RESULTANTS OF CYCLOTOMIC POLYNOMIALS

TOM M. APOSTOL

1. Introduction. The cyclotomic polynomial $F_n(x)$ of order $n \geqq 1$ is the primary polynomial whose roots are the primitive nth roots of unity,

$$F_n(x) = \prod_{k=1}^{n}{}' (x - e^{2\pi i k/n}), \tag{1.1}$$

where the $'$ indicates that the index k runs through integers relatively prime to n. The degree of $F_n(x)$ is $\phi(n)$, Euler's totient.

This paper determines the resultant $\rho(F_m, F_n)$ of any two cyclotomic polynomials F_m and F_n. Explicit formulas are given which show that if $m \neq n$ the resultant is either 1, -2, or a prime power. For the case $m > n > 1$ the results agree with a formula derived by Diederichsen [**3**, Hilfssatz 2] in a paper on group representations (see Theorem 4 below). Our proof is different from and somewhat simpler than that of Diederichsen; it is based on the following lemma on decompositions of reduced residue systems which the author has recently used to relate Gauss sums and primitive characters [**1**, Lemma 6].

Lemma. *Let S_k denote a reduced residue system modulo k, and let d be a divisor of k. Then S_k is the union of $\phi(k)/\phi(d)$ disjoint sets, each of which is a reduced residue system modulo d.*

We also make use of the following well-known formulas for cyclotomic polynomials [**2**, p. 31], [**4**, Chapter 8]:

$$x^n - 1 = \prod_{d|n} F_d(x) \tag{1.2}$$

and

$$\begin{aligned} F_n(1) &= 0 \qquad \text{if } n = 1, \\ &= p \qquad \text{if } n = p^a, \quad p \text{ prime}, \quad a \geqq 1, \\ &= 1 \qquad \text{otherwise}. \end{aligned} \tag{1.3}$$

Property (1.3) is an easy consequence of (1.2) and the relation $F_{p^a}(x) = F_p(y)$, $y = x^{p^{a-1}}$, p prime, $a > 1$ (see [**4**, p. 67]). We also use the fact that each $F_n(x)$ has integer coefficients [**4**, p. 61].

Received by the editors June 23, 1969.

2. Properties of resultants. Given two polynomials A and B, say

$$A(x) = \sum_{k=0}^{n} a_k x^k \quad \text{and} \quad B(x) = \sum_{k=0}^{m} b_k x^k,$$

their resultant $\rho(A, B)$ is defined to be the determinant

$$\rho(A, B) = \left| \begin{array}{cccccccc} a_n & a_{n-1} & a_{n-2} \cdots a_1 & a_0 & & & \\ & a_n & a_{n-1} \cdots a_2 & a_1 & a_0 & & \\ & & \cdots & & & & \\ & & & a_n & a_{n-1} \cdots a_1 & a_0 & \\ b_m & b_{m-1} & b_{m-2} \cdots b_1 & b_0 & & & \\ & b_m & b_{m-1} \cdots b_2 & b_1 & b_0 & & \\ & & \cdots & & & & \\ & & & b_m & b_{m-1} \cdots b_1 & b_0 & \end{array} \right| \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} n \text{ rows} \end{array},$$

the remaining entries being equal to zero. This formula shows that $\rho(A, B)$ is a polynomial in the a_i and b_j with integer coefficients. In particular, if all the a_i and b_j are integers then $\rho(A, B)$ is also an integer. Hence $\rho(F_n, F_m)$ is an integer for any two cyclotomic polynomials.

If A and B are expressed in terms of their zeros, say

$$A(x) = a_n \prod_{k=1}^{n} (x - x_k), \qquad B(x) = b_m \prod_{j=1}^{m} (x - y_j),$$

then the resultant can also be expressed as a product,

$$\rho(A, B) = a_n^m b_m^n \prod_{k=1}^{n} \prod_{j=1}^{m} (x_k - y_j). \tag{2.1}$$

A proof of (2.1) is given in [**5**]. This formula implies the multiplicative property

$$\rho(A, BC) = \rho(A, B)\rho(A, C) \tag{2.2}$$

for any polynomials A, B, C; the symmetry property

$$\rho(A, B) = (-1)^{mn}\rho(B, A); \tag{2.3}$$

and the factorization formula

$$\rho(A, B) = b_m^n \prod_{j=1}^{m} A(y_j). \tag{2.4}$$

Two polynomials A and B have a root in common if and only if $\rho(A, B)=0$. In particular, $\rho(F_m, F_n)=0$ if and only if $m=n$.

3. The resultant of F_1 and F_m. Applying equation (2.1) to the cyclotomic polynomials F_1 and F_m, where $m>1$, we find

$$\rho(F_1, F_m) = \prod_{k=1}^{m}{}' (1 - e^{2\pi ik/m}) = F_m(1). \tag{3.1}$$

Using (1.3) we obtain

THEOREM 1. *If $m>1$ we have*

$$\begin{aligned}\rho(F_1, F_m) &= p \qquad \text{if } m = p^a, \quad p \text{ prime}, \quad a \geqq 1,\\ &= 1 \qquad \text{otherwise.}\end{aligned}$$

It should be noted that $\rho(F_m, F_1)=(-1)^{\phi(m)}\rho(F_1, F_m)$, so $\rho(F_2, F_1) =-\rho(F_1, F_2)=-2$ and $\rho(F_m, F_1)=\rho(F_1, F_m)$ if $m>1$.

4. A product formula for $\rho(F_m, F_n)$ when $m>n>1$. The restriction $m>n>1$ is not serious because

$$\rho(F_m, F_n) = (-1)^{\phi(m)\phi(n)}\rho(F_n, F_m) = \rho(F_n, F_m).$$

We use the lemma of §1 to prove

THEOREM 2. *If $m>n>1$ we have*

$$\rho(F_m, F_n) = \prod_{d,p} p^{\mu(n/d)\phi(m)/\phi(p^a)}, \tag{4.1}$$

where the product is extended over those divisors d of n and those primes p such that $m/(m, d)=p^a$ for some $a\geqq 1$.

PROOF. Using (1.2) and the multiplicative property (2.2) we obtain

$$\rho(F_m, x^n - 1) = \prod_{d|n} \rho(F_m, F_d). \tag{4.2}$$

Since $m>n>1$ each factor in (4.2) is nonzero and we can apply the Möbius inversion formula to obtain

$$\rho(F_m, F_n) = \prod_{d|n} \rho(F_m, x^d - 1)^{\mu(n/d)}. \tag{4.3}$$

Using the symmetry property (2.3) and equation (2.4) we find

$$\rho(F_m, x^d - 1) = (-1)^{d\phi(m)}\rho(x^d - 1, F_m) = \prod_{k=1}^{m}{}' (e^{2\pi ikd/m} - 1).$$

In the exponential we write

$$\frac{kd}{m} = \frac{kd/\delta}{m/\delta}, \quad \text{where} \quad \delta = (m, d), \qquad \left(\frac{m}{\delta}, \frac{d}{\delta}\right) = 1.$$

By the lemma, as k runs through a reduced residue system modulo m the product kd/δ runs through a reduced residue system modulo m/δ with each residue appearing exactly $\phi(m)/\phi(m/\delta)$ times. Therefore

$$\begin{aligned} \rho(F_m, x^d - 1) &= \left\{ \prod_{r=1}^{m/\delta}{}' \left(e^{2\pi i r/(m/\delta)} - 1\right) \right\}^{\phi(m)/\phi(m/\delta)} \\ &= F_{m/\delta}(1)^{\phi(m)/\phi(m/\delta)}. \end{aligned}$$

Using (1.3) to evaluate $F_{m/\delta}(1)$ we find

$$\begin{aligned} \rho(F_m, x^d - 1) &= p^{\phi(m)/\phi(m/\delta)} \qquad \text{if } m/\delta = p^a \text{ for some prime } p, \\ &= 1 \qquad \text{otherwise.} \end{aligned}$$

Substituting this in (4.3) we obtain Theorem 2.

5. **Evaluation of $\rho(F_m, F_n)$ for $m>n>1$.** We consider two cases, $(m, n)=1$ and $(m, n)>1$. If $(m, n)=1$ then $(m, d)=1$ for every divisor d of n, so the product in Theorem 2 is empty unless m is a prime power. If $m=p^a$ the product in Theorem 2 becomes

$$\prod_{d|n} p^{\mu(n/d)} = 1$$

since $\sum_{d|n} \mu(n/d)=0$ for $n>1$. In other words, we have proved:

THEOREM 3. *If $m>n>1$ and $(m, n)=1$, then $\rho(F_m, F_n)=1$.*

Next we consider the case in which m and n are not relatively prime. In this case we obtain

THEOREM 4. *If $m>n>1$ and $(m, n)>1$, then*

$$\begin{aligned} \rho(F_m, F_n) &= p^{\phi(n)} \qquad \textit{if } m/n \textit{ is a power of a prime } p, \\ &= 1 \qquad \textit{otherwise.} \end{aligned}$$

PROOF. We replace d by n/d in the product (4.1) and rewrite it in the form

$$\rho(F_m, F_n) = \prod_{d,p} p^{\mu(d)\phi(m)/\phi(p^a)} \tag{5.1}$$

where the product is extended over those divisors d of n and those primes p such that $m/(m, n/d)=p^a$. Because of the Möbius function we need consider only square-free divisors d.

We write $m=km'$, $n=kn'$, where $k=(m, n)$ and $(m', n')=1$. Then

$$\frac{m}{(m, n/d)} = \frac{km'}{(km', kn'/d)} = \frac{km'n'}{kn'(m'd, n')/d} = \frac{m'd}{(m'd, n')} = \frac{m'd}{\delta}$$

where $\delta = (m'd, n')$. Since $(m', n') = 1$ we have $(\delta, m') = 1$ so $\delta | d$. Therefore $m'd/\delta$ is a multiple of m'. For this to be a prime power, both m' and d/δ must be powers of the same prime.

If m' is not a prime power the product in (5.1) is empty and $\rho(F_m, F_n) = 1$. Assume, then, that m' is a prime power, say

$$m' = p^\alpha.$$

We seek those divisors d of n for which d/δ is a power of the same prime, say $d/\delta = p^\beta$. This implies $d = \delta p^\beta$, $\beta \geqq 0$.

Now $n = kn'$ and $d | n$ so $\delta p^\beta | kn'$, hence $p^\beta | kn'$. But $(p, n') = 1$ since $(m', n') = 1$, so $p^\beta | k$. Therefore we can write $k = p^\gamma k'$, where $(p, k') = 1$. We now have

$$n = kn' = p^\gamma k'n', \qquad m = km' = p^{\alpha+\gamma}k', \qquad \frac{m}{(m, n/d)} = \frac{m'd}{\delta} = p^{\alpha+\beta}.$$

We also have $d = \delta p^\beta$. Since d is square-free this requires $\beta = 0$ or $\beta = 1$, so each d has the form δ or δp, where $(p, \delta) = 1$. Now $d | n$ so $d | p^\gamma k'n'$. If we let d' range through all the square-free divisors of $k'n'$ we see that the possible values of d are all the divisors d' (these correspond to $\beta = 0$) plus all products of the form pd' (these correspond to $\beta = 1$). The contribution to the product in (5.1) from each divisor d' is p raised to the power $\mu(d')\phi(m)/\phi(p^\alpha)$. The contribution from each divisor pd' is p raised to the power $-\mu(d')\phi(m)/\phi(p^{\alpha+1})$. But we have

$$\frac{\phi(m)}{\phi(p^\alpha)} = \frac{\phi(p^{\alpha+\gamma})\phi(k')}{\phi(p^\alpha)} = \frac{p^\gamma\phi(p^\alpha)\phi(k')}{\phi(p^\alpha)} = p^\gamma\phi(k')$$

and, similarly,

$$\phi(m)/\phi(p^{\alpha+1}) = p^{\gamma-1}\phi(k').$$

Therefore

$$\phi(m)/\phi(p^\alpha) - \phi(m)/\phi(p^{\alpha+1}) = (p^\gamma - p^{\gamma-1})\phi(k') = \phi(p^\gamma)\phi(k') = \phi(k).$$

Therefore the contribution to the product from each pair of divisors $d = d'$ and $d = pd'$ is $p^{\mu(d')\phi(k)}$. We do not alter the product if we also include as factors the same power of p taken over the nonsquare-free divisors of $k'n'$. Therefore we obtain

$$\rho(F_m, F_n) = \prod_{d' | k'n'} p^{\mu(d')\phi(k)} = \left\{p^{\phi(k)}\right\}^t,$$

where

$$t = \sum_{d' \mid k'n'} \mu(d') = 1 \qquad \text{if } k'n' = 1,$$

$$= 0 \qquad \text{if } k'n' > 1.$$

This shows that $\rho(F_m, F_n) = 1$ unless $k'n' = 1$, in which case $\rho(F_m, F_n) = p^{\phi(k)}$. But $k'n' = 1$ implies $k' = n' = 1$ and this implies $n = k = p^\gamma$, $m = np^\alpha$. Therefore the resultant is equal to 1 unless $m/n = p^\alpha$, in which case $\rho(F_m, F_n) = p^{\phi(n)}$. This completes the proof of Theorem 4.

References

1. Tom M. Apostol, *Euler's ϕ-function and separable Gauss sums*, Proc. Amer. Math. Soc. **24** (1970), 482–485.

2. L. E. Dickson, H. H. Mitchell, H. S. Vandiver and G. E. Wahlin, *Algebraic numbers*, Bulletin of the National Research Council, vol. 5, part 3, no. 28, National Academy of Sciences, 1923.

3. Fritz-Erdmann Diederichsen, *Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz*, Abh. Math. Sem. Hanischen Univ. **13** (1940), 357–412. MR **2**, 4.

4. Hans Rademacher, *Lectures on elementary number theory*, Blaisdell, Waltham, Mass., 1964. MR **30** #1079.

5. B. L. van der Waerden, *Moderne algebra*. Vol. I, 2nd rev. ed., Springer, Berlin, 1937; English transl., Ungar, New York, 1949. MR **2**, 120; MR **10**, 587.

California Institute of Technology