PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 123, Number 4, April 1995

RESULTANTS OF CYCLOTOMIC POLYNOMIALS

CHARLES CHING-AN CHENG, JAMES H. MCKAY, AND STUART SUI-SHENG WANG

(Communicated by William Adams)

ABSTRACT. A formula for $\operatorname{Res}_x(\Phi_a(x^b), \Phi_c(x^d))$ is given where $\Phi_a(x)$ denotes the a^{th} cyclotomic polynomial. This extends a result of Lehmer, Diederichsen, and Apostol.

The n^{th} *cyclotomic polynomial*, $n \geqslant 1$, is defined by

$$\Phi_n(x) = \prod (x - e^{2\pi ik/n})$$

where the product is over all values of k relatively prime to n such that $1 \leqslant k \leqslant n$. The polynomial $\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$ with degree $\varphi(n)$ where φ denotes the Euler phi-function. Lehmer [6], Diederichsen [4] and Apostol [1] have given formulas for $\operatorname{Res}_x(\Phi_m(x), \Phi_n(x))$. Later Apostol [2] extended it to a formula for $\operatorname{Res}_x(\Phi_m(ax), \Phi_n(bx))$ with the hope to shorten the 255-page proof of the celebrated Feit-Thompson Theorem [5]. In this paper we derive a formula for $\operatorname{Res}_x(\Phi_a(x^b), \Phi_c(x^d))$ extending the result of Lehmer, Diederichsen, and Apostol. In doing so, we first factorize $\Phi_a(x^b)$ in $\mathbb{Z}[x]$ followed by an application of the chain rule for resultants.

Throughout this paper, (a, b) will denote the greatest common divisor, and $[a, b]$ the least common multiple, of positive integers a and b. We also use the notation $a|b$ to indicate that a divides b.

1. REDUCTIONS

Lemma 1 (Factorization). *For positive integers a and b,*

$$\Phi_a(x^b) = \prod_{[m,b]=ab} \Phi_m(x). \tag{1.1}$$

Proof. Note that if θ is an element of a group, then the order of θ^b is given by

$$\operatorname{Ord}(\theta^b) = \frac{\operatorname{Ord}(\theta)}{(\operatorname{Ord}(\theta), b)} = \frac{[\operatorname{Ord}(\theta), b]}{b}.$$

Hence θ is a zero of $\Phi_a(x^b)$ $\iff$ $\operatorname{Ord}(\theta^b) = a$ $\iff$ $[\operatorname{Ord}(\theta), b] = ab$. Since $\Phi_a(x^b)$ has no multiple zeros, the left side of (1.1) divides the right

Received by the editors July 27, 1993.

1991 *Mathematics Subject Classification*. Primary 11B83, 12E10; Secondary 11R09, 11R18, 12D05.

Key words and phrases. Resultant, cyclotomic polynomial, chain rule for resultants.

side. On the other hand, if θ is a zero of $\Phi_m(x)$ where $[m, b] = ab$, then $\mathrm{Ord}(\theta) = m$ and so θ is a zero of $\Phi_a(x^b)$. Since cyclotomic polynomials are relatively prime with no multiple zeros, the right side of (1.1) divides the left side. Now the result follows from the fact that both sides of (1.1) are monic. □

Corollary 2. *Suppose* $(a, b) = 1$. *Then*

$$\Phi_a(x^b) = \prod_{s \text{ divides } b} \Phi_{as}(x).$$

Proof. Apply Lemma 1 and observe that if $(a, b) = 1$, then $[m, b] = ab \iff m = as$ for some divisor s of b. □

Let a be a positive integer. For any prime p, let $v_p(a)$ denote the largest integer k such that p^k divides a. Thus $a = \prod p^{v_p(a)}$ where the product is indexed by all primes p. If b is another positive integer, then $v_p(ab) = v_p(a) + v_p(b)$. We also define

$$\langle a, b\rangle = \prod_{v_p(a)>0} p^{v_p(ab)},$$

with the understanding that an empty product is 1 so that $\langle 1, b\rangle = 1$. Note that

$$v_p(\langle a, b\rangle) = \begin{cases} v_p(ab) & \text{if } v_p(a) > 0, \\ 0 & \text{if } v_p(a) = 0; \end{cases}$$

and therefore

$$v_p\left(\frac{ab}{\langle a, b\rangle}\right) = \begin{cases} 0 & \text{if } v_p(a) > 0, \\ v_p(ab) & \text{if } v_p(a) = 0. \end{cases} \tag{1.2}$$

Corollary 3.

$$\Phi_a(x^b) = \Phi_{\langle a, b\rangle}(x^{\frac{ab}{\langle a, b\rangle}}).$$

Proof. Express both sides as products using Lemma 1. Then observe that

$$[m, b] = ab \iff \left[m, \frac{ab}{\langle a, b\rangle}\right] = ab$$

by applying v_p to both and using (1.2). □

Lemma 4 (Chain Rule for Resultants [7, Corollary 11, p. 360], [3]). *Suppose* $f_1, f_2, h \in \mathbb{Z}[x]$ *and the leading term of* h *is* x^t. *Then*

$$\mathrm{Res}_x(f_1(h), f_2(h)) = [\mathrm{Res}_x(f_1, f_2)]^t. \quad \square$$

Corollary 5. $\mathrm{Res}_x(\Phi_a(x^b), \Phi_c(x^d)) = [\mathrm{Res}_x(\Phi_a(x^{b'}), \Phi_c(x^{d'}))]^g$ *where* $g = (b, d)$, $b = gb'$, *and* $d = gd'$.

Proof. Apply Lemma 4 with $f_1 = \Phi_a(x^{b'})$, $f_2 = \Phi_c(x^{d'})$, and $h = x^g$. □

Thus in calculating $\mathrm{Res}_x(\Phi_a(x^b), \Phi_c(x^d))$, it is sufficient to assume that $(b, d) = 1$. Furthermore, by Corollary 3, we may assume that $(a, b) = (c, d) = 1$. This is done in the next section.

The next lemma is a standard property of resultants [8, Chapter 5, Section 9, (5.24), p. 106].

Lemma 6. *Suppose* f_1, $f_2 \in \mathbb{Z}[x]$. *Then*

$$\operatorname{Res}_x(f_1(x), f_2(x)) = (-1)^{\deg f_1 \times \deg f_2} \operatorname{Res}_x(f_2(x), f_1(x)). \quad \square$$

Corollary 7.

$$\operatorname{Res}_x(\Phi_a(x^b), \Phi_c(x^d)) = (-1)^{\varphi(a)b\varphi(c)d} \operatorname{Res}_x(\Phi_c(x^d), \Phi_a(x^b)). \quad \square$$

2. Special case

Assume throughout this section that $(a, b) = (c, d) = (b, d) = 1$ and $S = \{s: s|b\}$, $T = \{t: t|d\}$.

Using Corollary 2 and the bi-multiplicative property of the resultant, we have

$$R = \operatorname{Res}_x(\Phi_a(x^b), \Phi_c(x^d)) = \prod_{(s,t)\in S\times T} \operatorname{Res}_x(\Phi_{as}(x), \Phi_{bt}(x)). \tag{2.1}$$

Lemma 8 (Lehmer [6], Diederichsen [4], Apostol [1]). *Suppose* $m \geqslant n \geqslant 1$. *Then*

$$\operatorname{Res}_x(\Phi_n(x), \Phi_m(x)) = \begin{cases} 0 & \textit{if } m = n, \\ p^{\varphi(n)} & \textit{if } \frac{m}{n} = p^e, \textit{ a prime power}, \\ 1 & \textit{otherwise.} \quad \square \end{cases}$$

Note that $\operatorname{Res}_x(\Phi_m(x), \Phi_n(x)) = (-1)^{\varphi(m)\varphi(n)} \operatorname{Res}_x(\Phi_n(x), \Phi_m(x))$ by Lemma 6. Hence the only case that $\operatorname{Res}_x(\Phi_m(x), \Phi_n(x))$ is negative is when $m = 2$ and $n = 1$. In fact, $\operatorname{Res}_x(\Phi_2(x), \Phi_1(x)) = -2$.

Lemma 9. $R = 0 \iff a|cd$ *and* $c|ab$.

Proof. By (2.1) and Lemma 8, $R = 0 \iff as = ct$ for some $s \in S$ and some $t \in T$. Therefore, we have to show that $as = ct \iff a|cd$ and $c|ab$.

$\Longrightarrow$: The hypothesis $as = ct$ implies $a|ct|cd$ and $c|as|ab$.

$\Longleftarrow$: The hypothesis $a|cd$, together with $(c, d) = 1$, implies $a = (a, cd) = (a, c)(a, d)$. Similarly, the hypothesis $c|ab$, together with $(a, b) = 1$, implies $c = (a, c)(b, c)$. Let $s = (b, c)$ and $t = (a, d)$. Then $s \in S$, $t \in T$ and $as = (a, d)(a, c)(b, c) = tc$. $\square$

Lemma 10. *If there exist* $s_1, s_2 \in S$ *and* $t_1, t_2 \in T$ *such that both* $\frac{as_1}{ct_1}$ *and* $\frac{ct_2}{as_2}$ *are integers, then* $R = 0$.

Proof. The hypothesis that $\frac{as_1}{ct_1}$ is an integer implies that c divides as_1, hence ab. Likewise, a divides cd. Now the result follows from Lemma 9. $\square$

Using Lemma 8 we see that if $R \neq 0$, then the product in (2.1) can be indexed by $(s, t) \in S \times T$ such that $\frac{as}{ct}$ or $\frac{ct}{as}$ is a prime power. Lemma 10 then guarantees that the indexing set is either all $(s, t) \in S \times T$ with $\frac{as}{ct}$ a prime power, or all $(s, t) \in S \times T$ with $\frac{ct}{as}$ a prime power. Without loss of generality, we may assume the former. The next lemma shows that the prime p involved is unique.

Lemma 11. *Suppose* $R \neq 0$ *and furthermore* $\frac{as_1}{ct_1} = p_1^{e_1}$ *and* $\frac{as_2}{ct_2} = p_2^{e_2}$ *where* $s_1, s_2 \in S$, $t_1, t_2 \in T$, p_1 *and* p_2 *are primes, and* $e_1, e_2 \geqslant 1$. *Then* $p_1 = p_2$.

Proof. If $p_1 \neq p_2$, then $\frac{p_1^{e_1} s_2(\frac{d}{t_2})}{p_2^{e_2}} = s_1(\frac{d}{t_1})$ and so $p_2^{e_2}$ divides $s_2(\frac{d}{t_2})$. Then $\frac{s_2(\frac{d}{t_2})}{p_2^{e_2}} = \frac{cd}{a}$ shows that a divides cd. On the other hand, by hypothesis, c

divides as_1, hence ab. So by Lemma 9, $R = 0$, a contradiction. Thus $p_1 = p_2$. □

Lemma 12. *Suppose $R \neq 0$ and suppose for some $s \in S$, $t \in T$, $\frac{ct}{as} = p^e$ is a prime power. Then $t = (a, d)$.*

Proof. Since $(c, t) = 1$ and $\frac{ct}{p^e} = as$, it follows that p^e divides either c or t but not both. Note that p^e does not divide t. For otherwise $\frac{t}{p^e} = \frac{as}{c}$ implies that $c|as$ and so $c|ab$. However, $a|cd$ since $a|ct$ by hypothesis. Thus we have $R = 0$ by Lemma 9, a contradiction. Hence $p^e|c$. Thus $\frac{c}{p^e} = \frac{as}{t}$ implies $t|as$ and so $t|a$ since $(s, t) = 1$. Thus $t|(a, d)$. On the other hand, $a = (a, cd) = (a, c)(a, d)$ since $a|cd$ and $(c, d) = 1$. Hence $a|ct$ is equivalent to $(a, c)(a, d)|ct$. Now this implies that $(a, d)|ct$ and thus $(a, d)|t$ since c and (a, d) are relatively prime. Thus $t = (a, d)$. □

Lemma 13. *Suppose $R \neq 0$. Then the following conditions are equivalent.*

(1) *There exist $s \in S$, $t \in T$ such that $\frac{ct}{as} = p^{e'}$ is a prime power.*

(2) *$a|cd$ and $\frac{c(a,d)}{(ab,cd)} = p^e$ is a prime power.*

Furthermore, if (1) *is true then the set of all s satisfying the equality in* (1) *consists of*

$$(b, \frac{cd}{a}), \frac{(b, \frac{cd}{a})}{p}, \frac{(b, \frac{cd}{a})}{p^2}, \dots, \frac{(b, \frac{cd}{a})}{p^u},$$

where $u = v_p(b, \frac{cd}{a}) = v_p(ab, cd) - v_p(a)$.

Proof. (2) $\Longrightarrow$ (1). Take $s = (b, \frac{cd}{a})$, $t = (a, d)$, and $e' = e$.

(1) $\Longrightarrow$ (2). By Lemma 12, we have $\frac{cd}{as} = \frac{d}{(a,d)}p^{e'}$ which shows that $a|cd$ and $s|\frac{cd}{a}$. Hence $s|(b, \frac{cd}{a})$. Therefore $\frac{c(a,d)}{(ab,cd)} = \frac{c(a,d)}{a(b,cd/a)}$ is a factor of $\frac{c(a,d)}{as} = p^{e'}$ and thus is equal to p^e for some $e \leqslant e'$. It remains to show that $e \geqslant 1$. However, $\frac{c(a,d)}{(ab,cd)} = 1$ implies $R = 0$ by Lemma 10, a contradiction. So $e \geqslant 1$.

From the above proof, we see that if s, t satisfy the equality in (1) then $t = (a, d)$ and $s|(b, \frac{cd}{a})$. Using (2) we also see that $s = (b, \frac{cd}{a})$, $t = (a, d)$ satisfy the equality in (1). If s_1 and s_2 both satisfy the equality in (1) then either $s_1 = p^{e''}s_2$ or $s_2 = p^{e''}s_1$. So the rest of the result follows. □

Proposition 14. *For each prime p, let $u(p) = v_p(ab, cd) - v_p(a)$ and $v(p) = v_p(ab, cd) - v_p(c)$. Then*

$$R = \begin{cases} 0 & \textit{if } a|cd \textit{ and } c|ab, \\ p^{\varphi(ab,cd)\frac{p^{u(p)}}{\varphi(p^{u(p)})}} & \textit{if } a|cd \textit{ and } \frac{c}{(c,ab)} = p^e, \textit{ a prime power}, \\ (-1)^{\varphi(a)\varphi(c)bd}p^{\varphi(ab,cd)\frac{p^{v(p)}}{\varphi(p^{v(p)})}} & \textit{if } c|ab \textit{ and } \frac{a}{(a,cd)} = p^e, \textit{ a prime power}, \\ 1 & \textit{otherwise}. \end{cases}$$

Proof. Note that

$$\frac{c(a, d)}{(ab, cd)} = \frac{c(a, d)}{(ab, c)(ab, d)} = \frac{c(a, d)}{(ab, c)(a, d)(b, d)} = \frac{c}{(ab, c)}.$$

Clearly, the conditions in the four cases are mutually exclusive. The first case follows from Lemma 9. To establish the second case, note that, by Lemmas 8 and 13,

$$R = \prod_{s \in S_1} p^{\varphi(as)} \tag{2.2}$$

where $S_1 = \left\{\frac{(b, cd/a)}{p^i} : i = 0, 1, \dots, u(p)\right\}$. Since $(a, s) = 1$,

$$\varphi(as) = \varphi(a)\varphi(s).$$

Thus the product of (2.2) equals $p^{\varphi(a)\sum_{s \in S_1} \varphi(s)}$. Setting $\bar{s} = \frac{(b, cd/a)}{p^u}$ where $u = u(p)$, and using the fact that $(\bar{s}, p) = 1$, we have

$$\begin{aligned}\sum_{s \in S_1} \varphi(s) &= \varphi(\bar{s}) + \varphi(\bar{s}p) + \cdots + \varphi(\bar{s}p^u) \\ &= \varphi(\bar{s})\left[1 + \varphi(p) + \cdots + \varphi(p^u)\right] \\ &= \varphi(\bar{s})\,p^u.\end{aligned}$$

Since $\bar{s}$ and p^u are relatively prime,

$$\varphi(\bar{s}) = \frac{\varphi(b, \frac{cd}{a})}{\varphi(p^u)}.$$

Hence

$$\varphi(a)\varphi(\bar{s}) = \varphi(a)\frac{\varphi(b, \frac{cd}{a})}{\varphi(p^u)} = \frac{\varphi(ab, cd)}{\varphi(p^u)}$$

since a and $(b, \frac{cd}{a})$ are relatively prime. The third case follows from Corollary 7 and the second case. □

3. The main theorem

Throughout this section, let $R = \mathrm{Res}_x(\Phi_a(x^b), \Phi_c(x^d))$.

Proposition 15. *Suppose $(a, b) = (c, d) = 1$. Let $g = (b, d)$, and, for each prime p, $u(p) = v_p(ab, cd) - v_p(a)$, $v(p) = v_p(ab, cd) - v_p(c)$. Then*

$$R = \begin{cases} 0 & \text{if } a|cd \text{ and } c|ab, \\ p^{\varphi(ab, cd)\frac{p^{u(p)}}{\varphi(p^{u(p)})}\frac{g}{\varphi(g)}} & \text{if } a|cd \text{ and } \frac{c}{(c, ab)} = p^e, \text{ a prime power,} \\ (-1)^{\varphi(a)\varphi(c)bd}p^{\varphi(ab, cd)\frac{p^{v(p)}}{\varphi(p^{v(p)})}\frac{g}{\varphi(g)}} & \text{if } c|ab \text{ and } \frac{a}{(a, cd)} = p^e, \text{ a prime power,} \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Using Corollary 5 and Lemma 16, we see that the result follows from Corollary 7 and Proposition 14. □

Lemma 16. *Let $g = (a, b)$, $b = b'g$, and $d = d'g$. Suppose $(a, b) = (c, d) = 1$. Then*

(1) $a|cd \iff a|cd'$.
(2) $c|ab \iff c|ab'$.

(3) $\frac{a}{(a,cd)} = \frac{a}{(a,cd')}$.

(4) $\frac{c}{(c,ab)} = \frac{c}{(c,ab')}$.

(5) $\varphi(ab, cd) = \varphi(ab', cd')\varphi(g)$.

(6) *If* $\frac{a}{(a,cd)} = p^e$, *a prime power, then* $v_p(ab, cd) - v_p(c) = v_p(ab', cd') - v_p(c)$.

(7) *If* $\frac{c}{(c,ab)} = p^e$, *a prime power, then* $v_p(ab, cd) - v_p(a) = v_p(ab', cd') - v_p(a)$.

Proof. (1) Since $(a, b) = 1$, $(a, g) = 1$. Hence $a|cd'g \iff a|cd'$.

(2) Similar to (1).

(3) Since $(a, b) = 1$, $(a, g) = 1$. So $(a, cd) = (a, cd'g) = (a, cd')(a, g)$.

(4) Similar to (3).

(5) Since $(a, b) = (c, d) = 1$, it follows that $(a, g) = (c, g) = 1$. Hence (ab', cd') and g are relatively prime.

(6) Since $p|a$ and $(a, g) = 1$, $v_p(g) = 0$. So $v_p(ab, cd) = v_p(ab', cd') + v_p(g) = v_p(ab', cd')$.

(7) Similar to (6). □

Using Corollary 3, we deduce the main result of the paper below from Corollary 7 and Proposition 15.

Theorem 17. *Let*

$$g = \left(\frac{ab}{\langle a, b\rangle}, \frac{cd}{\langle c, d\rangle}\right),$$

and for each prime p, *let* $u(p) = v_p(ab, cd) - v_p(\langle a, b\rangle)$, $v(p) = v_p(ab, cd) - v_p(\langle c, d\rangle)$, *and* $R = \mathrm{Res}_x(\Phi_a(x^b), \Phi_c(x^d))$. *Then*

$$R = \begin{cases} 0 & \text{if } \langle a, b\rangle | cd \text{ and } \langle c, d\rangle | ab, \\ p^{\varphi(ab,cd)\frac{p^{u(p)}}{\varphi(p^{u(p)})}\frac{g}{\varphi(g)}} & \text{if } \langle a, b\rangle | cd \text{ and } \frac{\langle c,d\rangle}{(\langle c,d\rangle, ab)} = p^e, \\ & \text{a prime power,} \\ (-1)^{\varphi(a)\varphi(c)bd} p^{\varphi(ab,cd)\frac{p^{v(p)}}{\varphi(p^{v(p)})}\frac{g}{\varphi(g)}} & \text{if } \langle c, d\rangle | ab \text{ and } \frac{\langle a,b\rangle}{(\langle a,b\rangle, cd)} = p^e, \\ & \text{a prime power,} \\ 1 & \text{otherwise.} \quad \square \end{cases}$$

Remarks. 1. $\mathrm{Res}_x(\Phi_a(x^b), \Phi_c(x^d))$ is negative if and only if $a = 2$, $c = 1$, and b, d are odd. For this is only possible in the third case above, i.e., when $\varphi(a)\varphi(c)bd$ is odd, or equivalently, when b, d are odd and either $(a = 1, c = 2)$ or $(a = 2, c = 1)$. But when $a = 1$ and $c = 2$ we are in the second case.

2. Note that

$$\frac{p^u}{\varphi(p^u)} = \begin{cases} 1 & \text{if } u = 0, \\ \frac{p}{p-1} & \text{if } u \geqslant 1. \end{cases}$$

References

1. T. M. Apostol, *Resultants of cyclotomic polynomials*, Proc. Amer. Math. Soc. **24** (1970), 457–462, MR 40 #4241.

2. ———, *The resultant of the cyclotomic polynomials* $F_m(ax)$ *and* $F_n(bx)$, Math. Comp. **29** (1975), 1–6, MR 51 #3047.

3. C. C.-A. Cheng, J. H. McKay, and S. S.-S. Wang, *A chain rule for multivariable resultants*, Proc. Amer. Math. Soc. (to appear).

4. F.-E. Diederichsen, *Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetisher Äquivalenz*, Abh. Math. Sem. Hansischen Univ. **13** (1940), 357–412, MR 2, 4.

5. W. Feit and J. G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775–1029, MR 29 #3538.

6. E. Lehmer, *A numerical function applied to cyclotomy*, Bull. Amer. Math. Soc. **36** (1930), 291–298, Jbuch 56, 861.

7. J. H. McKay and S. S.-S. Wang, *A chain rule for the resultant of two homogeneous polynomials*, Arch. Math. **56** (1991), 352–361, MR 92a:12006.

8. B. L. van der Waerden, *Algebra, Volume 1*, Frederick Ungar Publishing Company, New York, 1970 (Translated from the 1966 7th German edition), MR 41 #8187a.

Department of Mathematical Sciences, Oakland University, Rochester, Michigan 48309-4401

E-mail address, C. C.-A. Cheng: `cheng@vela.acs.oakland.edu`
E-mail address, J. H. McKay: `mckay@vela.acs.oakland.edu`
E-mail address, S. S.-S. Wang: `swang@vela.acs.oakland.edu`