The Resultant of the Cyclotomic Polynomials $F_m(ax)$ and $F_n(bx)$

By Tom M. Apostol

Abstract. The resultant $\rho(F_m(ax), F_n(bx))$ is calculated for arbitrary positive integers $m$ and $n$, and arbitrary nonzero complex numbers $a$ and $b$. An addendum gives an extended bibliography of work on cyclotomic polynomials published since 1919.

1. Introduction. Let $F_n(x)$ denote the cyclotomic polynomial of degree $\varphi(n)$ given by

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

where the ' indicates that $k$ runs through integers relatively prime to the upper index $n$, and $\varphi(n)$ is Euler's totient. The resultant $\rho(F_m, F_n)$ of any two cyclotomic polynomials was first calculated by Emma Lehmer [9] in 1930 and later by Diederichsen [21] and the author [64]. It is known that $\rho(F_m, F_n) = 1$ if $(m, n) = 1$, $m > n > 1$. This implies that for any integer $q$ the integers $F_m(q)$ and $F_n(q)$ are relatively prime if $(m, n) = 1$.

Divisibility properties of cyclotomic polynomials play a role in certain areas of the theory of numbers, such as the distribution of quadratic residues, difference sets, perfect numbers, Mersenne-type numbers, and primes in residue classes. There has also been considerable interest lately in relations between the integers $F_p(q)$ and $F_q(p)$, where $p$ and $q$ are distinct primes. In particular, Marshall Hall informs me that the Feit-Thompson proof [47] could be shortened by nearly 50 pages if it were known that $F_p(q)$ and $F_q(p)$ are relatively prime, or even if the smaller of these integers does not divide the larger. Recently, N. M. Stephens [69] has shown that when $p = 17$ and $q = 3313$, the prime $112643 = 2pq + 1$ divides both $F_p(q)$ and $F_q(p)$. These remarks suggest a study of relations connecting the polynomials $F_p(qx)$ and $F_q(px)$.

For example, if the resultant of $F_p(qx)$ and $F_q(px)$ were equal to 1 it would follow that the integers $F_p(q)$ and $F_q(p)$ are relatively prime. In this note we use the method developed in [64] to calculate the resultant $\rho(F_m(ax), F_n(bx))$ for arbitrary positive integers $m$ and $n$, and arbitrary nonzero complex numbers $a$ and $b$ (see Theorem 1). When $m$ and $n$ are distinct primes $p$ and $q$ the results of Theorem 1 simplify considerably to give the explicit formula.
\[
\rho(F_q(ax), F_p(bx)) = \frac{a^{pq} - b^{pq}}{a^p - b^p} \frac{a - b}{a^q - b^q} \quad \text{if } a \neq b,
\]
(1)

\[
= a^{(p-1)(q-1)} \quad \text{if } a = b.
\]

Unfortunately this formula sheds no light on the g.c.d of the integers \( F_q(p) \) and \( F_p(q) \).

An addendum to the paper gives an extended bibliography of work on cyclotomic polynomials published since 1919. The report by Dickson et al. in [1] contains a history of earlier work in this area.

2. A Product Formula for \( \rho(F_m(ax), F_n(bx)) \). We assume throughout this section that \( m \) and \( n \) are integers \( > 1 \) and that \( a \) and \( b \) are arbitrary non-zero complex numbers.

**Theorem 1.** We have

\[
(2) \quad \rho(F_m(ax), F_n(bx)) = \prod_{d \mid n} F_{\frac{m}{\delta}}(a^{d\delta}) \prod_{d \mid n} \left( a^d - b^d \right)^{\mu(n/d) \varphi(m)/\varphi(m/\delta)},
\]

where \( \delta = (m, d) \) for each divisor \( d \) of \( n \).

**Proof.** We use the notation and properties of \( \rho(A, B) \) described in [64, pp. 457–458]. From the multiplicative property \( \rho(A, BC) = \rho(A, B)\rho(A, C) \) and the factorization

\[
F_n(x) = \prod_{d \mid n} \left( x^d - 1 \right)^{\mu(n/d)},
\]
we find, as in [64, Section 4],

\[
(3) \quad \rho(F_m(ax), F_n(bx)) = \prod_{d \mid n} f(d)^{\mu(n/d)},
\]

where

\[
f(d) = \rho(F_m(ax), (bx)^d - 1) = \rho((bx)^d - 1, F_m(ax))
\]
since \( \rho(A, B) = \rho(B, A) \) when \( \deg A \deg B \) is even. Using Eq. (2.4) of [64], we have

\[
f(d) = a^{d\varphi(m)} \prod_{k=1}^{m} \left( \frac{b^d}{a^d} e^{2\pi i kd/m} - 1 \right) = b^{d\varphi(m)} \prod_{k=1}^{m} \left( \frac{a^d}{b^d} - e^{2\pi i kd/m} \right).
\]

In the last exponential we write

\[
kd \quad \text{if } d \mid m \quad \text{and then use the Lemma on p. 457 of [64] to obtain}
\]

\[
\end{equation}

\[
\frac{kd}{m} = \frac{kd/\delta}{m/\delta}, \quad \text{where } \delta = (m, d), (m/\delta, d/\delta) = 1,
\]
and then use the Lemma on p. 457 of [64] to obtain
Using this in (3) along with the relation \( \sum_{d|n} d \mu(n/d) = \varphi(n) \), we obtain (2).

3. Special Cases of Theorem 1. If \( (m, n) = 1 \), then \( \delta = (m, d) = 1 \) for each divisor \( d \) of \( n \), and Theorem 1 simplifies as follows:

**Theorem 2.** If \( (m, n) = 1 \) we have

\[
\rho(F_m(ax), F_n(bx)) = b^{\varphi(mn)} \prod_{d|n} F_m \left( \frac{a^d}{b^d} \right)^{\mu(n/d)}.
\]

Next, we take \( n = p^\alpha \) where \( p \) is prime, \( p \nmid m \), and \( \alpha \geq 1 \). Let \( c = a/b \). Then the product in (4) has only two factors with nonzero exponent, those corresponding to \( d = p^{\alpha-1} \) and \( d = p^\alpha \). Hence the product simplifies to \( F_m(c^{p\alpha})/F_m(c^{p\alpha-1}) \). But by Dickson’s formula [1, p. 32]

\[
F_m(x^{p\alpha})/F_m(x^{p^{\alpha-1}}) = F_{mp^\alpha}(x),
\]
valid if \( p \nmid m \), the last quotient simplifies to \( F_{mp^\alpha}(c) \). Therefore we have proved:

**Theorem 3.** If \( p \) is prime and \( p \nmid m \), then for \( ab \neq 0 \) and each integer \( \alpha \geq 1 \) we have

\[
\rho(F_m(ax), F_{p^\alpha}(bx)) = b^{\varphi(mp^\alpha)} F_{mp^\alpha}(a/b).
\]

Finally, we take \( \alpha = 1 \) and \( n = q \), where \( q \) is a prime \( \neq p \), to obtain:

**Theorem 4.** If \( p \) and \( q \) are distinct primes and \( ab \neq 0 \), we have

\[
\rho(F_q(ax), F_p(bx)) = b^{(p-1)(q-1)} F_{pq}(a/b).
\]

**Note.** If \( a = b \), then \( F_{pq}(1) = 1 \) and \( \rho(F_q(ax), F_p(ax)) = a^{(p-1)(q-1)}. \)

To calculate \( F_{pq}(a/b) \) when \( a \neq b \) it is preferable to use Dickson’s formula (5) with \( \alpha = 1 \) and \( x = a/b \) to write

\[
F_{pq}(a/b) = F_q(x^p)/F_q(x) = \frac{x^p - 1}{x^q - 1}.
\]

Using this in (6) we obtain the explicit formula (1) referred to in the introduction.

**Addendum. Bibliography on Cyclotomic Polynomials.** This bibliography updates the list of references on cyclotomic polynomials which appears in Chapter II of the report by Dickson et al. in [1], and fills a gap (entry [2]). The titles, which are listed chronologically, were obtained from Fortschritte der Mathematik, Zentralblatt für Mathematik, and Mathematical Reviews. References to these review journals are indicated by F, Z, or MR, respectively. Except for Storer's

Mathematics Department
California Institute of Technology
Pasadena, California 91125


2. J. PETERSEN, *On the Sum of Quadratic Residues and the Distribution of Prime Numbers of the form $4n + 3$*, Anniversary Volume, University of Copenhagen, 1907. (Danish)


27. W. KLOBE, “Über eine untere Abschätzung der $n$-ten Kreisteilungspolynome $g_n(z) = \prod_{d|n} (z^{d} - 1)^{\mu(n/d)}$,” J. Reine Angew. Math., v. 187, 1949, pp. 68–69. [MR 11, p. 417.]
41. J. VAN DE VOOREN-VAN VEN, “On the number of irreducible equations of degree $n$ in $GF(p)$ and the decomposability of the cyclotomic polynomials in $GF(p)$,” Simon Stevin, v. 31, 1957, pp. 80–82. (Dutch) [MR 18, p. 787.]


60. DAVID ZEITLIN, "On coefficient identities for cyclotomic polynomials \( F_{pq}(x) \)," *Amer. Math. Monthly*, v. 75, 1968, pp. 976–980. [MR 38 #4446.]


68. SISTER CHRISTELLE THEUSCH, "Composition of \( \Phi_3(X) \) modulo \( m \)," *Fibonacci Quart.*, v. 9, 1971, pp. 23–27. [MR 44 #1623.]


