ON WENDT’S DETERMINANT

CHARLES HELOU

Abstract. Wendt’s determinant of order $m$ is the circulant determinant $W_m$ whose $(i, j)$-th entry is the binomial coefficient $\binom{m}{i-j}$, for $1 \leq i, j \leq m$. We give a formula for $W_m$, when $m$ is even not divisible by 6, in terms of the discriminant of a polynomial $T_{m+1}$, with rational coefficients, associated to $(X + 1)^{m+1} - X^{m+1} - 1$. In particular, when $m = p - 1$ where $p$ is a prime $\equiv -1 \pmod{6}$, this yields a factorization of $W_{p-1}$ involving a Fermat quotient, a power of $p$ and the 6-th power of an integer.

Introduction

E. Wendt ([12]) introduced the $m \times m$ circulant determinant $W_m$ with first row the binomial coefficients $\binom{m}{0}, \binom{m}{1}, \ldots, \binom{m}{m-1}$, i.e.

\[ W_m = \begin{vmatrix} 1 & \binom{m}{1} & \binom{m}{2} & \cdots & \binom{m}{m-1} \\ \binom{m}{m-1} & 1 & \binom{m}{1} & \cdots & \binom{m}{m-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \binom{m}{1} & \binom{m}{2} & \binom{m}{3} & \cdots & 1 \end{vmatrix}, \]

which is the resultant of the polynomials $X^m - 1$ and $(X + 1)^m - 1$, in connection with Fermat’s last theorem ([10]). E. Lehmer ([9]) proved that $W_m = 0$ if and only if $m \equiv 0 \pmod{6}$, and that if $p$ is an odd prime number, then $W_{p-1}$ is divisible by $p^{p-2} q_p(2)$, where $q_p(2) = \frac{p^{p-1} - 1}{p}$ is a Fermat quotient. L. Carlitz ([2]) determined $W_{p-1}$ modulo $p^{p-1}$, which he then used to find high powers of $p$ dividing $W_{p-1}$ in an application in the same connection ([3]). Factorizations of the integers $W_m$ for $m \leq 50$ were given in ([7]). The size of $W_m$ was investigated in ([1]). Granville and Fee ([5]) determined the prime factors of $W_m$ for all even $m \leq 200$ and consequently improved on a classical result about Fermat’s equation. This was further improved in ([6]), where similar computations were carried up to $m \leq 500$.

In this article, we show that for all positive even integers $m$ not divisible by 6,

\[ W_m = -9^{h_m} (2^{m-1} - 1)^3 (m + 1)^{m-4|h_m|} D_m^6, \]

where $D_m$ is the discriminant of a polynomial with rational coefficients whose roots are given by a rational function of those of $(X + 1)^{m+1} - X^{m+1} - 1$, and $h_m = 2$ or $-1$ according as $m \equiv 2 \text{ or } 4 \pmod{6}$ respectively. In particular, if $p$ is a prime $\equiv -1 \pmod{6}$ then $D_{p-1}$ is a rational integer and we have the factorization

\[ W_{p-1} = -\frac{1}{9} q_p(2)^3 p^{p-2} D_{p-1}^6. \]

Received by the editor May 6, 1996.

1991 Mathematics Subject Classification. Primary 11C20; Secondary 11Y40, 11D41, 12E10.

©1997 American Mathematical Society
1. Preliminary results

For any positive integer \( m \), let \( \zeta_m \) be a primitive \( m \)-th root of unity in \( \mathbb{C} \). By a well-known expression for circulant determinants ([12]),

\[
W_m = \prod_{j=0}^{m-1} \left( \sum_{k=0}^{m-1} \binom{m-1}{k} \zeta_m^k \right) = \prod_{j=0}^{m-1} \left( (1 + \zeta_m^j)^m - 1 \right).
\]

Denote by \( n \) an odd integer \( \geq 3 \) and consider the polynomial

\[
P_n(X) = (X + 1)^n - X^n - 1.
\]

Its relation to Wendt’s determinant is the following

**Proposition 1.** For any odd integer \( n \geq 3 \), the discriminant of \( P_n \) is

\[
D(P_n) = (-1)^{\frac{n-1}{2}} n^{n-2} W_{n-1}.
\]

**Proof.** Since \( P_n \) has degree \( n - 1 \) and leading coefficient \( n \), we have ([4] or [11]) \( D(P_n) = (-1)^{\frac{n-1}{2}(n-2)} n^{n-1} R(P_n, P'_n) \), where \( R(P_n, P'_n) \) is the resultant of \( P_n \) and its derivative \( P'_n \). We also have \( R(P_n, P'_n) = (n(n-1))^{n-1} \prod_{k=1}^{n-2} P_n(y_k) \), where \( y_k = \frac{1}{\zeta_n^{k-1}} \) (\( 1 \leq k \leq n - 2 \)) are the roots of \( P'_n(X) = n((X + 1)^n - X^n - 1) \) in \( \mathbb{C} \). Every \( P_n(y_k) = \frac{1 - (\zeta_n^{k-1})^{n-1}}{(\zeta_n^{k-1})^{n-1}} \), for \( 1 \leq k \leq n - 2 \). The product \( \prod_{k=1}^{n-2} (1 - \zeta_n^{k-1})^{n-1} \) is the value at \( 1 \) of \( (X^{n-1} - 1)/(X - 1) \), which is \( n - 1 \). Moreover, since \( n \) is odd, \( \prod_{k=1}^{n-2} (1 - \zeta_n^{k-1})^{n-1} = \prod_{k=0}^{n-2} \left( 1 + \zeta_n^{k-1} \right)^{n-1} = W_{n-1} \), by (1). Hence \( \prod_{k=1}^{n-2} P_n(y_k) = \frac{W_{n-1}}{(n-1)!} \) and the result follows by substitution.

Now the polynomial \( P_n \) can be written ([8])

\[
P_n(X) = X(X + 1)(X^2 + X + 1)^{\nu_n} F_n(X),
\]

where \( F_n \) lies in \( \mathbb{Z}[X] \), is prime to \( X(X+1)(X^2+X+1) \), has degree \( d_n = n - 3 - 2\nu_n \) and leading coefficient \( n \), with \( \nu_n = 0 \), 1 or 2 according as \( n \equiv 0 \), 2 or 1 (mod 3) respectively. It follows from (2) and (3) that \( F_n(-X - 1) = F_n(X) \) and \( F_n(1/X) = F_n(X)/X^{d_n} \). Hence the set of roots \( z \) of \( F_n \) in \( \mathbb{C} \) is partitioned into \( r_n = d_n/6 \) orbits of 6 elements each, namely

\[
\text{Orb}(z) = \{ z, 1/z, -z, -1/z, -1/z + 1, -z + 1/z \}.
\]

Let \( z_1, \ldots, z_{r_n} \) be representatives of the different orbits of roots of \( F_n \). For every \( 1 \leq j \leq r_n \), let \( g_j \) be the monic polynomial whose roots are the elements of \( \text{Orb}(z_j) \). A straightforward computation gives

\[
g_j(X) = X^6 + 3X^5 + t_jX^4 + (2t_j - 5)X^3 + t_jX^2 + 3X + 1 \quad (1 \leq j \leq r_n)
\]

where

\[
t_j = 6 - J(z_j), \quad J(X) = \frac{(X^2 + X + 1)^3}{X^2(X + 1)^2}
\]

and

\[
F_n = n \prod_{j=1}^{r_n} g_j.
\]
Moreover

\[(8) \quad g_j(X) = X^2(X + 1)^2 (J(X) - J(z_j)) \quad (1 \leq j \leq r_n).\]

We now introduce the polynomial

\[(9) \quad T_n(X) = \prod_{j=1}^{r_n} (X - t_j)\]

which lies in \( \mathbb{Q}[X] \), since the automorphisms of the splitting field of \( F_n \) over \( \mathbb{Q} \) permute the roots of \( T_n \) and thus leave its coefficients fixed. Substituting (8) into (7) yields

\[(10) \quad F_n(X) = (-1)^{r_n} nX^{2r_n} (X + 1)^{2r_n} T_n(6 - J(X)).\]

This relation, linking \( T_n \) to \( F_n \) and thus to \( P_n \), facilitates computations with \( T_n \).

2. Discriminants calculations

The resultant of two non-zero polynomials \( f, g \in \mathbb{C}[X] \) is denoted by \( R(f, g) \) and the discriminant of \( f \) by \( D(f) \). The classic formula ([4]) \( D(fg) = D(f)D(g)R(f, g)^2 \) yields by induction

**Lemma 1.** If \( f_1, \ldots, f_m \) are non-constant polynomials in \( \mathbb{C}[X] \), then

\[D \left( \prod_{i=1}^{m} f_i \right) = \prod_{i=1}^{m} D(f_i) \cdot \prod_{1 \leq i < j \leq m} R(f_i, f_j)^2.\]

Using this, the relation (3) allows, when \( e_n < 2 \), to express \( D(F_n) \) in terms of \( D(P_n) \). Indeed,

**Lemma 2.** For a positive odd integer \( n \equiv 1 (mod \ 6) \),

\[D(F_n) = \frac{(-1)^{r_n} D(P_n)}{3^{e_n} n^{4(e_n + 1)}}.\]

**Proof.** Assume first \( n \equiv -1 (mod \ 6) \), so that \( e_n = 1 \) and

\[P_n(X) = X(X + 1)(X^2 + X + 1)F_n(X).\]

From Lemma 1,

\[D(P_n) = -3(F_n(0)F_n(-1)F_n(\zeta_3)F_n(\zeta_3^2))^2 D(F_n).\]

Now, for all odd \( n \), \( F_n(0) = F_n(-1) = n \), since these are the values of \( P_n(X)/X \) at 0 and \( -P_n(X)/(X + 1) \) at \(-1\) respectively. On the other hand, setting \( P_n(X) = (X^2 + X + 1)Q_n(X) \), with \( Q_n \in \mathbb{Z}[X] \), we have

\[F_n(\zeta_3) = \frac{Q_n(\zeta_3)}{\zeta_3(\zeta_3 + 1)} = \frac{P_n^r(\zeta_3)}{2\zeta_3 + 1} = \frac{n ((\zeta_3 + 1)^{n-1} - \zeta_3^{n-1})}{2\zeta_3 + 1} = n.\]

Also, \( F_n(\zeta_3^2) \), being the complex conjugate of \( F_n(\zeta_3) \), is equal to \( n \) too. Hence \( D(P_n) = -3n^8 D(F_n) \). Similarly, in the simpler case where \( n \equiv 3 (mod \ 6) \), we have

\[P_n(X) = X(X + 1)F_n(X) \quad \text{so that} \quad D(P_n) = (F_n(0)F_n(-1))^2 D(F_n) = n^8 D(F_n).\]

We now relate the discriminants of \( F_n \), \( T_n \) and the \( g_j \)'s.

**Lemma 3.** For any odd integer \( n \geq 3 \),

\[D(F_n) = n^{2(d_n-1)} \prod_{j=1}^{r_n} D(g_j). D(T_n)^6.\]
where the products are for \(D\) so that

\[
\prod_{i<j} R(g_i,g_j)^2.
\]

By (8), for \(1 \leq i,j \leq r_n, R(g_i,g_j) = \prod_z g_j(z) = (J(z_i) - J(z_j))^6 (\prod_z z(z+1)^2),
\]

where the products are for \(z\) ranging in \(\text{Orb}(z_i)\), in which case \(J(z) = J(z_i)\) by (5) and (6). Moreover, \(\prod_z z = g_j(0) = 1\) and \(\prod_z (z+1) = g_j(1) = 1\). Hence \(R(g_j,g_j) = R(g_i,g_j) = (J(z_i) - J(z_j))^6\). On the other hand, \(D(T_n) = (-1)^{r_n(r_n-1)/2} \prod_{i\neq j} (t_i - t_j) = \pm \prod_{i\neq j} (J(z_i) - J(z_j))\), where the products are for all \(i,j \in \{1,\ldots,r_n\}\) with \(i \neq j\). Hence \(\prod_{1 \leq i < j \leq r_n} R(g_i,g_j)^2 = \prod_{i \neq j} R(g_i,g_j) = \prod_{i \neq j} (J(z_i) - J(z_j))^6 = D(T_n)^2\) and the result follows.

Next, we compute the discriminants of the \(g_j\)'s.

**Lemma 4.** For any odd integer \(n \geq 3\) and \(1 \leq j \leq r_n,
\[
D(g_j) = -(4t_j + 3)^3(t_j - 6)^4.
\]

**Proof.** Let \(Y = X + 1/X\). Then \(g_j(X) = X^3 h_j(Y)\), where \(h_j(Y) = Y^3 + 3Y^2 + (t_j-3)Y + 2t_j - 11\); and \(g_j'(X) = 3g_j(X)/X + (X^3 - X)h_j'(Y)\). Hence

\[
D(g_j) = -\prod_z g_j'(z) = -\left(\prod_z \left(\prod_z (z+1)\right) \prod_z h_j'(z + 1/z)\right),
\]

where the products are for \(z \in \text{Orb}(z_i)\). From the proof of Lemma 3, \(\prod_z z = \prod_1(z+1) = 1\). Also \(\prod_1 (z+1) = g_j(1) = 4t_j + 3\). Moreover, \(y = z + 1/z\) ranges through the roots of \(h_j\), each repeated twice, as \(z\) ranges through \(\text{Orb}(z_i)\), so that \(\prod_z h_j'(z + 1/z) = \left(\prod_y h_j'(y)\right)^2 = D(h_j)^2\). Thus \(D(g_j) = -(4t_j + 3)D(h_j)^2\). Now, setting \(U = Y + 1\), we have \(h_j(Y) = f_j(U) = U^3 + (t_j - 6)U + t_j - 6\). By a well-known formula for the discriminant of a cubic polynomial \((11)\), we get \(D(h_j) = D(f_j) = -(4t_j + 3)(t_j - 6)^2\). Hence the result.

The product, appearing in Lemma 3, of the discriminants of the \(g_j\)'s is given by

**Lemma 5.** For any odd integer \(n \geq 3\),
\[
\prod_{j=1}^{r_n} D(g_j) = (-1)^{r_n} 4^{(2n-1)} \cdot 3^3 \cdot n^{4} \cdot (2n-1)^4 \cdot (n-1/2n)^2 \cdot \epsilon_n^{e_n-1}.
\]

**Proof.** By Lemma 4,
\[
(11) \quad \prod_{j=1}^{r_n} D(g_j) = (-1)^{r_n} \left(\prod_{j=1}^{r_n} (4t_j + 3)\right)^3 \left(\prod_{j=1}^{r_n} (t_j - 6)\right)^4.
\]

Now \(\prod_{j=1}^{r_n} (4t_j + 3) = (-4)^{r_n} T_n(3/4)\). Moreover, substituting \(X = 1\) into (10) and (3), we get \((-4)^{r_n} n T_n(-3/4) = F_n(1) = P_n(1)/(2.3^{r_n})\). Hence
\[
(12) \quad \prod_{j=1}^{r_n} (4t_j + 3) = F_n(1) = \frac{2^{n-1} - 1}{3^{r_n} n}.
\]

Similarly, \(\prod_{j=1}^{r_n} (t_j - 6) = (-1)^{r_n} T_n(6)\), and substituting \(X = \zeta_3\) into (10) yields \((-1)^{r_n} n T_n(6) = F_n(\zeta_3)\). Let \(Q_n(X) = X(X+1) F_n(X)\); then \(F_n(\zeta_3) = -Q_n(\zeta_3)\) and, by (3), \(P_n(X) = (X^2 + X + 1)^{r_n} Q_n(X)\). Taking \(\epsilon_n\)-th derivatives in the latter relation and making \(X = \zeta_3\), we get \(Q_n(\zeta_3) = P_n(\zeta_3)/\epsilon_n!(2\zeta_3 + 1)^{r_n}\) (here
2\zeta_3 + 1 is the value of the factor \( X - \zeta_3^3 \) in \( X^2 + X + 1 \), and the equality follows from Taylor’s formula. Hence

\[
\prod_{j=1}^{r_n} (t_j - 6) = \frac{F_n(\zeta_3)}{n} = -\frac{P_{n}^{(e_n)}(\zeta_3)}{e_n!n(2\zeta_3 + 1)^{e_n}}.
\]

Simple computations show that \(-P_{n}^{(e_n)}(\zeta_3)/(2\zeta_3 + 1)^{e_n} = 3 \) or \( n \) or \( n(n - 1)/3 \) according as \( n \equiv 0 \) or 2 or 1 (mod 3) respectively. Therefore \( \prod_{j=1}^{r_n} (t_j - 6) = 3/n \) or 1 or \((n - 1)/6 \) respectively. One formula representing all three cases is

\[
(13) \quad \prod_{j=1}^{r_n} (t_j - 6) = \left( \frac{n}{3} \right)^{e_n - 1} \left( \frac{n - 1}{2n} \right)^{\frac{e_n(e_n - 1)}{2}}.
\]

Substituting (12) and (13) into (11) yields the desired result.

3. Conclusion

We can now draw the formula relating Wendt’s determinant \( W_{n-1} \) to the discriminant of the polynomial \( T_n \), namely

**Proposition 2.** For any odd positive integer \( n \not\equiv 1 \) (mod 6),

\[
W_{n-1} = -9^{2 - 3e_n} (2n - 1)^3 n^{n + 4e_n - 9} D(T_n)^6,
\]

where \( e_n = 0 \) or 1 according as \( n \equiv 3 \) or \(-1 \) (mod 6) respectively, and \( T_n \) is defined by (9).

**Proof.** By Lemmas 3 and 5, since \( d_n = n - 3 - 2e_n \) and \( e_n = 0 \) or 1, we have \( D(F_n) = (-1)^{e_n} 3^4 - 7e_n (2n - 1)^3 n^{2n - 15} D(T_n)^6 \). On the other hand, Proposition 1 and Lemma 2 imply \( D(F_n) = (-1)^{e_n + (n - 1)/2} 3^{-e_n} n^{n - 4e_n - 6} W_{n-1} \). Equating the two expressions (and noting that \( r_n + e_n + (n - 1)/2 = 2(n + e_n)/3 - 1 \) is odd) yields the desired result.

**Remark.** In Proposition 2, let \( m = n - 1 \) and \( h_m = 2 - 3e_n \), so that \( m \) is an even positive integer \( \equiv 0 \) (mod 6) and \( h_m = 2 \) or \(-1 \) according as \( m \equiv 2 \) or 4 (mod 6) respectively. Noting that \( 2 - e_n \) coincides with \( |h_m| \) and writing \( D_m \) for \( D(T_{m+1}) \), we obtain the formula for \( W_m \) stated in the Introduction.

Assume now that \( n = p \) is a prime number \( \equiv -1 \) (mod 6). Then the leading coefficient \( p \) of \( F_p \) divides all its coefficients \( t_k \), for \( 1 \leq k \leq p - 1 \), so that, by (3), \( F_p = pE_p \), where \( E_p \) is a monic polynomial in \( \mathbb{Z}[X] \). Thus the roots of \( F_p \) are algebraic integers. Since, by (5), \( t_j \) is a sum of products of roots of \( F_p \), then \( t_j \) is also an algebraic integer, for \( 1 \leq j \leq r_p \). Hence \( T_p \) has rational integer coefficients and \( D(T_p) \) lies in \( \mathbb{Z} \). Therefore Proposition 2 (where now \( e_p = 1 \)) implies

**Corollary.** If \( p \) is a prime number \( \equiv -1 \) (mod 6), then

\[
W_{p-1} = -\frac{1}{9} q_p(2)^3 p^{p-2} D(T_p)^6,
\]

where the discriminant \( D(T_p) \) is a rational integer and \( q_p(2) = 2^{p-1} - 1/p \).

Penn State University, Delaware County, 25 Yearsley Mill Road, Media, Pennsylvania 19063

E-mail address: cxh22@psu.edu