

Resultants of Cyclotomic Polynomials

Gregory Dresden
Washington & Lee University
dresdeng@wlu.edu

In this paper we present new and elementary proofs of two related lemmas about the cyclotomic polynomials $\Phi_n(x)$. The first lemma concerns their resultant.

Lemma 1 (Emma Lehmer, Diederichsen, Apostol). *For $0 < m < n$ integers, then*

$$\text{Res}(\Phi_m, \Phi_n) = \begin{cases} p^{\phi(m)} & \text{if } n/m \text{ is a power of a prime } p \\ 1 & \text{otherwise} \end{cases}$$

Since the above Lemma 1 was proved at least three separate times [1, 2, 5], we feel justified in offering a fourth proof, this time using very little machinery.

The second lemma of our paper involves linear combinations of cyclotomic polynomials.

Lemma 2 (Filaseta, Schinzel). *Let n and m be positive integers with $m < n$. Then, there exist polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ such that*

$$\Phi_n(x)u(x) + \Phi_m(x)v(x) = k \tag{1}$$

where k is equal to the prime p if $n/m = p^t$, and equal to 1 if not. This k is the smallest such positive integer that can be written in this manner.

Filaseta gave two proofs of Lemma 2 in his paper [3]. The first proof involved the cyclotomic extensions $\mathbb{Q}(\zeta_n)$, and the second proof (this one by Schinzel, via private communication to Filaseta) used Lemma 1 on the resultant of cyclotomic polynomials.

We proceed as follows. We begin with an independent proof of Lemma 2, using neither the cyclotomic extensions of Filaseta nor the resultants of Schinzel, but instead only elementary facts about cyclotomic polynomials. Along the way, we also give explicit formulas for the polynomials $u(x)$ and $v(x)$ in the statement of the lemma, something which has not been done before. We then use Lemma 2, along with some basic statements about determinants and resultants, to prove Lemma 1, thus establishing the equivalence of these two lemmas.

Proof of Lemma 2

We begin by reminding ourselves of some basic facts about cyclotomic polynomials, as seen in Filaseta's paper [3] and elsewhere.

Lemma 3. For p prime, then

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{if } p \mid n \\ \Phi_n(x^p)/\Phi_n(x) & \text{otherwise} \end{cases}$$

Two immediate consequences are:

1. $\Phi_{p^i n}(x)$ equals $\Phi_n(x^{p^i})$ if $p \mid n$, and equals $\Phi_n(x^{p^i})/\Phi_n(x^{p^{i-1}})$ if $p \nmid n$.
2. For $a, b \in \mathbb{Z}^+$, then $\Phi_{ab}(x) \mid \Phi_a(x^b)$.

Lemma 4. Let k be an integer > 1 . Then,

$$\Phi_k(1) = \begin{cases} p & \text{if } k = p^r \text{ for some } r \in \mathbb{Z}^+ \\ 1 & \text{otherwise} \end{cases}$$

We now proceed to give two lemmas that describe the exact polynomials $u(x)$, $v(x)$ that satisfy equation (1). Finally, we will establish that the k in equation (1) is indeed the smallest such positive integer, thus concluding the proof of Lemma 2.

Lemma 5. For $m < n$ positive integers with $m \mid n$, let

$$u(x) = \frac{\Phi_{n/m}(x^m)}{\Phi_n(x)} \quad v(x) = \frac{-(\Phi_{n/m}(x^m) - \Phi_{n/m}(1))}{\Phi_m(x)}$$

Then, $u(x)$ and $v(x)$ are both in $\mathbb{Z}[x]$, and

$$\Phi_n(x)u(x) + \Phi_m(x)v(x) = \begin{cases} p & \text{if } n/m = p^r \text{ for some } r \in \mathbb{Z}^+ \\ 1 & \text{otherwise} \end{cases}$$

Proof. By direct substitution, we note that $\Phi_n(x)u(x) + \Phi_m(x)v(x) = \Phi_{n/m}(1)$, and we appeal to Lemma 4 to establish the desired equality. We use Lemma 3 to show that $u(x)$ is in $\mathbb{Z}[x]$, and as for $v(x)$, we write it as

$$v(x) = \frac{x^m - 1}{\Phi_m(x)} \cdot \frac{-(\Phi_{n/m}(x^m) - \Phi_{n/m}(1))}{x^m - 1}$$

Now, $\Phi_m(x)$ divides $x^m - 1$, and since $x - 1$ divides $p(x) - p(1)$ for any polynomial p , then by substituting x^m for x , we have that $x^m - 1$ divides $p(x^m) - p(1)$. We can conclude that $v(x) \in \mathbb{Z}[x]$. \square

Lemma 6. For $m < n$ positive integers with $m \nmid n$, let $d = \gcd(m, n)$ and let s, t be positive integers such that $ns - mt = d$. If we now define

$$u(x) = \frac{x^{ns} - 1}{(x^d - 1)\Phi_n(x)} \quad v(x) = \frac{(-x^d)(x^{mt} - 1)}{(x^d - 1)\Phi_m(x)}$$

Then, $u(x)$ and $v(x)$ are both in $\mathbb{Z}[x]$, and

$$\Phi_n(x)u(x) + \Phi_m(x)v(x) = 1$$

Proof. By direct substitution, we note that

$$\Phi_n(x)u(x) + \Phi_m(x)v(x) = \frac{x^{ns} - 1 - x^{d+mt} + x^d}{x^d - 1}$$

and since $ns - mt = d$, then $x^{ns} = x^{d+mt}$, and the above fraction cancels to 1.

We now show that our functions $u(x)$ and $v(x)$ are indeed in $\mathbb{Z}[x]$. Beginning with $u(x)$, since $m < n$ then $d < n$, and so $\Phi_n(x)$ is not a factor of $x^d - 1$. However, both $\Phi_n(x)$ and $x^d - 1$ are factors of $x^{ns} - 1$, so we can conclude that $u(x) \in \mathbb{Z}[x]$. In the case of $v(x)$, we note that since $m \nmid n$ then $d < m$ and so $\Phi_m(x)$ is not a factor of $x^d - 1$. However, both $\Phi_m(x)$ and $x^d - 1$ are factors of $x^{mt} - 1$. \square

We conclude with:

Proof of Lemma 2. By Lemmas 5 and 6, we know that there exist $u(x)$ and $v(x)$ satisfying equation (1). It remains to show that the k is indeed the smallest such positive integer that can be so written. This is trivial for $k = 1$, so let us assume that n/m is a power of a prime. Suppose, then, that $n = p^j a$ and $m = p^i a$ with $0 < i < j$. (The case when $i = 0$ is nearly identical, and will not be discussed further.) Let C be a positive integer such that there exist $u(x), v(x) \in \mathbb{Z}[x]$ with

$$\Phi_{p^j a}(x)u(x) + \Phi_{p^i a}(x)v(x) = C.$$

Let us show that $p \mid C$. By Lemma 4, we can write the above equation as

$$\frac{\Phi_a(x^{p^j})}{\Phi_a(x^{p^{j-1}})}u(x) + \frac{\Phi_a(x^{p^i})}{\Phi_a(x^{p^{i-1}})}v(x) = C.$$

Now recall that $f(x^p) \equiv f(x)^p \pmod{p}$, so the above equation simplifies mod p to

$$\Phi_a(x)^{p^j - p^{j-1}}u(x) + \Phi_a(x)^{p^i - p^{i-1}}v(x) \equiv C \pmod{p}.$$

Since $\mathbb{Z}[x]/\langle p \rangle$ is a UFD, we conclude that $\Phi_a(x) \mid C$ and so $C \equiv 0 \pmod{p}$ as desired. \square

Proof. For f and g of degrees m and n respectively, consider the following detail of the matrix representation of $\text{Res}(f, g)$:

$$\text{Res}(f(x), g(x)) = \begin{vmatrix} f_m & f_{m-1} & f_{m-2} & \cdots & & \\ 0 & f_m & f_{m-1} & f_{m-2} & \cdots & \\ \vdots & & & & & \end{vmatrix}$$

The above determinant has n rows of coefficients of f and m rows (not shown) of coefficients of g . When we now consider $f(x^t)$ and $g(x^t)$, we realize that these polynomials will have the same coefficients as $f(x)$ and $g(x)$ but separated by $t - 1$ zeros. This implies the following type of structure (here, \mathbf{I} represents the t by t identity matrix):

$$\text{Res}(f(x^t), g(x^t)) = \begin{vmatrix} f_m & 0 & \cdots & 0 & f_{m-1} & 0 & \cdots \\ 0 & f_m & \cdots & 0 & 0 & f_{m-1} & \cdots \\ \vdots & & \ddots & \vdots & \vdots & & \ddots \\ 0 & 0 & \cdots & f_m & 0 & 0 & \cdots \\ & & & & f_m & 0 & \cdots \\ & & & & & & \ddots \end{vmatrix} = \begin{vmatrix} f_m \cdot \mathbf{I} & f_{m-1} \cdot \mathbf{I} & \cdots \\ & f_m \cdot \mathbf{I} & \cdots \\ & & \ddots \end{vmatrix}$$

As the above detail suggests, we can think of $\text{Res}(f(x^t), g(x^t))$ as the determinant of a block matrix where the individual entries, or blocks, are multiples of the t by t identity matrix \mathbf{I} . It is a nice result of linear algebra (see [4] or [7]) that the determinant of a block matrix equals the determinant of the original matrix, and a moment's thought will lead to the following expression for the determinant of the block matrix:

$$\text{Res}(f(x^t), g(x^t)) = |\text{Res}(f, g) \cdot \mathbf{I}| = \text{Res}(f, g)^t$$

□

Lemma 9. For n/m not the power of a prime, then $\text{Res}(\Phi_m, \Phi_n) = 1$

Proof. We know from the matrix representation that the resultant is an integer. Suppose p divides the resultant, for p prime. Then, the resultant is equivalent to 0 mod p , so Φ_m and Φ_n share a root over the field $\mathbb{Z}/p\mathbb{Z}$. However, by Lemma 5 we know that there exist $u(x), v(x) \in \mathbb{Z}[x]$ such that

$$\Phi_m(x)u(x) + \Phi_n(x)v(x) = 1$$

The above equation also holds over $\mathbb{Z}/p\mathbb{Z}$, which contradicts the existence of a common root for Φ_m and Φ_n over this field. Hence, no prime divides the resultant, so the resultant is ± 1 , and since one of m and n must be at least 3, then either Φ_m and Φ_n has all non-real roots and thus (by part 6 of Lemma 7) the resultant is $+1$. □

Lemma 10. For p prime, p relatively prime to a and b , and $i > 0$, then $\text{Res}(\Phi_{ap^i}, \Phi_{bp^i}) = \text{Res}(\Phi_a, \Phi_b)^{p^{i-1}(p-1)}$.

Proof. If $a = b$ then $\text{Res}(\Phi_a, \Phi_b) = \text{Res}(\Phi_{ap^i}, \Phi_{bp^i}) = 0$, so we can safely assume that a and b are different. We proceed by induction on i .

For $i > 1$, then by Lemma 3 $\Phi_{ap^i}(x) = \Phi_{ap^{i-1}}(x^p)$ and likewise $\Phi_{bp^i}(x) = \Phi_{bp^{i-1}}(x^p)$. Thus, we have $\text{Res}(\Phi_{ap^i}(x), \Phi_{bp^i}(x)) = \text{Res}(\Phi_{ap^{i-1}}(x^p), \Phi_{bp^{i-1}}(x^p))$, and by Theorem 8, this is $\text{Res}(\Phi_{ap^{i-1}}(x), \Phi_{bp^{i-1}}(x))^p$.

For $i = 1$, we consider

$$\begin{aligned} \text{Res}(\Phi_a, \Phi_b)^p &= \text{Res}(\Phi_a(x^p), \Phi_b(x^p)) \\ &= \text{Res}(\Phi_{ap}(x)\Phi_a(x), \Phi_{bp}(x)\Phi_b(x)) \\ &= \text{Res}(\Phi_{ap}, \Phi_{bp}) \cdot \text{Res}(\Phi_{ap}, \Phi_b) \cdot \text{Res}(\Phi_a, \Phi_{bp}) \cdot \text{Res}(\Phi_a, \Phi_b) \end{aligned}$$

Now, recall that we can assume that a and b are both different and (by hypothesis) that they are relatively prime to p . This implies that neither ap/b nor a/bp are powers of a single prime, and so by Lemma 9 we have $\text{Res}(\Phi_{ap}, \Phi_b) = \text{Res}(\Phi_a, \Phi_{bp}) = 1$. So, our previous equations imply

$$\text{Res}(\Phi_a, \Phi_b)^p = \text{Res}(\Phi_{ap}, \Phi_{bp}) \cdot 1 \cdot 1 \cdot \text{Res}(\Phi_a, \Phi_b)$$

and this implies that $\text{Res}(\Phi_{ap}, \Phi_{bp}) = \text{Res}(\Phi_a, \Phi_b)^{p-1}$. \square

Corollary 11. For c relatively prime to both a and b , then $\text{Res}(\Phi_{ac}, \Phi_{bc}) = \text{Res}(\Phi_a, \Phi_b)^{\phi(c)}$.

Proof. This follows by using Lemma 10 on all the primes p dividing c . \square

Lemma 12. For $n > m$ and n/m a power of a prime p , then $\text{Res}(\Phi_m, \Phi_n) = p^{\phi(m)}$.

Proof. We write n/m as p^i for some positive i , and we consider the options for m and n . First, suppose $m = 1$ (and thus $n = p^i$). Note that by part 5 of Lemma 7, $\text{Res}(\Phi_1, \Phi_{p^i}) = \Phi_{p^i}(1)$, which is $\Phi_p(1^{p^{i-1}}) = p = p^{\phi(m)}$ as desired.

Next, suppose $m = p$ (and thus $n = p^{i+1}$). Consider the following:

$$\begin{aligned} \text{Res}(\Phi_1, \Phi_{p^i})^p &= \text{Res}(\Phi_1(x^p), \Phi_{p^i}(x^p)) \\ &= \text{Res}(\Phi_p(x)\Phi_1(x), \Phi_{p^{i+1}}(x)) \\ &= \text{Res}(\Phi_p, \Phi_{p^{i+1}}) \cdot \text{Res}(\Phi_1, \Phi_{p^{i+1}}) \end{aligned}$$

and we can re-write both sides of this last equation as

$$p^p = \text{Res}(\Phi_p, \Phi_{p^{i+1}}) \cdot p$$

allowing us to conclude that $\text{Res}(\Phi_p, \Phi_{p^{i+1}}) = p^{p-1}$ which is $p^{\phi(m)}$ as desired.

We now suppose $m = p^k$. In this case, $\text{Res}(\Phi_{p^k}(x), \Phi_{p^{i+k}}(x)) = \text{Res}(\Phi_p(x^{p^{k-1}}), \Phi_{p^{i+1}}(x^{p^{k-1}})) = \text{Res}(\Phi_p(x), \Phi_{p^{i+1}}(x))^{p^{k-1}}$ which by above is $(p^{p-1})^{p^{k-1}} = p^{\phi(m)}$ as desired.

Finally, suppose $m = cp^k$ for c relatively prime to p . Thus, $n = cp^{k+i}$ and by Corollary 11 we have $\text{Res}(\Phi_{cp^k}(x), \Phi_{cp^{i+k}}(x)) = \text{Res}(\Phi_{p^k}(x), \Phi_{p^{i+k}}(x))^{\phi(c)}$ which by the previous case becomes $p^{\phi(p^k)\phi(c)} = p^{\phi(m)}$ as desired. \square

Bibliography

- [1] Tom M. Apostol. Resultants of cyclotomic polynomials. *Proc. Amer. Math. Soc.*, 24:457–462, 1970.
- [2] Fritz-Erdmann Diederichsen. Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz. *Abh. Math. Sem. Hansischen Univ.*, 13:357–412, 1940.
- [3] Michael Filaseta. Coverings of the integers associated with an irreducibility theorem of A. Schinzel. In *Number theory for the millennium, II (Urbana, IL, 2000)*, pages 1–24. A K Peters, Natick, MA, 2002.
- [4] Istvan Kovacs, Daniel S. Silver, and Susan G. Williams. Determinants of commuting-block matrices. *Amer. Math. Monthly*, 106(10):950–952, 1999.
- [5] Emma T. Lehmer. A numerical function applied to cyclotomy. *Bull. Amer. Math. Soc.*, 36(4):291–298, 1930.
- [6] James H. McKay and Stuart Sui Sheng Wang. A chain rule for the resultant of two polynomials. *Arch. Math. (Basel)*, 53(4):347–351, 1989.
- [7] John R. Sylvester. Determinants of block matrices. *Math. Gazette*, 84(501):460–467, Nov 2000.