 75], [8, Theorem 17] implies

$$\det C_v = \prod_{x^n - 1 = 0} f(x) = \operatorname{Res}(x^n - 1, f). \tag{12}$$

(ii) Let $h(x) = a_0 + \cdots + a_{n-1}x^{n-1}$. By (i) we have $\det C_v = \operatorname{Res}(x^n - 1, h)$ and thus by applying Lemma 2.1 we obtain $\det C_v = \operatorname{Res}(x^n - 1, h) = \operatorname{Res}(x^n - 1, f)$.
(iii) Combine (i) and (ii). □

Example 3.3. Let $v = (3, -1, 0, \ldots, 0) \in \mathbb{Z}^n$, $n \geq 2$. Then $\det C_v = \operatorname{Res}(x^n - 1, 3 - x) = 3^n - 1$. For $n = 2^k$, with $k \geq 1$, this example verifies Remark 1.3; in fact, induction on $k \geq 1$ shows that $3^n - 1 = 2^{k+2} \cdot \text{odd}$, and hence $\det C_v \notin \mathbb{Z}_2^* \cup 2^{k+3}\mathbb{Z}$.

Remark 3.4. For $v \in \mathbb{Z}^n$, define the skew-circulant matrix S_v like the circulant matrix C_v but with reversed signs below the diagonal. The formula for a skew-circulant determinant is analogous to (12), by using [2, p. 84], [9, Theorem 22] we have

$$\det S_v = \prod_{x^n + 1 = 0} f(x) = \operatorname{Res}(x^n + 1, f). \tag{13}$$

By (12) and (13) we observe that Lemma 2.3 includes formulas for $\det C_v$ and $\det S_v$, for

$$v = (\underbrace{1,\dots,1}_{k},\underbrace{0,\dots,0}_{n-k}) \in \mathbb{Z}^n, \qquad 1 \le k \le n,$$

$$v = (1,\underbrace{0,\dots,0}_{k-1},\pm 1,\underbrace{0,\dots,0}_{n-k-1}) \in \mathbb{Z}^n, \qquad 1 \le k \le n-1;$$

thus in particular it yields a proof based solely on integer computations of a determinant formula in [2, p. 82], [10, Lemma 2], [15, Theorem 1].

By the next lemma we prove a property of resultants that we will use in the proof of Lemma 3.6 below.

Lemma 3.5. *Let $f, g_1, g_2 \in \mathbb{Z}[x]$ and suppose g_1, g_2 are monic and non-constant. Define $h \in \mathbb{Z}[x]$ by $h(u) = \operatorname{Res}\big(g_2(x) - u, f(x)\big)$. Then $\operatorname{Res}(g_1 \circ g_2, f) = \operatorname{Res}(g_1, h)$.*

Proof. Since g_1 and g_2 are monic and non-constant, also $g_1 \circ g_2$ is monic and non-constant and we have

$$\begin{aligned}\operatorname{Res}(g_1 \circ g_2, f) &= \prod_{g_1 \circ g_2(x)=0} f(x) \\ &= \prod_{g_1(u)=0} \prod_{g_2(x)-u=0} f(x) \\ &= \prod_{g_1(u)=0} \operatorname{Res}\big(g_2(x) - u, f(x)\big) = \prod_{g_1(u)=0} h(u) = \operatorname{Res}(g_1, h).\end{aligned}$$

□

The lower bound for $\mathscr{D}(n)$ in (1) is applicable for general $n \ge 1$. In contrast, upper bounds are stated above only for special n. The next lemma allows us to deduce an upper bound for $\mathscr{D}(n)$, with arbitrary $n \ge 1$, from the case that $n = p^k$ is a prime power (Equation (3) and Theorem 1.1). As usual, we write $p^k \parallel n$, when $p^k \mid n$ and $p^{k+1} \nmid n$, for p prime and $k \ge 1$; thus $n = \prod_{p^k \parallel n} p^k$.

Lemma 3.6. *Let $n, q \ge 1$. If $q \mid n$, then $\mathscr{D}(n) \subseteq \mathscr{D}(q)$. In particular,*

$$\mathscr{D}(n) \subseteq \bigcap_{p^k \parallel n} \mathscr{D}(p^k).$$

Proof. It is known from a construction by Torelli [18, p. 74], that an $n \times n$ integer circulant determinant can be written, for any positive $q \mid n$, as a $q \times q$ integer circulant determinant, see also the specific formula in [10, Theorem 2]. We state a particularly transparent construction in terms of resultants, as follows. Let $q \ge 1$ such that $q \mid n$, and define $h \in \mathbb{Z}[x]$ by

$$h(u) = \operatorname{Res}(x^{n/q} - u, f(x)), \qquad \text{for } f \in \mathbb{Z}[x],$$

Then by Lemma 3.5 we have

$$\operatorname{Res}(x^n - 1, f) = \operatorname{Res}(x^q - 1, h).$$

□

Example 3.7. For example, let $n = 12 = 3 \cdot 4$. Then Lemma 3.6 allows us to deduce from (1), (3), and Theorem 1.1 that

$$\mathbb{Z}_6^* \cup 144\mathbb{Z} \subseteq \mathscr{D}(12) \subseteq \mathbb{Z}_6^* \cup 9\mathbb{Z}_2^* \cup 16\mathbb{Z}_3^* \cup 144\mathbb{Z},$$

note that $\mathbb{Z}_{12}^* = \mathbb{Z}_6^*$.

4. Refining the lower bound

For $n = 2^k$, a power of two, the lower bound in (3) reads

$$\mathbb{Z}_2^* \cup 2^{2k}\mathbb{Z} \subseteq \mathscr{D}(2^k), \quad k \geq 2. \tag{14}$$

In this section we sharpen this lower bound, see Theorem 4.4 below with $q = 2^{k-3}$, for $k \geq 3$. Our approach is based on the ideas in the proof of (2) by Laquer [10].

We formulate a result by Laquer for circulant determinants [10, Theorem 1], see also [15, Theorem 4], in terms of resultants.

Lemma 4.1. *Let $n \geq 1$ and $f_0 \in \mathbb{Z}[x]$. For $a \in \mathbb{Z}$, let $f_a(x) = f_0(x) + a \cdot (1 + \cdots + x^{n-1})$. If $f_0(1) \neq 0$, then*

$$\operatorname{Res}(x^n - 1, f_a) = \frac{f_0(1) + n \cdot a}{f_0(1)} \operatorname{Res}(x^n - 1, f_0).$$

This identity expresses $\det C_{v_a}$, for $v_a = v_0 + (a, \ldots, a) \in \mathbb{Z}^n$, in terms of $\det C_{v_0}$, for $v_0 \in \mathbb{Z}^n$.

Proof. The case $n = 1$ is clear. Let $n \geq 2$. Since $f_a \equiv f_0 \bmod (1 + \cdots + x^{n-1})$ and $f_0(1) \neq 0$, we have by Lemma 2.1 that

$$\begin{aligned} \frac{\operatorname{Res}(x^n - 1, f_0)}{f_0(1)} &= \frac{\operatorname{Res}(x^n - 1, f_0)}{\operatorname{Res}(x - 1, f_0)} \\ &= \operatorname{Res}(1 + \cdots + x^{n-1}, f_0) \\ &= \operatorname{Res}(1 + \cdots + x^{n-1}, f_a) \\ &= \frac{\operatorname{Res}(x^n - 1, f_a)}{\operatorname{Res}(x - 1, f_a)} = \frac{\operatorname{Res}(x^n - 1, f_a)}{f_0(1) + n \cdot a} \end{aligned}$$

□

The next lemma is concerned with the determinant of an integer circulant $n \times n$ matrix constructed by Laquer [10] for use in his proof of the identity (2) above. While Laquer treats the case $n = 2p$, where p is an odd prime [10, Theorem 9], we are interested in the case that n is a power of two and indeed we we determine $\det C_v$ for general $n = 2, 4, 6, \ldots$. For example, the reduction principle in [10, Corollary of Theorem 2] is limited to the case $n = 2\cdot$odd; our more general version is inspired by a determinantal formula by Scott [18, p. 75] and arguments in [19, Section 2].

Lemma 4.2. *Let $n = 2, 4, 6, \ldots$, let $a \in \mathbb{Z}$, and let*

$$f_a(x) = 1 + (x^2 + \cdots + x^{n/2}) + a \cdot (1 + \cdots + x^{n-1}).$$

Then

$$\operatorname{Res}(x^n - 1, f_a) = \begin{cases} (2a+1) \cdot n^2/2, & n \equiv 0 \bmod 8, \\ (2a+1) \cdot n^2/4, & n \equiv 2, 6 \bmod 8, \\ 0, & n \equiv 4 \bmod 8. \end{cases}$$

This identity expresses $\det C_v$ for $v = (1, 0, \underbrace{1, \ldots, 1}_{n/2-1}, \underbrace{0, \ldots, 0}_{n/2-1}) + (a, \ldots, a) \in \mathbb{Z}^n$.

Proof. STEP 1 ($a = 0$). Let $m = n/2$, thus $f_0(x) = 1 + (x^2 + \cdots + x^m)$. First, note that

$$\operatorname{Res}(x^{2m} - 1, f_0) = \operatorname{Res}(x - 1, f_0)\, \operatorname{Res}(1 + \cdots + x^{m-1}, f_0)\, \operatorname{Res}(x^m + 1, f_0). \tag{15}$$

The next two equations express a determinant in [10, Lemma 1], [15, Theorem 4], we include a short proof in the language of resultants. First, note that

$$\operatorname{Res}(x - 1, f_0) = f_0(1) = m. \tag{16}$$

By using Lemma 2.1 and Lemma 2.3(iii) we have

$$\begin{aligned} &\operatorname{Res}(1 + \cdots + x^{m-1}, f_0) \\ &= \operatorname{Res}\left(1 + \cdots + x^{m-1}, f_0 - x\cdot(1 + \cdots + x^{m-1})\right) \\ &= \operatorname{Res}(1 + \cdots + x^{m-1}, 1 - x) = m. \end{aligned} \tag{17}$$

Next, by using Lemma 2.1 and Lemma 2.3(iv) we compute

$$\begin{aligned} \operatorname{Res}(x^m + 1, f_0) &= \operatorname{Res}\left(x^m + 1, f_0 + x \cdot (x^m + 1)\right) \\ &= \operatorname{Res}(x^m + 1, 1 + \cdots + x^{m+1}) = \begin{cases} 2, & m \equiv 0 \bmod 4, \\ 1, & m \text{ odd}, \\ 0, & m \equiv 2 \bmod 4. \end{cases} \end{aligned} \tag{18}$$

Combining (15), (16), (17), (18), and noting that $n = 2m$, we obtain the lemma for $a = 0$.
STEP 2 ($a \in \mathbb{Z}$). Apply Lemma 4.1 to the case $a = 0$ treated in Step I. Since $f_0(1) = n/2$, we obtain $\operatorname{Res}(x^n - 1, f_a) = (2a + 1) \cdot \operatorname{Res}(x^n - 1, f_0)$. □

Part (i) of the next result is obtained from [10, Lemma 4], we include a simple proof in terms of resultants.

Lemma 4.3. *For $q \geq 1$ odd, the following hold.*

(i) $$\operatorname{Res}(x^{2q} - 1, 1 + x^{q+1}) = 4 \quad \textit{and} \quad \operatorname{Res}(x^{2q} - 1, 1 + x + x^2 + x^{q+1}) = 8.$$

(ii) $$2^k \in \mathscr{D}(2q), \qquad \textit{for } k \geq 2.$$

Proof. (i) For the first identity, see Lemma 2.3(vii). For the second identity we compute by using Lemma 2.3(vii),(viii), for $f(x) = 1 + x + x^2 + x^{q+1}$,

$$\begin{aligned} &\operatorname{Res}(x^{2q} - 1, f) \\ &= \operatorname{Res}(x^q - 1, f)\, \operatorname{Res}(x^q + 1, f) \\ &= \operatorname{Res}\left(x^q - 1, f - x \cdot (x^q - 1)\right) \operatorname{Res}\left(x^q + 1, f - x \cdot (x^q + 1)\right) \\ &= \operatorname{Res}(x^q - 1, 1 + 2x + x^2)\, \operatorname{Res}\left(x^q + 1, 1 + x^2\right) \\ &= \operatorname{Res}(x^q - 1, 1 + x)^2\, \operatorname{Res}\left(x^q + 1, 1 + x^2\right) = 2^2 \cdot 2 = 8. \end{aligned}$$

(ii) Since $\{4,\ 8,\ 4^2,\ 8\cdot 4,\ 4^3,\ 8\cdot 4^2, \dots\} = \{2^k \colon k \geq 2\}$ and since $\mathscr{D}(n)$ is closed under multiplication, we observe that (i) implies (ii). □

Combining Lemma 4.2 and Lemma 4.3 we have the following.

Theorem 4.4. (i) *We have $\mathbb{Z}_{2q}^* \cup 32q^2\mathbb{Z} \subseteq \mathscr{D}(8q)$, for $q \geq 1$.*
(ii) *We have $\mathbb{Z}_{2q}^* \cup 4\mathbb{Z}_q^* \cup q^2\mathbb{Z}_2^* \cup 4q^2\mathbb{Z} \subseteq \mathscr{D}(2q)$, for $q \geq 1$ odd.*

Proof. (i) By Lemma 4.2 we have $32q^2\mathbb{Z}_2^* \subseteq \mathscr{D}(8q)$. Combined with (1) we conclude that

$$\underbrace{32q^2\mathbb{Z}_2^* \cup (\mathbb{Z}_{2q}^* \cup 64q^2\mathbb{Z})}_{\mathbb{Z}_{2q}^* \cup 32q^2\mathbb{Z}} \subseteq \mathscr{D}(8q).$$

(ii) By (1) we have $\mathbb{Z}_{2q}^* \subseteq \mathscr{D}(2q)$ and $4q^2\mathbb{Z} \subseteq \mathscr{D}(2q)$. By Lemma 4.2 we have $q^2\mathbb{Z}_2^* \subseteq \mathscr{D}(2q)$. By Lemma 4.3 we have $\{2^k \colon k \geq 2\} \subseteq \mathscr{D}(2q)$ and hence also

$$4\mathbb{Z}_q^* = \{2^k \colon k \geq 2\}\, \mathbb{Z}_{2q}^* \subseteq \mathscr{D}(2q).$$

Combining these inclusions we obtain (ii). □

5. Refining the upper bound

For $n = 2^k$, a power of two, the upper bound in (3) reads

$$\mathscr{D}(2^k) \subseteq \mathbb{Z}_2^* \cup 2^{k+1}\mathbb{Z}, \quad k \geq 2.$$

In this section we show how to complement Newman's arguments in [15, 16] so to refine this upper bound, see Theorem 5.8 below.

The next lemma is concerned with the factorization of an integer circulant determinant, expressed as a resultant. The factors of the product in (12) are not integers, in general. Newman [15, 16] makes use of a factorization by cyclotomic field norms, such that the factors are integers. It is expressed in terms of resultants by the next lemma. Let $\Phi_m \in \mathbb{Z}[x]$, $m \geq 1$, denote the m^{th} cyclotomic polynomial, i.e., the monic polynomial whose zeros are the primitive m^{th} roots of unity, such as $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$, $\Phi_3(x) = x^2 + x + 1$, or $\Phi_4(x) = x^2 + 1$.

Lemma 5.1. *Let $f \in \mathbb{Z}[x]$.*
(i) *For general $n \geq 1$,*

$$\operatorname{Res}(x^n - 1, f) = \prod_{q|n} \operatorname{Res}(\Phi_q, f).$$

(ii) *In particular, for $n = p^k$, a prime power,*

$$\operatorname{Res}(x^{p^k} - 1, f) = \prod_{j=0}^{k} \operatorname{Res}(\Phi_{p^j}, f) = f(1) \prod_{j=1}^{k} \operatorname{Res}(\Phi_{p^j}, f), \qquad p \text{ prime},\ k \geq 1.$$

(iii) *More specifically, for $n = 2^k$, a power of two,*

$$\operatorname{Res}(x^{2^k} - 1, f) = \prod_{j=0}^{k} \operatorname{Res}(\Phi_{2^j}, f) = f(1)\, f(-1)\, |f(i)|^2 \prod_{j=3}^{k} \operatorname{Res}(\Phi_{2^j}, f), \qquad k \geq 3.$$

Proof. (i),(ii) Note that $x^n - 1 = \prod_{q|n} \Phi_q$, for $n \geq 1$.
(iii) For $n = 2^k$, also notice that

$$\operatorname{Res}(\Phi_{2^j}, f) = \begin{cases} \operatorname{Res}(x - 1, f) = f(1), & j = 0, \\ \operatorname{Res}(x^{2^{j-1}} + 1, f) = \displaystyle\prod_{x^{2^{j-1}}+1=0} f(x), & j \geq 1, \end{cases}$$

such as

$$\text{(19)}\qquad \operatorname{Res}(\Phi_1, f) = f(1), \quad \operatorname{Res}(\Phi_2, f) = f(-1), \quad \text{and} \quad \operatorname{Res}(\Phi_4, f) = |f(i)|^2. \qquad \square$$

The next result will be used in the proof of Lemma 5.4 below.

Lemma 5.2. *Let p prime and $k \geq 1$. Then $\Phi_{p^k}(x) \equiv (x-1)^{p-1} \bmod p$.*

Proof. Case I ($k = 1$). Let ϕ denote the Euler totient function. A formula by Guerrier [5] states, if $n \geq 1$ and $n = qp^k$ such that $p \nmid q$, then $\Phi_n(x) \equiv \big(\Phi_q(x)\big)^{\phi(p^k)} \bmod p$. Hence in particular,

$$\Phi_p(x) \equiv \underbrace{\big(\Phi_1(x)\big)^{p-1}}_{=(x-1)^{p-1}} \qquad \bmod p.$$

Case II ($k \geq 2$). Note that $\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}}) \equiv \Phi_p(x) \bmod p$, and apply Case I. $\square$

Remark 5.3. The lemma can also be proved more explicitly by computing

$$\begin{aligned}\Phi_{p^k}(x) &= 1 + x^{p^{k-1}} + x^{2p^{k-1}} + \cdots + x^{(p-1)p^{k-1}} \\ &\equiv 1 + x + x^2 + \cdots + x^{p-1} \equiv \begin{cases} 0, & x \equiv 1 (\bmod\ p), \\ 1, & x \not\equiv 1 (\bmod\ p), \end{cases} \qquad \bmod p,\end{aligned}$$

whence $\Phi_{p^k}(x+1) \equiv \chi_0(x) \bmod p$, where χ_0 denotes the principal character modulo p. Note that also $x^{p-1} \equiv \chi_0(x) \bmod p$.

The next lemma refines a key argument in the proof of [15, Theorem 2]. In fact, it can be deduced from [15, Equation (4)] by applying Euler's theorem. The use of resultants allows us to give a simple self-contained proof.

Lemma 5.4. *Let p prime and $f \in \mathbb{Z}[x]$. Then the following hold.*
(i) *We have the congruence*

$$\operatorname{Res}(\Phi_p, f) \equiv \operatorname{Res}(\Phi_{p^2}, f) \equiv \operatorname{Res}(\Phi_{p^3}, f) \equiv \cdots \equiv \begin{cases} 0, & p \mid f(1), \\ 1, & p \nmid f(1), \end{cases} \qquad \bmod p.$$

(ii) *For $k \geq 1$, we have $\operatorname{Res}(x^{p^k} - 1, f) \equiv f(1) \bmod p$.*

Proof. (i) By Lemma 5.2, we have $\Phi_{p^k}(x) \equiv (x-1)^{p-1} \bmod p$. Hence,

$$\begin{aligned}\operatorname{Res}(\Phi_{p^k}, f) &\equiv \operatorname{Res}\big((x-1)^{p-1}, f\big) \\ &= f(1)^{p-1} \equiv \begin{cases} 0, & p \mid f(1), \\ 1, & p \nmid f(1), \end{cases} \qquad \bmod p.\end{aligned}$$

(ii) Apply (i) to Lemma 5.1(ii), reduced modulo p. $\square$

Remark 5.5. Expressing Lemma 5.4(ii) in terms of determinants we have for $n = p^k$, a prime power, and $v = (a_0, \ldots, a_{n-1}) \in \mathbb{Z}^n$, that

$$\text{(20)}\qquad \det C_v \equiv a_0 + \cdots + a_{n-1}, \qquad \bmod p.$$

Thus the lemma implies a more general version of the result in [10, Lemma 3], [11, Theorem 1], [17, Theorem 7], where (20) is obtained in the special case $n = p$. (The two different expressions used in these references, $a_0 + \cdots + a_{p-1}$ and $a_0^p + \cdots + a_{p-1}^p$, are equivalent modulo p.) Related congruences are treated in [20] for a probabilistic analysis of integer circulant determinants.

A key step by Newman in [16] is to determine, for $p \geq 3$ prime, whether there exists $f \in \mathbb{Z}[x]$ such that

$$(*) \qquad \underbrace{\mathrm{Res}(\Phi_1, f)}_{= f(1)} = \mathrm{Res}(\Phi_p, f) = \mathrm{Res}(\Phi_{p^2}, f) = p.$$

In fact, by [16, Theorem 2], and [16, Theorem 4], he proved that

$$(21) \qquad (*) \text{ is } \begin{cases} \text{possible}, & \text{for } p = 3, \\ \text{impossible}, & \text{for } p \geq 5 \text{ prime}; \end{cases}$$

the case $p = 3$ being verified explicitly by the example $f(x) = 1 + x + x^4$. Our next result yields the complement of (21) for $p = 2$. Indeed in light of (19) the next lemma implies that

$$(*) \text{ is impossible}, \qquad \text{for } p = 2.$$

Lemma 5.6. *Let $f \in \mathbb{Z}[x]$. Then $\{f(1), f(-1), |f(i)|^2\} \not\subseteq 2\mathbb{Z}_2^*$.*

Proof. Write f in the form $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots$, with only finitely many non-zero $a_j \in \mathbb{Z}$. Let

$$A = a_0 + a_2 + a_4 + \ldots \quad \text{and}$$
$$B = a_1 + a_3 + a_5 + \ldots$$

Case I: Suppose that $A \not\equiv B \pmod 2$. Then $f(1) = A + B$ is odd, hence $f(1) \notin 2\mathbb{Z}_2^*$.

Case II: Suppose that A, B are odd. Then

$$f(1)f(-1) = (A + B)(A - B) = A^2 - B^2$$

is the difference of two odd squares, and thus it divisible by 8. Hence, $8 \mid f(1)f(-1)$ and thus $\{f(1), f(-1)\} \not\subseteq 2\mathbb{Z}_2^*$.

Case III: Suppose that A, B are even. Let

$$\widehat{A} = a_0 - a_2 + a_4 - a_6 + - \ldots \quad \text{and}$$
$$\widehat{B} = a_1 - a_3 + a_5 - a_7 + - \ldots.$$

Then $\widehat{A} \equiv A \pmod 2$ is even, $\widehat{B} \equiv B \pmod 2$ is even, and therefore

$$|f(i)|^2 = |\widehat{A} + i\widehat{B}|^2 = \widehat{A}^2 + \widehat{B}^2$$

is divisible by 4. Hence, $4 \mid |f(i)|^2$ and thus $|f(i)|^2 \notin 2\mathbb{Z}_2^*$. □

We obtain the following result.

Lemma 5.7. *Let $f \in \mathbb{Z}[x]$. Then $f(1)\, f(-1)\, |f(i)|^2 \in \mathbb{Z}_2^* \cup 16\mathbb{Z}$.*

Proof. Let $d = f(1)\, f(-1)\, |f(i)|^2$ and note that by Lemma 5.4(i) with $p = 2$,

$$f(1) \equiv f(-1) \equiv |f(i)|^2 \mod 2.$$

Case I: Suppose that $f(1), f(-1), |f(i)|^2$ are odd. Then d is odd, that is, $d \in \mathbb{Z}_2^*$.

Case II: Suppose that $f(1), f(-1), |f(i)|^2$ are even. Then by Lemma 5.6 at least one of these three numbers is divisible by 4. Hence, we conclude that $16 \mid d$, that is, $d \in 16\mathbb{Z}$. □

By Lemma 3.2 and the fact that $\mathrm{Res}(x^4 - 1, f) = f(1)\, f(-1)\, |f(i)|^2$ from Lemma 5.1 we observe that Lemma 5.7 yields

$$\mathscr{D}(4) \subseteq \mathbb{Z}_2^* \cup 16\mathbb{Z}.$$

The next result is more general and it implies the new upper bound to be applied in the proof of Theorem 1.1 above.

Theorem 5.8. *We have $\mathscr{D}(2^k q) \subseteq \mathbb{Z}_2^* \cup 2^{k+2}\mathbb{Z}$, for $q \geq 1$ and $k \geq 2$.*

Proof. Since $\mathscr{D}(2^k q) \subseteq \mathscr{D}(2^k)$ by Lemma 3.6, we need to consider only $q = 1$.

Let $f \in \mathbb{Z}[x]$ and $d = \mathrm{Res}(x^{2^k} - 1, f)$. In view of Lemma 3.2 we prove the lemma by showing that $d \in \mathbb{Z}_2^* \cup 2^{k+2}\mathbb{Z}$, for $k \geq 2$.

Case I: Suppose that $f(1)$ is odd. Then Lemma 5.4(i) implies that d is factorized by Lemma 5.1 into the product of solely odd numbers. Hence d is odd, that is, $d \in \mathbb{Z}_2^*$.

Case II: Suppose that $f(1)$ is even. Then Lemma 5.4(i) implies that d is factorized by Lemma 5.1 into the product of $k+1$ many even numbers. By Lemma 5.7 the product of the first three of these even numbers is divisible by 16. Hence d is divisible by $16 \cdot 2^{k-2} = 2^{k+2}$, that is, $d \in 2^{k+2}\mathbb{Z}$. □

Acknowledgements

The author would like thank the referees for suggesting Remark 1.3 and other valuable comments.

References

[1] Cremona, J.E.: Unimodular integer circulants. Math. Comp. **77**, 1639–1652 (2008).
[2] Davis, P.J.: Circulant Matrices. John Wiley & Sons, New York (1979).
[3] Dilcher, K., Stolarsky, K.B.: Resultants and discriminants of Chebyshev and related polynomials. Trans. Amer. Math. Soc. **357**, 965–981 (2005).
[4] Gelfand, I.M., Kapranov, M.M., Zelevinsky, A.V.: Discriminants, Resultants, and Multidimensional Determinants. Birkhäuser, Boston (1994).
[5] Guerrier, W.J.: The factorization of the cyclotomic polynomials mod p. Amer. Math. Monthly **75**, 46 (1968).
[6] Hillar, C.J., Levine, L.: Polynomial recurrences and cyclic resultants. Proc. Amer. Math. Soc. **135**, 1607–1618 (2007).
[7] Kaiblinger, N.: On the Lehmer constant of finite cyclic groups. Acta Arith. **142**, 79–84 (2010).
[8] Krattenthaler, C.: Advanced determinant calculus. Sém. Lothar. Combin. **42**, Art. B 42 q, 67 pp. (1999).
[9] Krattenthaler, C.: Advanced determinant calculus: a complement. Linear Algebra Appl. **411**, 68–166 (2005).
[10] Laquer, H.T.: Values of circulants with integer entries. In: A Collection of Manuscripts Related to the Fibonacci Sequence, pp. 212–217. Fibonacci Assoc., Santa Clara (1980).

[11] Lehmer, D.H.: Some properties of circulants. J. Number Theory **5**, 43–54 (1973).
[12] Lind, D.: Lehmer's problem for compact abelian groups. Proc. Amer. Math. Soc. **133**, 1411–1416 (2005).
[13] Mahoney, M.K., Newman, M.: Determinants of abelian group matrices. Linear Multilinear Algebra **9**, 121–132 (1980).
[14] McKay, J.H., Wang, S.S.S.: A chain rule for the resultant of two polynomials. Arch. Math. **53**, 347–351 (1989).
[15] Newman, M.: On a problem suggested by Olga Taussky-Todd. Illinois J. Math. **24**, 156–158 (1980).
[16] Newman, M.: Determinants of circulants of prime power order. Linear Multilinear Algebra **9**, 187–191 (1980).
[17] Ore, O.: Some studies on cyclic determinants. Duke Math. J. **18**, 343–354 (1951).
[18] Pascal, E.: Die Determinanten (German edition by H. Leitzmann). Teubner, Leipzig (1900).
[19] Pierce, T.A.: The numerical factors of the arithmetic forms $\prod_{i=1}^{n}(1\pm\alpha_i^m)$. Ann. of Math. **18**, 53–64 (1916).
[20] Sburlati, G.: On prime factors of determinants of circulant matrices. Linear Algebra Appl. **432**, 100–106 (2010).

N. Kaiblinger, Faculty of Mathematics, University of Vienna, Nordbergstrasse 15, 1090 Vienna, Austria
E-mail address: norbert.kaiblinger@univie.ac.at