MATHEMATICS OF COMPUTATION, VOLUME 29, NUMBER 129
JANUARY 1975, PAGES 1–6

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

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

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

Received March 18, 1974.
AMS (MOS) subject classifications (1970). Primary 10A40; Secondary 12A20.
Key words and phrases. Cyclotomic polynomials, resultants.

$$\rho(F_q(ax), F_p(bx)) = \frac{a^{pq} - b^{pq}}{a^p - b^p} \frac{a - b}{a^q - b^q} \quad \text{if } a \neq b, \tag{1}$$
$$= a^{(p-1)(q-1)} \quad \text{if } a = b.$$

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*

$$\rho(F_m(ax), F_n(bx)) = b^{\varphi(m)\varphi(n)} \prod_{d|n} F_{m/\delta}\left(\frac{a^d}{b^d}\right)^{\mu(n/d)\varphi(m)/\varphi(m/\delta)}, \tag{2}$$

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

$$F_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)}$$

we find, as in [64, Section 4],

$$\rho(F_m(ax), F_n(bx)) = \prod_{d|n} f(d)^{\mu(n/d)}, \tag{3}$$

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

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

In the last exponential we write

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

and then use the Lemma on p. 457 of [64] to obtain

$$f(d) = b^{d\varphi(m)} \prod_{k=1}^{m/\delta}{}' \left(\frac{a^d}{b^d} - e^{2\pi i k/(m/\delta)}\right)^{\varphi(m)/\varphi(m/\delta)}$$
$$= b^{d\varphi(m)} F_{m/\delta}\left(\frac{a^d}{b^d}\right)^{\varphi(m)/\varphi(m/\delta)}.$$

Using this in (3) along with the relation $\Sigma_{d/n}\, d\mu(n/d) = \varphi(n)$, 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*

$$\rho(F_m(ax), F_n(bx)) = b^{\varphi(mn)} \prod_{d|n} F_m\left(\frac{a^d}{b^d}\right)^{\mu(n/d)}. \tag{4}$$

Next, we take $n = p^\alpha$ where p is prime, $p \nmid m$, and $\alpha \geqslant 1$. 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]

$$F_m(x^{p^\alpha})/F_m(x^{p^{\alpha-1}}) = F_{mp^\alpha}(x), \tag{5}$$

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* $\alpha \geqslant 1$ *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 $m = q$, where q is a prime $\neq p$, to obtain:

THEOREM 4. *If* p *and* q *are distinct primes and* $ab \neq 0$, *we have*

$$\rho(F_q(ax), F_p(bx)) = b^{(p-1)(q-1)} F_{pq}(a/b). \tag{6}$$

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

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

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 jornals are indicated by F, Z, or MR, respectively. Except for Storer's

book [55], works on cyclotomy and cyclotomic fields are not listed.

Several textbooks on Algebra and Number Theory discuss cyclotomic polynomials, for example, N. Tschebotaröw and H. Schwerdtfeger, *Grundzüge der Galois'schen Theorie,* P. Noordhoff, Groningen, 1950; Trygve Nagell, *Introduction to Number Theory*, John Wiley and Sons, New York, 1951; Hans Rademacher, *Lectures on Elementary Number Theory*, Blaisdell, New York, 1964.

Mathematics Department
California Institute of Technology
Pasadena, California 91125

1. L. E. DICKSON, H. H. MITCHELL, H. S. VANDIVER & G. E. WAHLIN, *Algebraic Numbers*, Bulletin of the National Research Council, vol. 5, part 3, #28, National Academy of Sciences, 1923.

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)

3. E. JACOBSTHAL, "Fibonaccische Polynome und Kreisteilungsgleichungen," *Sitzungsber. Ber. Math. Ges.*, v. 17, 1919/20, pp. 43–51. [F **47**, p. 109.]

4. P. O. UPADHYAYA, "A general theorem for the representation of X, where X represents the polynomial $(x^p - 1)/(x - 1)$," *Calcutta Math. Soc. Bull.*, v. 14, 1923, pp. 41–54. [F **49**, p. 51.]

5. K. GRANDJOT, "Über die Irreduzibilität der Kreisteilungsgleichung," *Math. Z.*, v. 19, 1924, pp. 128–129. [F **49**, p. 51.]

6. H. SPATH, "Über die Irreduzibilität der Kreisteilungsgleichung," *Math. Z.*, v. 26, 1926, p. 442. [F **53**, p. 999.]

7. E. LANDAU, "Über die Irreduzibilität der Kreisteilungsgleichung," *Math. Z.*, v. 29, 1929, p. 462. [F **54**, p. 123.]

8. I. SCHUR, "Zur Irreduzibilität der Kreisteilungsgleichung," *Math. Z.*, v. 29, 1929, p. 463. [F **54**, p. 123.]

9. EMMA LEHMER, "A numerical function applied to cyclotomy," *Bull. Amer. Math. Soc.*, v. 36, 1930, pp. 291–298. [F **56**, p. 861.]

10. FRIEDRICH HARTMANN, "Miszellen zur Primzahltheorie. I," *Jber. Deutsch. Math.-Verein.*, v. 40, 1931, pp. 228–232. [F **57**, p. 185.]

11. FRIEDRICH HARTMANN, "Miszellen zur Primzahltheorie. II," *Jber. Deutsch. Math.-Verein.*, v. 42, 1932, pp. 135–141. [Z **6**, p. 10.]

12. D. H. LEHMER, "Quasi-cyclotomic polynomials," *Amer. Math. Monthly*, v. 39, 1932, pp. 383–389. [Z **5**, p. 193.]

13. D. H. LEHMER, "Factorization of certain cyclotomic functions," *Ann. of Math.* (2), v. 34, 1933, pp. 461–479. [Z **7**, p. 199.]

14. JOSEF PLEMELJ, "Die Irreduzibilität der Kreisteilungsgleichung," *Publ. Math. Univ. Belgrade*, v. 2, 1933, pp. 164–165. [Z **8**, p. 388.]

15. ROLF BUNGERS, *Über die Koeffizienten von Kreisteilungspolynomen*, Dissertation, Göttingen, 1934, 15 S. [Z **9**, p. 102.]

16. FRIEDRICH LEVI, "Zur Irreduzibilität der Kreisteilungspolynome," *Compositio Math.*, v. 1, 1934, pp. 303–304. [Z **9**, p. 100.]

17. EMMA LEHMER, "On the magnitude of the coefficients of the cyclotomic polynomial," *Bull. Amer. Math. Soc.*, v. 42, 1936, pp. 389–392. [Z **14**, p. 392.]

18. O. HÖLDER, "Zur Theorie der Kreisteilungsgleichung $K_m(x) = 0$," *Prace Mat. Fiz.*, v. 43, 1936, pp. 13–23. [Z **13**, p. 5.]

19. HEINRICH TOEPKEN, "Zur Irreduzibilität der Kreisteilungsgleichung," *Deutsche Math.*, v. 2, 1937, pp. 631–633. [Z **18**, p. 99.]

20. J. E. EATON, "A formula for the coefficients of the cyclotomic polynomial," *Bull. Amer. Math. Soc.*, v. 45, 1939, pp. 178–186. [Z **20**, p. 289.]

21. FRITZ-ERDMANN DIEDERICHSEN, "Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz," *Abh. Math. Sem. Hanisches Univ.*, v. 13, 1940, pp. 357–412. [Z 23, p. 13.]

22. HANS-JOACHIM KANOLD, "Untersuchungen über ungerade vollkommene Zahlen," *J. Reine Angew. Math.*, v. 183, 1941, pp. 98–109. [MR 3, p. 268.]

23. T. VIJAYARAGHAVAN & S. CHOWLA, "The complete factorization (mod p) of the cyclotomic polynomial of order $p^2 - 1$," *Proc. Nat. Acad. Sci. India Sect. A*, v. 14, 1944, pp. 101–105. [MR 7, p. 273.]

24. PAUL ERDÖS, "On the coefficients of the cyclotomic polynomial," *Bull. Amer. Math. Soc.*, v. 52, 1946, pp. 179–184. [MR 7, p. 242.]

25. HANS-JOACHIM KANOLD, "Kreisteilungspolynome und ungerade vollkommene Zahlen," *Ber. Math.-Tagung Tübingen*, v. 1946, pp. 84–87. [MR 9, p. 78.]

26. P. T. BATEMAN, "Note on the coefficients of the cyclotomic polynomial," *Bull. Amer. Math. Soc.*, v. 55, 1949, pp. 1180–1181. [MR **11**, p. 329.]

27. W. KLOBE, "Über eine untere Abschätzung der n-ten Kreisteilungspolynome $g_n(z) = \Pi_{d|n}(z^d - 1)^{\mu(n/d)}$," *J. Reine Angew. Math.*, v. 187, 1949, pp. 68–69. [MR **11**, p. 417.]

28. PAUL ERDÖS, "On the coefficients of the cyclotomic polynomial," *Portugal. Math.*, v. 8, 1949, pp. 63–71. [MR **12**, p. 11.]

29. HANS-JOACHIM KANOLD, "Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme. I," *J. Reine Angew. Math.*, v. 187, 1950, pp. 169–182. [MR **12**, p. 592.]

30. HANS-JOACHIM KANOLD, "Sätze über Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme. II," *J. Reine Angew. Math.*, v. 188, 1950, pp. 129–146. [MR **13**, p. 443.]

31. L. REDÉI, "Ein Beitrag zum Problem der Faktorisation von endlichen Abelschen Gruppen," *Acta Math. Acad. Sci. Hungar.*, v. 1, 1950, pp. 197–207. [MR **13**, p. 623.]

32. N. G. W. H. BEEGER, "On a new quadratic form for certain cyclotomic polynomial," *Nieuw Arch. Wisk.*, v. 23, 1951, pp. 249–252. [MR **13**, p. 211.]

33. HANS-JOACHIM KANOLD, "Abschätzungen bei Kreisteilungspolynomen und daraus hergeleitete Bedingungen für die kleinsten Primzahlen gewisser arithmetischer Folgen," *Math. Z.*, v. 55, 1952, pp. 284–287. [MR **14**, p. 728.]

34. N. G. DeBRUIJN, "On the factorization of finite abelian groups," *Nederl. Akad. Wetensch. Proc. Ser. A*, v. 56 = *Indag. Math.*, v. 15, 1953, pp. 370–377. [MR **15**, p. 503.]

35. L. CARLITZ, "Note on the cyclotomic polynomial," *Amer. Math. Monthly*, v. 61, 1954, pp. 106–108. [MR **15**, p. 508.]

36. LADISLAUS RÉDEI, "Über das Kreisteilungspolynom," *Acta Math. Acad. Sci. Hungar.*, v. 5, 1954, pp. 27–28. [MR **16**, p. 13.]

37. MORGAN WARD, "Cyclotomy and the converse of Fermat's theorem," *Amer. Math. Monthly*, v. 61, 1954, p. 564. [MR **16**, p. 115.]

38. ROBERT BALLIEU, "Factorisation des polynomes cyclotomiques modulo un nombre premier," *Ann. Soc. Sci. Bruxelles Sér. I*, v. 68, 1954, pp. 140–144. [MR **16**, p. 570.]

39. HANS PETERSSON, "Über eine Zerlegung des Kreisteilungspolynoms von Primzahlordnung," *Math. Nachr.*, v. 14, 1955, pp. 361–375. [MR **18**, p. 867.]

40. PAUL ERDÖS, "On the growth of the cyclotomic polynomial in the interval (0, 1)," *Proc. Glasgow Math. Assoc.*, v. 3, 1957, pp. 102–104. [MR **19**, p. 1039.]

41. J. VAN DE VOOREN-VAN VEEN, "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.]

42. ERNST JACOBSTHAL, "Zur Theorie der Einheitswurzeln. I," *Norske Vid. Selsk. Forh.*, v. 31, 1958, pp. 125–129. [MR 23 #A1583.]

43. ERNST JACOBSTHAL, "Zur Theorie der Einheitswurzeln. II," *Norske Vid. Selsk. Forh.*, v. 31, 1958, pp. 130–137. [MR 23 #A1584.]

44. MORGAN WARD, "Tests for primality based on Sylvester's cyclotomic numbers," *Pacific J. Math.*, v. 9, 1959, pp. 1269–1272. [MR **21** #7180.]

45. L. K. DURST, "The growth of Sylvester's cyclotomic numbers," *Duke Math. J.*, v. 29, 1962, pp. 447–454. [MR **25** #3889.]

46. L. MIRSKY, "A note on cyclotomic polynomials," *Amer. Math. Monthly*, v. 69, 1962, pp. 772–775. [MR **27** #2473.]

47. WALTER FEIT & JOHN G. THOMPSON, "Solvability of groups of odd order," *Pacific J. Math.*, v. 13, 1963, pp. 775–1029. [MR **29** #3538.]

48. SISTER MARION BEITER, "The midterm coefficient of the cyclotomic polynomial $F_{pq}(x)$," *Amer. Math. Monthly*, v. 71, 1964, pp. 769–770. [Z **125**, p. 8.]

49. HELEN HABERMEHL, SHARON RICHARDSON & MARY ANN SZWAJKOS, "A note on coefficients of cyclotomic polynomials," *Math. Mag.*, v. 37, 1964, pp. 183–185. [Z **122**, p. 254.]

50. I. J. SCHOENBERG, "A note on the cyclotomic polynomial," *Mathematika*, v. 11, 1964, pp. 131–136. [MR **30** #1122.]

51. HENRY B. MANN, "On linear relations between roots of unity," *Mathematika*, v. 12, 1965, pp. 107–117. [MR **33** #119.]

52. K. E. KLOSS, "Some number-theoretic calculations," *J. Res. Nat. Bur. Standards Sect. B*, v. 69B, 1965, pp. 335–336. [MR **32** #7473.]

53. L. CARLITZ, "The number of terms in the cyclotomic polynomial $F_{pq}(x)$," *Amer. Math. Monthly*, v. 73, 1966, pp. 979–981. [MR **34** #2517.]

54. D. H. LEHMER, "Some properties of the cyclotomic polynomial," *J. Math. Anal. Appl.*, v. 15, 1966, pp. 105–117. [MR **33** #5606.]

55. THOMAS STORER, *Cyclotomy and Difference Sets*, Markham, Chicago, Ill., 1967. [MR **36** #128.]

56. L. CARLITZ, "The sum of the squares of the coefficients of the cyclotomic polynomial," *Acta Math. Acad. Sci. Hungar.*, v. 18, 1967, pp. 295–302. [MR **36** #139.]

57. SISTER MARION BEITER, "Magnitude of the coefficients of the cyclotomic polynomial $F_{pqr}(x)$," *Amer. Math. Monthly*, v. 75, 1968, pp. 370–372. [MR **37** #2670.]

58. D. M. BLOOM, "On the coefficients of the cyclotomic polynomials," *Amer. Math. Monthly*, v. 75, 1968, pp. 372–377. [MR **37** #2671.]

59. KAU-UN LU, *Some Properties of the Coefficients of Cyclotomic Polynomials*, Ph. D. Thesis, California Institute of Technology, 1968.

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

61. VOLKMAR FELSCH & ECKART SCHMIDT, "Über Perioden in den Koeffizienten der Kreisteilungspolynome $F_{np}(x)$," *Math. Z.*, v. 106, 1968, pp. 267–272. [MR **38** #1080.]

62. JACQUES JUSTIN, "Bornes des coefficients du polynôme cyclotomique et de certains autres polynômes," *C. R. Acad. Sci. Paris Sér. A*, v. 268, 1969, pp. A995–A997. [MR **39** #2692.]

63. HERBERT MÖLLER, "Über die i-ten Koeffizienten der Kreisteilungspolynome," *Math. Ann.*, v. 188, 1970, pp. 26–38. [MR **42** #1801.]

64. TOM M. APOSTOL, "Resultants of cyclotomic polynomials," *Proc. Amer. Math. Soc.*, v. 24, 1970, pp. 457–462. [MR **40** #4241.]

65. WAYNE L. McDANIEL, "The nonexistence of odd perfect numbers of a certain form," *Arch. Math. (Basel)*, v. 21, 1970, pp. 52–53. [MR **41** #3369.]

66. HERBERT MÖLLER, "Über die Koeffizienten des n-ten Kreisteilungspolynoms," *Math. Z.*, v. 119, 1971, pp. 33–40. [MR **43** #148.]

67. MARION BEITER, "Magnitude of the coefficients of the cyclotomic polynomial F_{pqr}. II," *Duke Math. J.*, v. 38, 1971, pp. 591–594. [MR **43** #6152.]

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

69. N. M. STEPHENS, "On the Feit-Thompson conjecture," *Math. Comp.*, v. 25, 1971, p. 625. [MR **45** #6738.]

70. BERND RICHTER, "Die Primfaktorzerlegung der Werte der Kreisteilungspolynome," *J. Reine Angew. Math.*, v. 254, 1972, pp. 123–132. [MR **46** #1764.]

71. WAYNE L. McDANIEL, "On multiple prime divisors of cyclotomic polynomials," *Math. Comp.*, v. 28, 1974, pp. 847–850.

Added in proof. For further papers on cyclotomic polynomials, see

WILLIAM J. LeVEQUE, *Reviews in Number Theory*, Vol. 1, Amer. Math. Soc., Providence, R. I., 1974, pp. 404–411.