CIRCULANTS (Extract)

Alun Wyn-jones

Last revised in December 2013.

Chapter 10.
Formulæ for the Circulant Determinant.

In this chapter, various formulæ for the general circulant determinant in complex fields will be derived, and some immediate conclusions drawn where appropriate. There are many reasons for wanting to evaluate the circulant determinant, but probably the earliest was Kummer's proof that the class groups of the cyclotomic fields of prime order were finite.

For convenience, we restate the resultant formula for the circulant determinant.

1.11.3 **Theorem (The Resultant Formula).** Let $a \in \mathbf{circ}_N(R)$ where R is an integral domain and let $A(x) = \sum_{i=0}^{N-1} a_i x^i \in R[x]$ be the representer polynomial for a of degree d with roots $\alpha_1, \alpha_2, \ldots, \alpha_d$ if necessary in some extension of R. Then,

$$\Delta_N(a) \quad = \quad (-1)^{d(N-1)} a_d^N \prod_{i=1}^{d} (1 - \alpha_i^N) \qquad \square$$

The theorem is easily generalized to any polynomial $A(x) \in \left(\Gamma^N\right)^{-1}(a)$ where $d = \deg A$ and $\alpha_1, \alpha_2, \ldots, \alpha_d$ are the roots of $A(x)$. In fact, the only change required in the proof of the theorem is to use A_i throughout for the coefficients of the polynomial instead of the circulant vector components, a_i.

10.1.1 **Corollary** For a given $a = (a_0, a_1, \ldots, a_d) \in R^d \subset \mathbb{C}^d$ with $a_d \neq 0$, extend a with zeroes to a vector in R^N thus defining $\Delta_N = \Delta_N(a)$, for all $N \geq d$. Let $\mathscr{A}$ be the multiset of the roots of $A(x) = \sum_{i=0}^{d} a_i x^i$. Let S_1 be the unit circle in $\mathbb{C}$, and let $\breve{D}_1$ be the open unit disc.

(i) If $\mathscr{A} \cap S_1 = \emptyset$, then $|\Delta_N| \sim |a_d|^N \prod_{|\alpha|>1} |\alpha|^N$, as $N \to \infty$.

(ii) If $\mathscr{A} \cap \breve{D}_1 = \emptyset$, then $|\Delta_N| \sim |a_d a_0|^N$, as $N \to \infty$.

(iii) If $\mathscr{A} \subset \breve{D}_1$, then $|\Delta_N| \sim |a_d|^N$, as $N \to \infty$. $\square$

In the next proposition the base ring R is the field of residues modulo a prime q and is not a complex domain.

10.1.2 **Proposition** Let $A(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$ and extend a with zeroes to a_{N-1} if necessary as in the previous corollary. Let $q = rN + 1$ be prime in $\mathbb{Z}$. Then,

$$\Delta_N(a) \equiv 0 \;\Leftrightarrow\; \exists x \in \mathbb{Z} \text{ s.t. } A(x^r) \equiv 0 \pmod{q}$$

Proof. Take $R = \mathbb{F}_q$. R contains a primitive N^{th} root of unity, ζ, say, so $R_\zeta = R$. The set of N^{th} roots of unity is equal to the set of r^{th} powers of residues, so

RTP: In $\mathbb{F}_q$, $\Delta = 0$ iff $A(\zeta^i) = 0$ for some $i \in \{0, 1, \ldots, N-1\}$

$\Leftarrow$: If $A(\zeta^i) = 0$ in $\mathbb{F}_q$, then $\lambda_i(a) = 0$. QED ($\Rightarrow$)

$\Rightarrow$:

$$\begin{aligned} \Delta = 0 \;&\Rightarrow\; \prod_{A(\alpha)=0} (1 - \alpha^N) = 0 \\ &\Rightarrow\; \alpha^N = 1 \text{ for some root } \alpha \text{ of } A \\ &\Rightarrow\; \alpha = \zeta^i \text{ for some } i \\ &\Rightarrow\; \alpha = x^r \text{ for some } x \in \mathbb{F}_q^* \;\square \end{aligned}$$

10.1.3 **Proposition** Let $A(x) \in \mathbb{Z}[x]$ be monic. Given any element $r \in \mathbb{F}_p$, define $n(r)$ to be the highest power of p dividing $r^{p-1} - 1$ (with $n(1) = \infty$). Let $x_1, x_2, \ldots, x_f$ be the roots of A in $\mathbb{F}_p^*$, and define $e := \sum\{n(x_i) \vdash 0 \le i \le f\}$. Then,

$$p^e \mid \Delta_{p-1}\left(A(\mathrm{u}_{p-1})\right)$$

and e is highest such, and $e \ge f$. (Divisibility by p^∞ indicates Δ is zero.)

Proof. Let $E \supset \mathbb{F}_p$ be the root field of A, and let the roots lying in $E - \mathbb{F}_p$ be $x_{f+1}, x_{f+2}, \ldots, x_{f+g}$. (Thus, the zero root has multiplicity $\deg A - f - g$).

We have $n(r) \ge 1$ for every $r \in \{x_1, x_2, \ldots, x_f\}$ which proves $e \ge f$.

We shall apply the theorem to the root field of the polynomial A regarded as a polynomial in $\mathbb{F}_p[x]$.

$$\begin{aligned}\Delta_{p-1}(a) &= \pm \prod_{i=1}^{f}\left(x_i^{p-1} - 1\right) \prod_{i=1}^{g}\left(x_{f+i}^{p-1} - 1\right) \\ &= \pm \prod_{i=1}^{f} H(x_i) \prod_{i=1}^{g} H(x_{f+i}) \quad \text{where } H(x) := x^{p-1} - 1\end{aligned}$$

Since each $x_i \in \mathbb{F}_p^*$, and $\left|\mathbb{F}_p^*\right| = p - 1$, we have $x_i^{p-1} = 1$. Therefore, $H(x) = 0$ at $x = x_1, x_2, \ldots, x_f$ showing that p^f divides $\Delta_{p-1}(a)$.

Now, $(d/dx)H(x) = (p-1)x^{p-2} \neq 0$ for $x \in \mathbb{F}_p^*$. Hence $H(x)$ does not have repeated roots at these values. One would therefore expect that $p^2 \nmid H(x)$. But this mistakes a repeated root mod p for repeated divisibility by p. (See the discussion after the proposition for counterexamples.) A repeated root implies repeated divisibility, but the converse is false. Hence, in general, we must set $e = n(x_1) + n(x_2) + \cdots + n(x_f)$.

It remains to show that the other factors, $H(x_{f+i})$, are not divisible by p. But, we need only note that $H(x) = x^{p-1} - 1$ is a polynomial of degree $p - 1$ over the field E, and therefore has exactly $p - 1$ roots in E. These are all accounted for by $\mathbb{F}_p^*$. That is, there are no roots of $H(x)$ in $E - \mathbb{F}_p$. □

One wonders: How frequently is $r^{p-1} - 1$ divisible by p^2? Let us call such a residue a second degree residue of p. Heuristically, one would expect most primes to have at least one second degree residue because if $r^p \equiv r + bp \pmod{p^2}$, then $(r + bp)^p \equiv r + bp \pmod{p^2}$. This shows that there are p solutions to $x^p - x \equiv 0 \pmod{p^2}$, so one would expect roughly one solution to fall in the range 0 to $p - 1$.

In fact, as the table below demonstrates, few primes below 100 possess second degree residues.

Prime	2^{nd} Degree Residues
11	3, 9
29	14
37	18
43	19
59	53
71	11, 26
79	31
97	53

In the 182 odd primes to 1093, there are only 169 second degree residues, and only one of these is a third degree residue (at $p = 113$, $r = 68$). Curiously, the first prime for which 2 is a second degree residue is $p = 1093$ which also has the distinction of having all powers of 2 to 1024 as second degree residues. This particular fact is of importance to the traditional analysis of Fermat's Last Theorem. (See [HaW].)

The fact that we know the exact power of p dividing Δ_{p-1} allows us to deduce the existence of roots in a finite field. To take a simple example, let $A(x) = x^2 - 2$, $p = 17$. $\Delta_{16}(\mathrm{u}^2 - 2) = (2^8 - 1)^2 = 65025 = 3^2 \times 5^2 \times 17^2$. So, 2 must be a quadratic residue mod 17.

We now give a slight generalization of the proposition.

10.1.4 **Proposition** Let $A(x) \in \mathbb{Z}[x]$ be monic of degree d, let $N = n(p-1)$ with p prime. Suppose $A(x)$ has roots $x_1, x_2, \ldots, x_f$ in $\mathbb{F}_p^*$. Let $e = \sum\{n(x_i) \vdash 1 \leq i \leq f\}$ where $n(r)$ is the highest power of p dividing $r^N - 1$. Then, for all $n \geq 1$, $p^e \mid \Delta_N(A(\mathrm{u}_N))$.

If n is coprime to $p^{h-1} + p^{h-2} + \cdots + p^2 + p + 1$ for all $h \leq d!$, then e is the largest such.

Proof. As before, let E be the root field for $A(x)$. Following the same reasoning as in the proposition we still deduce $p^e \,|\, \Delta_N(A(\mathrm{u}))$. However, we can no longer deduce that e is the largest such because it is now possible for $H(x) = x^N - 1 = 0$ when $x = \alpha \notin \mathbb{F}_p$.

Assume $\alpha \in E - \mathbb{F}_p$ is such a root of H. Then, some power of α must be in the base field. Now, we already know that $\alpha^N = 1 \in \mathbb{F}_p$. Therefore, $t \,|\, N$. Now, $\alpha^{p-1} \neq 1$ since all the $p-1$ roots are accounted for in $\mathbb{F}_p$. Therefore, $\gcd(t, n) > 1$. Let $g = \gcd(t, n)$.

Let $\bar{\alpha}$ be the image of α under the natural map to $E^* \to E^*/\mathbb{F}_p^*$. Then, $\bar{\alpha}$ must satisfy $\bar{\alpha}^t = 1$. Now, the order of any element in a finite group must divide the order of the group. Therefore, $t \mid \left|E^*/\mathbb{F}_p^*\right|$. $\therefore g \mid \left|E^*/\mathbb{F}_p^*\right| = (q-1)/(p-1) = p^{h-1} + p^{h-2} + \cdots + p + 1$. The coprimality of n with respect to this latter expression makes $g \mid n$ impossible for $h \leq d!$. We now recall that the greatest possible dimension of the root field of a polynomial over the base field is $d!$ where d is the degree of the polynomial. But, $\dim E = [E : \mathbb{F}_p] = h$. Hence $h \leq d!$. □

10.1.5 **Wendt's circulant.**

An important application of the proposition is finding factors of "Wendt's circulant," W_N, which is defined as $W_N := \left|\Delta_N\left((\mathrm{u}-1)^N - 1\right)\right|$. (See §10.3 for a fuller discussion of Wendt's circulant.)

10.1.6 **Corollary** Suppose N is divisible by $p-1$ for some prime p. Then, $p^{p-2} \,|\, W_N$.

Proof. Let $A(x) = (x-1)^N - 1$. Then, $W_N = A(\mathrm{u})$.

It is easy to see that all residues in $\mathbb{F}_p$ are roots of A except for $x = 1$. Hence, the non-zero roots are $2, 3 \ldots, p-1$ giving $p-2$ non-zero roots in all. □

(See §10.3.5 for an improvement of this corollary.)

10.2 **Homogenous Diophantine Equations.**

The above proposition has application to certain homogenous diophantine equations. The next theorem places necessary conditions on a class of diophantine equations for them to have non-trivial solutions. One such diophantine equation is the famous equation of Fermat's Last Theorem which is discussed in more detail.

10.2.1 **Theorem**

Let $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ be a solution to the diophantine equation $a_1 x_1^r + a_2 x_2^r + \cdots + a_n x_n^r = 0$.

Suppose $q = 1 + rN$ is prime for some N. Given any map, $\beta : \{1, 2, \ldots, n\} \mapsto \mathbb{Z}_N$. Define $\beta a \in \mathbf{circ}_N(\mathbb{F}_q)$ by $(\beta a)_i = \sum\{a_j \vdash \beta(j) = i\} \bmod q$. If, for all such maps β, $\Delta_N(\beta a) \not\equiv 0 \pmod q$ then q divides $x_1 x_2 \cdots x_n$.

Proof. We have $\displaystyle\sum_{i \in \mathbb{Z}_N} a_i x_i^r \equiv 0 \pmod q$.

Suppose $x_i \not\equiv 0$ for all i. Let x_i also represent its residue modulo q. Then, each x_i^r is an N^{th} root of unity in $\mathbb{F}_q$, and we can replace x_i^r by $\zeta^{\beta(i)}$ where ζ is a primitive N^{th} root of unity in $\mathbb{F}_q$ and $\beta : \{1, 2, \ldots, n\} \mapsto \mathbb{Z}_N$. Let $b = \beta a$. Then the congruence becomes in $\mathbb{F}_q$,

$$\sum_{i \in \mathbb{Z}_N} b_i \zeta^i = 0$$

Multiplying this equation throughout by successively higher powers of ζ, we get the following system of equations in $\mathbb{F}_q$.

$$\begin{pmatrix} b_0 & b_1 & b_2 & \dots & b_{N-1} \\ b_{N-1} & b_0 & b_1 & \dots & b_{N-2} \\ b_{N-2} & b_{N-1} & b_0 & \dots & b_{N-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_1 & b_2 & b_3 & \dots & b_0 \end{pmatrix} \begin{pmatrix} 1 \\ \zeta \\ \zeta^2 \\ \vdots \\ \zeta^{N-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

For consistency, $\Delta_N(b) \equiv 0 \pmod{q}$. Since this contradicts the assumptions, the only possibility is that x_i^r is not a power of ζ for some i. But, ζ is a primitive residue for all non-zero r^{th} powers in $\mathbb{F}_q$; so, x_i must be divisible by q. □

Remark If the conditions of the theorem hold for an infinity of primes $q = 1 + rN$, then we can deduce $q \,|\, x_1 x_2 \cdots x_n$ for an infinity of primes and hence $x_1 x_2 \cdots x_n = 0$. Note also that by a well-known theorem of Dirichlet, that there always are an infinity of primes of the form $1 + rN$ with r fixed. (See for instance [Edw], [HaW]. Washington's book [Was] contains a particularly simple proof.)

10.2.2 **Fermat's Last Theorem** The most famous example of a diophantine equation of the type covered by the above theorem is the equation of Fermat's Last Theorem, $x^n + y^n = z^n$. It states that there are no non-zero solutions to this equation for $n > 2$. The only proof at the time of writing is extremely lengthy since it involves the highly developed theory of elliptic curves. (The ancient Greeks proved that there are an infinity of solutions when $n = 2$. See §8.1.3.) The theorem is often referred to as the "FLT Conjecture" in earlier works, and "FLT" in works after the appearance of the proof by Andrew Wiles. It is easily shown that the theorem is true if and only if it is true for $n = 4$ and all primes $n > 2$, that is for all odd prime exponents.

It is quite easy to prove the theorem for $n = 4$. Therefore, one can assume that the equation is $x^p + y^p = z^p$ where p is an odd prime. Since p is odd, the sign of z can be reversed and the equation written in the more symmetric form $x^p + y^p + z^p = 0$. The theorem naturally falls into two cases traditionally called the First and Second Cases. In the First Case it is assumed that none of the variables x, y, z are divisible by p whereas in the Second Case it is assumed that $p \,|\, xyz$.

If in the statement of Theorem 10.2.1 we set $n = 3$, $r = p$, and $a_1 = a_2 = a_3 = 1$, we get the FLT equation. On the face of it, Theorem 10.2.1 appears insensitive to the conditions of the two traditional FLT cases. It matters not whether $p \,|\, xyz$ since the modulus of importance is not p but the prime $q = Np + 1$. This is so. In fact, the conditions $\Delta(\beta a) \not\equiv 0$ in the theorem naturally fall into the following cases:

$$\left.\begin{array}{ll} (i) & \Delta_N(3, 0, \dots, 0) \not\equiv 0 \\ (ii) & \Delta_N(2, 0, \dots, 0, 1, 0, \dots, 0) \not\equiv 0 \\ (iii) & \Delta_N(1, 0, \dots, 0, 1, 0, \dots, 0, 1, 0, \dots, 0) \not\equiv 0 \end{array}\right\} \pmod{q} \qquad (1)$$

where the 1 in *(ii)* occurs in any position $i \neq 0$, and the latter two 1's in *(iii)* are in any positions $0 < i < j$.

Case *(i)* holds trivially. Theorem 10.1 gives the following value for the determinant in case *(ii)*

$$|\Delta_N| = (2^n - (-1)^n)^d \quad \text{where } d = \gcd(N, i) \text{ and } n = N/d$$

Little is known about the determinant in case *(iii)*. Since the determinant has only three non-zero entries per row, all equal to 1, it is natural to try to evaluate the determinant in this case by direct expansion. Although a general formula for the terms in the determinant expansion is known (see Chapter 11), it has not as yet provided much insight into the residue class of the determinant modulo a prime q. Some insight into the terms appearing in such an expansion came from an article in 2004 by Loehr, Warrington, & Wilf ([LWW]). Whose results which are germane to the FLT question are summarized in the next proposition.

10.2.2.3 **Proposition** Let $c(r, s)$ be the coefficient of $x^r y^s$ in the expansion of $\Delta_N(1 + x\mathrm{u} + y\mathrm{u}^j)$. Then,

(i) $c(r, s) \neq 0$ iff $N \,|\, r + sj$.

(ii) $c(r,s)$ is positive or negative according as $\gcd\left(r, s, (r+sj)/N\right)$ is respectively even or odd. □ ([LWW])

As the authors point out, the above proposition can be easily extended to the expansion of $\Delta_N(1 + x\mathrm{u}^i + y\mathrm{u}^j)$ for any i coprime to N by applying the ν_i map to the circulant $1 + x\mathrm{u} + y\mathrm{u}^j$. It can also be extended to cases where i is not coprime provided j is coprime by applying the ν_j^{-1} map.

In conditions (1), we have simplest possible application of the proposition: $x = y = 1$. Evaluating the determinant is reduced to adding and substracting coefficients according to the odd-even rule given in the proposition. Unfortunately, we still lack a good understanding of the magnitudes of the coefficients. Loehr et al. proved only that coefficients grow exponentially with N.

Should conditions (1) be proved for some p and for an infinity of primes $q = Np + 1$, then FLT would be a consequence for the exponent p since any solution x, y, z would have to satisfy $q \,|\, xyz$ for an infinity of primes which is impossible unless $xyz = 0$. Needless to say this has not been proved.

We obtain some partial results in §10.6 by setting bounds on the circulant determinant which imply $q \,|\, xyz$ for several primes q and for various exponent primes p.

Although the two traditional cases of FLT are not salient in the above approach, there is a theorem of Sophie Germain which makes Theorem 10.2.1 directly relevant to the First Case of FLT. We omit the proof as the theorem is not directly relevant to theory of circulants. The proof and more on FLT including the development of cyclotomic theory in the 19^{th} century can be found in Edwards book [Edw]. Also, see Ribenboim's book [Rib1] for a general exposition of "elementary" approaches to FLT.

10.2.3 **The Theorem of Sophie Germain.** Let $p > 2$ be prime. If there is an auxiliary prime q with the properties that

(i) $x_1^p + x_2^p + x_3^p \equiv 0 \pmod{q}$ implies that $x_1 x_2 x_3 \equiv 0 \pmod{q}$, and

(ii) $x^p \equiv p \pmod{q}$ is impossible

then the First Case of FLT is true for p.

Proof. See [Edw]. □

When the auxiliary prime q is of the form $Np + 1$, condition *(ii)* of the Sophie Germain Theorem can be stated more powerfully.

10.2.4 **Proposition** $q = Np + 1$ satisfies condition *(ii)* of the Sophie Germain Theorem if and only if

$$N^N \not\equiv 1 \pmod{q}$$

Proof. We shall represent the statement of condition *(ii)* by C_2 and its negation by $\sim C_2$. Thus, $\sim C_2$ means that there is a solution to $x^p \equiv p \pmod{q}$. Throughout this proof all congruences are modulo q.

$$\begin{aligned} \sim C_2 \quad &\Rightarrow \quad p \equiv x^p \pmod{q} \quad \text{for some } x \\ &\Rightarrow \quad p^N \equiv x^{Np} = x^{q-1} \equiv \begin{cases} 0 & \text{if } q \,|\, x \\ 1 & \text{otherwise} \end{cases} \end{aligned}$$

But, $q \,|\, x$ is impossible if $p \equiv x^p$ since p and q are distinct primes so $p \not\equiv 0 \pmod{q}$.

$$\therefore \sim C_2 \quad \Rightarrow \quad p^N \equiv 1$$

Now suppose that $p^N \equiv 1$, then $p = \zeta_N^a$ for some a where ζ_N is a primitive N^{th} root of unity in $\mathbb{F}_q$. But, $\zeta_N = \zeta^p$ for some primitive $(q-1)^{\text{th}}$ root of unity, ζ. $\therefore p \equiv (\zeta^a)^p$ and this is a solution to the congruence $x^p \equiv p$. Therefore, $p^N \equiv 1 \;\Rightarrow \sim C_2$

$$\begin{aligned}\therefore \sim C_2 &\Leftrightarrow p^N \equiv 1\\ &\Leftrightarrow \left(\frac{q-1}{N}\right)^N \equiv 1\\ &\Leftrightarrow (q-1)^N \equiv N^N\\ &\Leftrightarrow (-1)^N \equiv N^N\\ &\Leftrightarrow 1 \equiv N^N \text{ since } N \text{ is even}\end{aligned}$$

In the last step, N is said to be even. This must be so since p is odd, so $q = Np+1$ can be odd only if N is even. □

Using estimates for the maximum value of the the three-term determinant of §10.2.2, and using these to limit the maximum factor dividing the determinant, it is possible to deduce the first case of FLT for many primes. However, the standard, and more successful approach using a circulant determinant, is that based on Wendt's Theorem which we now turn to.

10.3 **Definition** Define **Wendt's Circulant of order** n as

$$W_n \;:=\; \mathbf{circ}\left(1,\ \binom{n}{1},\ \binom{n}{2},\ \ldots,\ \binom{n}{n-1}\right) \quad = \quad (\mathrm{u}+1)^n - 1$$

10.3.1 **Wendt's Theorem** Let $p > 2$ be prime and assume that $q = Np+1$ is also prime. Then there exist integers x, y, z, not multiples of q, such that $x^p + y^p + z^p \equiv 0 \pmod{q}$ iff $q \,|\, \det(W_N)$.

Proof. [Rib1]. As in Theorem 10.2.1, we replace each of x^p, y^p, z^p by powers of a primitive N^{th} root of unity in $\mathbb{F}_q$ giving us the equation $1 + \zeta^i = \zeta^j$ in $\mathbb{F}_q$ for some $i, j, 0 \le i, j < N$. Setting $\xi = \zeta^i$ we see that this is equivalent to the equation $(1+\xi)^N = 1$ in $\mathbb{F}_q$. Expanding,

$$1 + \binom{N}{1}\xi + \binom{N}{2}\xi^2 + \cdots + \binom{N}{N-1}\xi^{N-1} \;=\; 0$$

Proceeding as in Theorem 10.2.1, we multiply this equation throughout by successively higher powers of ξ obtaining a system of simultaneous equations over $\mathbb{F}_q$ equivalent to $W_N\boldsymbol{\xi} = 0$ where $\boldsymbol{\xi}$ is the vector of powers of ξ. Hence, W_N is singular in $\mathbb{F}_q$. □

Note that Wendt's criterion does not require consideration of cases depending on the residues of $x, y, z \pmod{q}$, and this is its great advantage over the three-term determinant of §10.2.2.

Much work has been done on divisibility properties of Wendt's determinant. Some of this is summarised in the next theorem.

10.3.2 **Theorem** Let $\Delta_n = \det W_n$.

(i) $\Delta_n = 0 \;\Leftrightarrow\; 6 \,|\, n$.

(ii) $d \,|\, n \;\Rightarrow\; \Delta_d \,|\, \Delta_n$. (E.Lehmer)

(iii) if $p > 2$ is prime then $p^{p-2}\left(\dfrac{2^{p-1}-1}{p}\right) \;\Big|\; \Delta_{p-1}$.

(iv) If $n \equiv 2$ or $4 \pmod{6}$, then $\Delta_n \;=\; -3\left(\dfrac{2^n-1}{3}\right)^3 w^6$ for some integer w. (J.S.Frame).

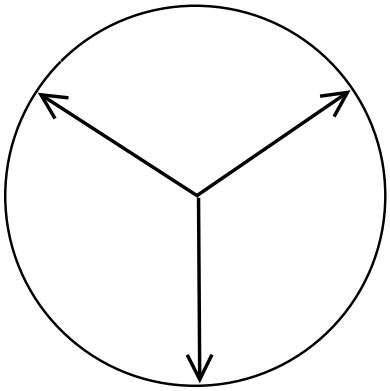
(v) If $2n+1 = p$ is prime then $p^{\lfloor (n-1)/2 \rfloor} \mid \Delta_n$. (J.S.Frame)

Proof. The proofs of these statements appear in Propositions 10.3.3 through 10.3.6 below. Most of the proofs are adapted from [Rib1] where more details concerning Wendt's determinant can be found. □

Throughout the remaining propositions of this section, $\zeta = \zeta_n$, and $\Delta_n = \det W_n$.

10.3.3 **Proposition** $\Delta_n = 0 \Leftrightarrow 6 \,|\, n$.

Proof. We are given $\Delta\left((1+\mathrm{u})^n - 1\right) = 0$. So, $\exists i$, $(1+\zeta^i)^n = 1$ and so $1+\zeta^i = \zeta^j$ for some j. The diagram below depicts the three terms as vectors in the complex plane. If we think of these vectors as unit forces in balance it is clear that ζ^i and $-\zeta^j$ must be third roots of unity. This is possible only if $6 \,|\, n$. □



Three Unit Forces in Balance

10.3.4 **Proposition** $d \,|\, n \;\Rightarrow\; \Delta_d \,|\, \Delta_n$.

Proof. We have

$$\frac{W_n}{W_d} \;=\; \prod_{i\in\mathbb{Z}_d} \frac{(1+\zeta_d^i)^n - 1}{(1+\zeta_d^i)^d - 1} \;\prod\{(1+\zeta_n^i)^n - 1 \vdash\; i \in \mathbb{Z}_n,\; n/d \nmid i\}$$

The second product ranges over a union of residue classes mod n, and so is a rational; it is also manifestly a cyclotomic integer, and therefore is a rational integer.

The typical term under the first product expands into the geometric series $\sum_{j=0}^{n/d-1}(1+\zeta_d^i)^{dj}$ which is also manifestly an algebraic integer; the product is over all d^{th} roots of unity and so is rational. □

10.3.5 **Proposition** If $p > 2$ is prime then $p^{p-3}\left(2^{p-1}-1\right) \,|\, \Delta_{p-1}$.

Proof. We already know from Corollary 10.1.6 that $p^{p-2} \,|\, \Delta_{p-1}$.

By definition, $W_{p-1} := (1+\mathrm{u})^{p-1} - 1$. $\therefore \lambda_0(W_{p-1}) = 2^{p-1} - 1$. Since a determinant of an integer circulant is always divisible by λ_0, it follows that $2^{p-1} - 1 \,|\, \Delta_{p-1}$.

Now $p \,|\, 2^{p-1} - 1$, and so p must be removed from $2^{p-1} - 1$ since Proposition 10.1.6 guarantees only that $p^{p-2} \,|\, \Delta$ in all cases. Suppose generally that $p^t \,|\, 2^{p-1} - 1$ then, in the notation of Proposition 10.1.3, $n(2) = t$, and therefore, $p^{p-3+t} \,|\, \Delta$, but we would need to remove a factor of p^t from $2^{p-1} - 1$. Hence, Δ_{p-1} is divisible by

$$p^{p-3+t}\left(\frac{2^{p-1}-1}{p^t}\right) \;=\; p^{p-3}\left(2^{p-1}-1\right) \;\square$$

10.3.6 **Proposition** If $n \equiv 2$ or $4 \pmod 6$, then $\Delta_n \;=\; -3\left(\dfrac{2^n-1}{3}\right)^3 w^6$ for some integer w.

Proof. We term this the "hat trick" proof because three "rabbits" (actually integers) are pulled out of a "hat" (actually a product) leaving an integer still in the hat. The real trick comes at the end when it is revealed that the integer left in the hat is a perfect sixth power.

We let $\rho = \zeta^3$. Since $3 \nmid n$, ρ is a primitive n^{th} root of unity. Hence, $W_n = \prod_{i\in\mathbb{Z}_n}\left((1+\rho^i)^n - 1\right)$. Later in the proof it will be convenient to replace ρ by ζ^3.

Consider the double product $P_n = \prod_{j,k\in\mathbb{Z}_n}(1+\rho^{j+n/2}+\rho^{k+n/2})$.

$$\begin{aligned} P_n &= \prod_{j\in\mathbb{Z}_n}\prod_{k\in\mathbb{Z}_n}(1-\rho^j-\rho^k) \\ &= \prod_{j\in\mathbb{Z}_n}\left((1-\rho^j)^n-1\right) \quad \text{since } \prod_{k\in\mathbb{Z}_n}(x-\zeta^k)=x^n-1 \\ &= W_n \quad \text{since } \{-\rho \vdash \rho^n=1\}=\{\rho\vdash\rho^n=1\} \text{ for } n \text{ even.} \end{aligned}$$

We pull out the following integers from P_n:

(a) All terms with $j=\frac{1}{2}n$ yielding $\pi_a=\prod_{k\in\mathbb{Z}_n}(2-\rho^k) \;=\; 2^n-1.$

(b) All terms with $k=\frac{1}{2}n$ yielding $\pi_b=\prod_{j\in\mathbb{Z}_n}(2-\rho^j) \;=\; 2^n-1.$

(c) All terms with $j=k$ yielding $\pi_c=\prod_{j\in\mathbb{Z}_n}(1-2\rho^j) \;=\; 1-2^n.$

The ranges of the products π_a,π_b,π_c intersect as follows:

$$\mathrm{Ran}(\pi_a)\cap\mathrm{Ran}(\pi_b)=\mathrm{Ran}(\pi_b)\cap\mathrm{Ran}(\pi_c)=\mathrm{Ran}(\pi_c)\cap\mathrm{Ran}(\pi_a) \;=\; 1-\zeta^{n/2}-\zeta^{n/2} \;=\; 3$$

$$\therefore\ \mathrm{Ran}(\pi_a)\cap\mathrm{Ran}(\pi_b)\cap\mathrm{Ran}(\pi_c) \;=\; 3$$

By the intersection-complement principle, we must divide $\pi_a\pi_b\pi_c$ by $3^3\,3^{-1}=9$ to eliminate duplications.

$$\therefore\ P_n \;=\; -\frac{1}{9}(2^n-1)^3H$$

The remaining terms are gathered in H where

$$H \;=\; \prod_{(j,k)\in D}\left(1+\rho^{j+n/2}+\rho^{k+n/2}\right) \quad \text{and } D \;:=\; \{(j,k)\in\mathbb{Z}_n^2 \vdash\ j\neq\tfrac{1}{2}n,\ k\neq\tfrac{1}{2}n,\ j\neq k\} \tag{2}$$

To finish statement *(iii)*, it remains to prove that H is a perfect 6^{th} power.

The geometric mean of the three terms appearing under the product in H is $\rho^{(j+k)/3}=\zeta^{j+k}$. (This is why we started with ρ rather than ζ.) We move this term out of the main product obtaining

$$H \;=\; \prod_{j,k\in D}\zeta^{j+k}\prod_{j,k\in D}\left(\zeta^{-j-k}+\zeta^{2j-k+n/2}+\zeta^{2k-j+n/2}\right)$$

The first product in H evaluates to ζ^s where

$$\begin{aligned} s &= \sum_{(j,k)\in D}(j+k) \\ &= \sum_{(j,k)\in\mathbb{Z}_n^2}(j+k) \;-\; \sum_{\substack{(j,k)\in\mathbb{Z}_n^2\\ j=n}}(j+k) \;-\; \sum_{\substack{(j,k)\in\mathbb{Z}_n^2\\ k=n}}(j+k) \;-\; \sum_{\substack{(j,k)\in\mathbb{Z}_n^2\\ j=k}}(j+k) \;+\; 2\sum_{\substack{(j,k)\in\mathbb{Z}_n^2\\ j=k=n}}(j+k) \\ &\quad \text{(The coefficient of 2 on the last sum comes from 3 double intersections } - \text{ 1 triple intersection.)} \\ &\equiv 0 \pmod{n} \end{aligned}$$

Therefore, the first product is 1, and the second is

$$H \;=\; \prod_{(e,f,g)\in E}\left(\zeta^e+\zeta^f+\zeta^g\right) \tag{3}$$

where $E \subset \mathbb{Z}_n^3$ consists of distinct triples summing to $0 \pmod{n}$. This follows by the identifications below.

$$\left.\begin{array}{rcl} e &=& -j-k \\ f &=& 2j-k+\frac{1}{2}n \\ g &=& 2k-j+\frac{1}{2}n \end{array}\right\} \text{ in } \mathbb{Z}_n$$

together with the conditions $j \neq \frac{1}{2}n$, $k \neq \frac{1}{2}n$, $j \neq k$, and $3 \nmid n$. For example, $e = f \Leftrightarrow 3j+\frac{1}{2}n = 0 \Leftrightarrow 3 \mid n$.

Define $t(e,f,g) := \zeta^e + \zeta^f + \zeta^g$, the typical term in the product of formula (3). We can separate the product into six factors, $H_1, H_2, \ldots, H_6$ defined by

$$H_1 = \prod_{e<f<g} t(e,f,g), \quad H_2 = \prod_{g<e<f} t(e,f,g), \quad H_3 = \prod_{f<g<e} t(e,f,g),$$
$$H_4 = \prod_{f<e<g} t(e,f,g), \quad H_5 = \prod_{e<g<f} t(e,f,g), \quad H_6 = \prod_{g<f<e} t(e,f,g).$$

where the range of the variables e, f, g is $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ with constraints as indicated.

All these factors have the same value since $t(e,f,g)$ is invariant under all permutations of (e,f,g),

$$\therefore \; H \;=\; H_1 H_2 \cdots H_6 \;=\; H_1^6$$

(This implies that $H_1 \in \mathbb{Z}(\zeta_n) \cap \mathbb{R}(\zeta_6)$ with $3 \nmid n$, but is not quite enough to clinch the proof.) Consider the effect of a field automorphism, $\zeta \mapsto \zeta^h$ on H_1. Its effect on a typical term is $t(e,f,g) \mapsto t(eh, fh, gh)$ which is also in H_1 (with (eh, fh, gh) possibly in a different order). Hence, H_1 is rational, is manifestly a cyclotomic integer, and is therefore a rational integer. □

In 1991 Fee and Granville [FG] succeeded in using the Wendt determinant to prove FLT for all primes $p = nq + 1$ where $n \leq 200$ and $6 \nmid n$, a remarkable achievement.

10.4 Formulæ for the Determinantal Coefficients.

The general circulant determinant is

$$\Delta_N(a_0, a_1, \ldots, a_{N-1}) \quad = \quad \begin{vmatrix} a_0 & a_1 & a_2 & \cdots & a_{N-1} \\ a_{N-1} & a_0 & a_1 & \cdots & a_{N-2} \\ a_{N-2} & a_{N-1} & a_0 & \cdots & a_{N-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \cdots & a_0 \end{vmatrix}$$

This determinant can obviously be expanded in terms of the entries $a_0, a_1, \ldots, a_{N-1}$ into a sum of monomials thus,

$$\Delta_N(a_0, a_1, \ldots, a_{N-1}) \;=\; \sum_{v_0 \leq v_1 \leq \cdots \leq v_{N-1}} c(v_0, v_1, \ldots, v_{N-1})\, a_{v_0} a_{v_1} a_{v_2} \cdots a_{v_{N-1}} \; .$$

The constraint on the summation ensures that only algebraically distinct terms appear in the summation. The constants or coefficients, $c(v)$, which appear in the summation are called the **circulant determinantal coefficients**. These are functions of the numbers $v_0, v_1, \ldots, v_{N-1}$ which are the subscripts appearing in the monomial $a_{v_0} a_{v_1} a_{v_2} \cdots a_{v_{N-1}}$. By construction, $c(v)$ is a fully symmetric function in its arguments $v_0, v_1, \ldots, v_{N-1}$.

Consider Theorem 10.2.1 when applied to the FLT Conjecture. The circulant vector has only three non-zero components, and all three equal 1. It would appear that the best approach to evaluating the circulant determinant would be to find a formula for the determinantal coefficients as functions of the subscripts $v_0, v_1, \ldots, v_{N-1}$. Even if the general formula was rather complex, it would be reasonable to hope that in special cases such as the FLT conjecture, that the formula would simplify enough to allow an estimate of the determinant. Another instance where a formula would be useful would be the problem of finding the units of the ring $\mathbf{circ}_N(\mathbb{Z})$. In this section, two intermediate expressions are found for the determinantal coefficient which are later used in Chapter 11 to derive an explicit formula.

10.4.1 **Phase Formula** The derivation of the first formula starts with product of the eigenvalues.

$$\Delta_N(a) \;=\; (a_0 + a_1 + \ldots + a_{N-1})(a_0 + a_1\zeta + \ldots)\cdots(a_0 + a_1\zeta^j + a_2\zeta^{2j} + \ldots)\cdots(a_0 + a_1\zeta^{N-1} + \ldots) \quad (4)$$

where ζ is a primitive N^{th} root of unity.

Since we shall be writing formulæ containing fairly complex exponents of ζ, we shall be using $e_N(x)$ (or just $e(x)$, if N is understood) to stand for ζ^x.

Pick a sequence of a_i's, one from each factor of equation (4). Suppose the sequence is $a_{v_0}a_{v_1}\cdots a_{v_{N-1}}$. The coefficient of this particular monomial is

$$\zeta^{0\cdot v_0 + 1\cdot v_1 + 2\cdot v_2 + \cdots + (N-1)\cdot v_{N-1}} \quad = \quad e\Big(\sum_{r\in\mathbb{Z}_N} r v_r\Big)$$

Therefore, $\Delta(a)$ is the sum of all monomials, $a_{v_0}a_{v_1}\cdots a_{v_{N-1}}e\Big(\sum_{r\in\mathbb{Z}_N} r v_r\Big)$ over all sequences of subscripts $(v_0, v_1, \ldots, v_{N-1}) \in \mathbb{Z}_N^N$.

If $(t_0, t_1, \ldots, t_{N-1})$ is a rearrangement of $(v_0, v_1, \ldots, v_{N-1})$ then $a_{t_0}a_{t_1}\cdots a_{t_{N-1}}$ is algebraically the same as $a_{v_0}a_{v_1}\cdots a_{v_{N-1}}$. We wish to collect all such algebraically equal terms into a single term. A sequence of subscripts is therefore naturally a **multiset** since order is immaterial, and multiplicities count.

To distinguish a multiset from a particular sequence defining it, $v = (v_0, v_1, \ldots, v_{N-1})$, say, we shall use the notation $[v]$ for the multiset. Clearly, two multisets are equal iff they have the same elements with the same multiplicities.

To avoid repeated double-subscripts, we shall abbreviate the sequence a_{v_0}, a_{v_1}, …, $a_{v_{N-1}}$ to a_v, and we shall represent the monomial $a_{v_0}a_{v_1}\cdots a_{v_{N-1}}$ by Πa_v. With this new notation, the formula now becomes,

$$\Delta_N(a) \;=\; \sum_{\{[v]\,\vdash\, v\in\mathbb{Z}_N^N\}} \Pi a_v \sum_{\rho} e_N\Big(\sum_{r\in\mathbb{Z}_N} r\rho(v)_r\Big) \quad (5)$$

The ρ summation is over all rearrangements of the sequence v; $\rho(v)$ denotes the rearranged sequence, and $\rho(v)_r$ is the r^{th} component in the rearranged sequence.

Since $[v]$ can have repeated entries, for instance, $v = (0, 0, 0, 1, 1, 4)$, it is not immediately apparent what the set of rearrangements is. Suppose $\rho = (012)$ in cycle notation. Then ρ has no effect on v, merely permuting zeroes in the first three entries. Clearly, all rearrangements of v can be represented by a permutation of the subscripts of v (itself a sequence of subscripts). So, if ρ is any permutation, $\rho : \mathbb{Z}_N \to \mathbb{Z}_N$, then ρ acts on v by:

$$\rho \times v \mapsto (v_{\rho(0)}, v_{\rho(1)}, \ldots, v_{\rho(N-1)})$$

which following the previously introduced convention can be written

$$\rho \times v \mapsto v_\rho$$

Let S_N denote the symmetric group on $\mathbb{Z}_N$. The set of distinct permutations on v corresponds to the set of cosets of the stabilizer subgroup of S_N acting on v through its subscripts. Denote this stabilizer subgroup by $\text{Stab}(v)$ and denote its cardinality by $F(v) := |\text{Stab}(v)|$. Since elements of $\text{Stab}(v)$ leave $e(\sum_r r v_r)$ invariant, it follows that every action of $\rho \in S_N$ on v is one of $F(v)$ permutations which have the same action. Therefore, equation (5) becomes

$$\Delta_N(a) \;=\; \sum_{\{[v]\,\vdash\, v\in\mathbb{Z}_N^N\}} \Pi a_v \frac{1}{F(v)} \sum_{\rho\in S_N} e_N\Big(\sum_{r\in\mathbb{Z}_N} r v_{\rho(r)}\Big)$$

The coefficient of the Πa_v term is therefore,

$$c(v) \;=\; \frac{1}{F(v)} \sum_{\rho \in S_N} e_N\Big(\sum_{r \in \mathbb{Z}_N} \rho(r) v_r \Big) \tag{6}$$

The exponent (argument of $e_N(\cdot)$) has been changed to a more readable form. The change has no effect as ρ is summed over the entire S_N group. The above notation will occur repeatedly in what follows so we provide formal definitions.

10.4.2 **Definition**

(i) Denote by $\mathrm{Stab}(v)$ the group of permutations on the components v which leave v unchanged.

(ii) Define $F(v) := |\mathrm{Stab}(v)|$.

There is a fundamental fact about the determinantal coefficients which can now be proved.

10.4.3 **Proposition** If $c(v) \neq 0$ then $\sum_{r \in \mathbb{Z}_N} v_r \equiv 0 \pmod N$.

Proof. Let $\imath$ be the permutation of $\mathbb{Z}_N$ which increments each residue mod N. That is, $\imath(x) = 1+x \bmod N$. Summing over ρ is the same as summing over $\imath\rho$. Therefore,

$$\begin{aligned} c(v) &= \frac{1}{|F(v)|} \sum_{\rho \in S_N} e\Big(\sum_{r \in \mathbb{Z}_N} \imath\rho(r) v_r \Big) \\ &= \frac{1}{|F(v)|} \sum_{\rho \in S_N} e\Big(\sum_{r \in \mathbb{Z}_N} (1+\rho(r)) v_r \Big) \\ &= e\Big(\sum_{r \in \mathbb{Z}_N} v_r \Big) c(v) \end{aligned}$$

This is possible iff $c(v) = 0$ or $\sum_r v_r \equiv 0 \pmod N$. □

The property of a set of subscripts summing to zero modulo N is a key fact used in the derivation of a formula for the coefficients in Chapter 11.

10.4.4 **Parity Formula** We shall now present a third formula for $\Delta_N(a)$. This one is derived directly from the determinant and is therefore valid over any commutative ring. The formula for expanding the general $N \times N$ determinant $|c_{i,j}|$ by rows and columns is

$$\Delta \;=\; \sum_{\tau \in S_N} (-1)^\tau \prod_{i \in \mathbb{Z}_N} c_{i,\tau(i)}$$

where $\mathbb{Z}_N$ is taken as the index set for both rows and columns, and $(-1)^\tau$ denotes the parity of the permutation $\tau \in S_N$. Substituting values for a circulant determinant, $|a_{j-i}|$, we get

$$\Delta_N(a) \;=\; \sum_{\tau \in S_N} (-1)^\tau \prod_{i \in \mathbb{Z}_N} a_{\tau(i)-i}$$

As before, we rearrange this into algebraic monomials,

$$\Delta_N(a) \;=\; \sum_{[v]} \Pi a_v \sum_{\{\tau \in S_N \vdash [\tau] \equiv [v]\}} (-1)^\tau$$

where $[\tau] := [\tau(0){-}0,\ \tau(1){-}1,\ \tau(2){-}2,\ \ldots,\ \tau(N{-}1) - (N{-}1)]$ is the multiset of translations, and the equivalence $[\tau] \equiv [v]$ is modulo N. The above immediately gives the parity formula for the determinantal coefficient.

$$c(v) \;=\; \sum_{\{\tau\in S_N \vdash [\tau]\equiv[v]\}} (-1)^{\tau} \tag{7}$$

Formula (7) provides a reasonably efficient method for calculating all the circulant determinantal coefficients on a computer. However,formula (7) is not practical for calculating individual coefficients as it requires testing $N!$ permutations for each calculation. For single coefficients a recursive algorithm in section 11.2.3 is the simplest for computer calculations, and the coefficient formula of Chapter 11 is amenable to hand reckoning.

10.5.3 **Proposition** If $c(v) \neq 0$ then $[v]$ is the multiset of translations of some permutation of $\mathbb{Z}_N$.

Proof. This is a corollary of the Parity Formula of §10.4.4. □

10.5.4 **When is $c(v)$ non-zero?** We have already shown that if $c(v)$ is non-zero then v is a null multiset. The question is whether the converse is true. It will be shown in Chapter 11 that the converse does hold when N is prime. Even when N is compound Loehr, Warrington, and Wilf ([LWW]), have shown that it holds when

(i) there are only three distinct elements in v,

(ii) v can be transformed by the increment and multiplier maps to a multiset of zeroes, ones, and one other residue.

However, the converse does not always hold as the following examples demonstrate.

Examples

(i) $N = 6,\ v = [0,0,1,3,3,5],\ c(v) = 0$. Note that v is generated by permutations, namely, $\tau = (01)(25)$, and $\tau = (0143)$ in cycle notation.

(ii) $N = 10,\ v = [0,0,0,0,1,1,1,3,6,8],\ c(v) = 0$. Again, v is generated by $\tau = (012)(347)$ and $\tau = (012397)$.

The next proposition could have been proved immediately after Proposition 10.4.3, but with the parity formula in hand, the proof of its first part is slightly easier. Recall that the reverse position multiplier map is the map $\bar{\nu}_h : (a_0, a_1, \ldots, a_{N-1}) \mapsto (a_0, a_h, a_{2h}, \ldots, a_{h(N-1)})$. The effect of $\bar{\nu}_h$ on the monomial Πa_v is to map it to Πa_{hv} where $hv = h(v_0, v_1, \ldots, v_{N-1}) = (hv_0, hv_1, \ldots, hv_{N-1})$. Likewise, the effect of the rotation map σ on Πa_v is to map it to $\Pi a_{\imath v}$ where $\imath$ is the increment map.

10.5.5 **Proposition** Let $\imath$ be the increment map, and let $h \in \mathbb{Z}_N^*$.

(i) $c(\imath v) = (-1)^{N+1} c(v)$

(ii) $c(hv) = c(v)$

Proof.

(i) For the first part, we shall use the parity formula (7). First note that $\langle \imath\tau \rangle_i = \imath\tau(i) - i = \tau(i) + 1 - i$. Secondly, $(\imath \langle \tau \rangle)_i = \imath(\tau(i) - i) = \tau(i) - i + 1 = \langle \imath\tau \rangle_i$. Hence, $[\tau]$ generates $[v]$ iff $[\imath\tau]$ generates $[\imath v]$.

$$c(\imath v) = \sum_{[\tau]=[\imath v]} (-1)^{\tau} = \sum_{[\imath\tau]=[\imath v]} (-1)^{\imath\tau} = (-1)^{\imath} \sum_{[\imath\tau]=[\imath v]} (-1)^{\tau} = (-1)^{\imath} \sum_{[\tau]=[v]} (-1)^{\tau} = (-1)^{\imath} c(v)$$

The parity of the N-cycle $\imath$ is $(-1)^{N+1}$. QED *(i)*

From equation (6),

$$c(hv) \;=\; \frac{1}{F(v)} \sum_{\rho\in S_N} e_N\Big(\sum_{r\in\mathbb{Z}_N} h\rho(r) v_r \Big)$$

Since h is coprime to N, multiplication by h is a permutation of $\mathbb{Z}_N$. Therefore $h\rho$ ranges over all of S_N. Now change the summation variable from ρ to $h\rho$ giving formula (6) for $c(v)$. □

The next proposition is useful for finding divisibility properties of the coefficients.

10.5.6 **Proposition** Let $[v] = [\tau]$. Then $[v]$ is also generated by every permutation in the set $\{\tau^\alpha \vdash \alpha \in \langle \iota, \kappa \rangle\}$ where $\iota, \kappa : \mathbb{Z}_N \to \mathbb{Z}_N$ are maps given by $\iota : x \mapsto x+1$, and $\kappa : x \mapsto -x^{-1}$.

Proof. Very easy. □

10.6 Upper-Bounds on $|\Delta(a)|$.

Since there is no simple computational formula for $\Delta(a)$, it is often convenient to have instead a simple upper-bound on $|\Delta(a)|$. The goal of this section is derive two upper-bounds and compare them. It turns out to be much easier to derive the upper-bounds than to decide which is the better (that is, lower) bound. The first upper-bound is the simpler and the easiest to derive, but the second is more constraining, though we do not demonstrate this here.

10.6.1 **Theorem** Let $a \in \mathbf{circ}_N(\mathbb{R})$. Then, $|\Delta(a)| \leq d^N$ where $d = \sqrt{\sum_{i \in \mathbb{Z}_N} a_i^2}$.

Proof. Let $A = \mathrm{CIRC}_n(a)$. Now, $\det(A)$ is the Jacobian of the transformation $A : \mathbb{R}^N \to \mathbb{R}^N$. Therefore, N-dimensional volumes are increased by the factor of $|\det(A)|$. Since $\{\mathrm{u}^i : i \in \mathbb{Z}_N\}$ is an orthonormal basis for $\mathbb{R}^N$, the volume spanned by these vectors equals 1. So what we need is an estimate of the volume enclosed by the transformed vectors $A\mathrm{u}^i$.

Let $\vec{v}_i = A\mathrm{u}^i$, then $\vec{v}_i = (a_i, a_{i-1}, a_{i-2}, \ldots, a_{i+1})^T$. Let V denote the volume spanned by the hyper-parallelepiped $\{\vec{v}_0, \vec{v}_1, \ldots, \vec{v}_{N-1}\}$. The volume of V cannot exceed the volume enlosed by orthogonal vectors of lengths $\{|\vec{v}_0|, |\vec{v}_1|, \ldots, |\vec{v}_{N-1}|\}$. Therefore,

$$|\det(A)| \;=\; |V| \;\leq\; \prod_{i=0}^{N-1} |\vec{v}_i| \;=\; \prod_{i=0}^{N-1} \sqrt{\sum_{j \in \mathbb{Z}_N} a_j^2} \;=\; \left(\sum_{j \in \mathbb{Z}_N} a_j^2 \right)^{\frac{1}{2}N} \quad \square$$

The next theorem provides a different bound on $|\Delta(a)|$. The new bound is not as simple as that of Theorem 10.6.1, nor is it quite as easy to derive.

10.6.2 **Theorem** Let $a \in \mathbf{circ}_N(\mathbb{R})$. Let $d^2 = \sum_{i \in \mathbb{Z}_N} a_i^2$. Then,

$$|\Delta(a)| \leq \begin{cases} |\lambda_0| \left(\dfrac{Nd^2 - \lambda_0^2}{N-1} \right)^{\frac{1}{2}(N-1)} & \text{if } N \text{ is odd} \\ \left| \lambda_0 \lambda_{\frac{1}{2}N} \right| \left(\dfrac{Nd^2 - \lambda_0^2 - \lambda_{\frac{1}{2}N}^2}{N-2} \right)^{\frac{1}{2}N-1} & \text{if } N \text{ is even} \end{cases}$$

Proof. First we estimate the sum of all pairs $\lambda_i \lambda_{-i}$.

$$\sum_{k \in \mathbb{Z}_N} \lambda_k \lambda_{-k} \;=\; \sum_{k \in \mathbb{Z}_N} \left(\sum_{i \in \mathbb{Z}_N} a_i \zeta^{ki} \right) \left(\sum_{j \in \mathbb{Z}_N} a_j \zeta^{-kj} \right) \;=\; \sum_{i \in \mathbb{Z}_N} \sum_{j \in \mathbb{Z}_N} a_i a_j \sum_{k \in \mathbb{Z}_N} \zeta^{k(i-j)} \;=\; N \sum_{i \in \mathbb{Z}_N} a_i^2$$

$$\therefore \quad \sum_{k \in \mathbb{Z}_N} |\lambda_k|^2 \;=\; Nd^2$$

Case I. N is odd. In the above sum, each eigenvalue except λ_0 is counted twice.

$$\therefore \quad \lambda_0^2 \;+\; 2 \sum_{k=1}^{\frac{1}{2}(N-1)} |\lambda_k|^2 \;=\; Nd^2$$

On the other hand, the determinant, Δ, is given by

$$\frac{\Delta}{\lambda_0} \;=\; \prod_{j=1}^{N-1} \lambda_j \;=\; \prod_{j=1}^{\frac{1}{2}(N-1)} |\lambda_i|^2$$

The geometric mean of non-negative reals cannot exceed the arithmetic mean. Therefore,

$$\left|\frac{\Delta}{\lambda_0}\right|^{\frac{2}{N-1}} \;=\; \left(\prod_{j=1}^{\frac{1}{2}(N-1)} |\lambda_i|^2\right)^{\frac{2}{N-1}} \;\leq\; \frac{2}{N-1} \sum_{k=1}^{\frac{1}{2}(N-1)} |\lambda_i|^2 \;\doteq\; \frac{2}{N-1}\left(\tfrac{1}{2}\, N d^{\,2} - \tfrac{1}{2}\,\lambda_0^2\right)$$

$$\therefore\; |\Delta| \;\leq\; |\lambda_0| \left(\frac{N d^{\,2} - \lambda_0^2}{N-1}\right)^{\frac{1}{2}(N-1)}$$

This completes the proof for N odd. QED(Case I).

Case II. N is even. In this case, there are two real eigenvalues, so

$$\lambda_0^2 \;+\; \lambda_{\frac{1}{2}N}^2 \;+\; 2 \sum_{k=1}^{\frac{1}{2}N-1} |\lambda_k|^2 \;=\; N d^{\,2}$$

Now we estimate instead

$$\frac{\Delta}{\lambda_0 \lambda_{\frac{1}{2}N}} \;=\; \prod_{k=1}^{\frac{1}{2}N-1} |\lambda_i|^2$$

Applying the principle of the geometric mean $\leq$ arithmetic mean again gives the formula of the theorem statement. □

10.6.3 Relative Merits of the Two Bounds.

The bound of Theorem 10.6.1 can be improved if it is known that two vectors $\vec{v}_i = A\mathrm{u}^i$ and $\vec{v}_j = A\mathrm{u}^j$ are close to parallel and their mutual angle can be estimated. (The bound was derived on the worst-case assumption that all vectors $\vec{v}_k$ were orthogonal.) The bound of Theorem 10.6.2 can be improved if $|\lambda_i|$ can be estimated for some i, particularly if the value is close to zero.

It is not immediately apparent which of the two bounds is the best, that is, the lowest. In fact the bound of Theorem 10.6.2 is always at least as good as the bound of Theorem 10.6.1. Ironically, probably the easiest way of demonstrating this is to show that the bound of Theorem 10.6.1 implies that of Theorem 10.6.2. Here is the idea. We add an arbitrary constant to every entry in the circulant vector; so $(a_0, a_1, \ldots, a_N) \mapsto (a_0{+}x, a_1{+}x, \ldots, a_{N-1}{+}x) = a'$, say, This affects only λ_0 leaving all other eigenvalues unchanged. So the determinant of a' is easily computed given the determinant of a. We then use the bound of Theorem 10.6.1 to bound $\det(a')/\lambda_0(a')$ and find the lowest possible value of this by finding its stationary point. But, $\det(a')/\lambda_0(a') = \det(a)/\lambda_0(a)$; so we obtain a new bound on $\det(a)$. The best possible bound over all $x \in \mathbb{R}$ is actually the bound of Theorem 10.6.2!

Bounds on the circulant determinant are important in the theory cyclotomic integers. Suppose momentarily that $N = p$, an odd prime, and that $a \in \mathbf{circ}_p(\mathbb{Z})$. Let $\xi = \lambda_1(a)$, then ξ is an algebraic integer in the domain $\mathbb{Z}(\zeta_p)$. The algebraic norm $\mathcal{N}(\xi)$ of ξ is the product of all algebraic conjugates of ξ. Hence, $\Delta(a) = \lambda_0(a)\mathcal{N}(\xi)$, and so, if given $\lambda_0(a) \neq 0$, a bound on the determinant implies a bound on the norm of ξ, and vice versa. Indeed, assuming $\lambda_0 \neq 0$, the bound Theorem 10.6.2 immediately gives the following bound on the norm:

$$\mathcal{N}(\xi) \;\leq\; \left(\frac{p d^{\,2} - \lambda_0^2}{p-1}\right)^{\frac{1}{2}(p-1)} \qquad \text{where } d^{\,2} = \sum a_i^2$$

Kummer derived this same bound for the norm using essentially the same argument as we used to derive the bound of Theorem 10.6.2, and with this bound was able to show that the class group of the p^{th} cyclotomic field is finite.