ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 42, Number 5, 2012

# RESULTANTS OF CYCLOTOMIC POLYNOMIALS

GREGORY DRESDEN

In this paper we present a new and elementary proof of a theorem about resultants of cyclotomic polynomials $\Phi_n(x)$, and we prove an enhanced and constructive version of an old result about linear combinations of cyclotomics. The two theorems are as follows.

**Theorem 1** [**1, 2, 5, 6**]. *For $0 < m < n$ integers, then*

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

Since the above Theorem 1 was proved at least four separate times [**1, 2, 5, 6**], we feel justified in offering a fifth proof, this time using very little machinery.

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

**Theorem 2** [**3**]. *Let $n$ and $m$ be positive integers with $m < n$. Then, we have (explicit) polynomials $u(x)$ and $v(x)$ in $\mathbf{Z}[x]$ such that*

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

*where $k$ is equal to 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 Theorem 2 in his paper [**3**]. The first proof involved cyclotomic extensions $\mathbf{Q}(\zeta_n)$, and the second proof (this one by Schinzel, via private communication to Filaseta) used Theorem 1 on the resultant of cyclotomic polynomials.

We proceed as follows. We begin with an independent proof of Theorem 2, using neither the cyclotomic extensions of Filaseta nor the

Received by the editors on November 23, 2009.
DOI:10.1216/RMJ-2012-42-5-1461 

resultants of Schinzel, but instead only elementary facts about cyclotomic polynomials. Along the way, we also give explicit formulas for polynomials $u(x)$ and $v(x)$ in the statement of the theorem, something which has not been done before. We then use Theorem 2, along with some basic statements about determinants and resultants, to prove Theorem 1, thus establishing the equivalence of these two theorems.

**Proof of Theorem 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 $a, b \in \mathbf{Z}^+$, then $\Phi_{ab}(x) \mid \Phi_a(x^b)$.*

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

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

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 Theorem 2.

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

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

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

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

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

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

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

**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*

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

*then $u(x)$ and $v(x)$ are both in $\mathbf{Z}[x]$, and*

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

*Proof.* By direct substitution, we note that

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

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

We now show that our functions $u(x)$ and $v(x)$ are indeed in $\mathbf{Z}[x]$. In the case of $u(x)$, 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 $x^{mt} - 1$, so we can conclude that $u(x)$ is in $\mathbf{Z}[x]$. As for $v(x)$, 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 $v(x) \in \mathbf{Z}[x]$. □

We conclude with:

*Proof of Theorem* 2. By Lemmas 5 and 6, we know that $u(x)$ and $v(x)$ exist satisfying equation (1). It remains to show that $k$ 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 $u(x), v(x) \in \mathbf{Z}[x]$ exist with

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

Let us show that $p \mid C$. By Lemma 3, we can write the above equation as

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

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

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

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

**Proof of Theorem 1.** We now remind ourselves of some basic facts about resultants, as seen in [**1, 7**] and others. Recall that the resultant of two polynomials $f(x) = f_m x^m + \cdots + f_0$ and $g(x) = g_n x^n + \cdots + g_0$ over an integral domain and with roots $\alpha_i$ and $\beta_j$, respectively, is given by:

$$\operatorname{Res}(f, g) = f_m^n g_n^m \prod_{i,j} (\alpha_i - \beta_j).$$

The author still considers it a minor miracle that the resultant is equal to the determinant of the Sylvester matrix of $f$ and $g$, as seen here:

$$\operatorname{Res}(f, g) = \begin{vmatrix} f_m & \cdots & f_0 & & & \\ & f_m & \cdots & f_0 & & \\ & & \ddots & & \ddots & \\ & & & f_m & \cdots & f_0 \\ g_n & \cdots & \cdots & g_0 & & \\ & \ddots & & & \ddots & \\ & & g_n & \cdots & \cdots & g_0 \end{vmatrix}.$$

The following facts are easy consequences of the definition and the matrix representation of the resultant.

**Lemma 7.** *Let $R$ be an integral domain. For $f(x), g(x), h(x) \in R[x]$, then*:

1. *There exist $u(x), v(x) \in R[x]$ such that $f(x)u(x) + g(x)v(x) = \operatorname{Res}(f, g)$.*

2. $\operatorname{Res}(f, g) = 0$ *if and only if $f(x)$ and $g(x)$ share a root with respect to the algebraic closure of $R$.*

3. $\operatorname{Res}(f, gh) = \operatorname{Res}(f, g)\operatorname{Res}(f, h)$.

4. *For $f$ or $g$ of even degree, then* $\operatorname{Res}(f, g) = \operatorname{Res}(g, f)$.

5. $\operatorname{Res}(x - a, g) = g(a)$ *for $a \in R$.*

6. *For $f, g \in \mathbf{Z}[x]$ and $f$ with all non-real roots, then* $\operatorname{Res}(f, g)$ *is a non-negative integer.*

We provide an independent proof of the following theorem, first proved (in greater generality) in [**7**]:

**Theorem 8** [**7**]. *For $f, g$ non-constant polynomials, then* $\operatorname{Res}(f(x^t), g(x^t)) = \operatorname{Res}(f(x), g(x))^t$.

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

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

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):

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

$$= \begin{vmatrix} f_m \cdot \mathbf{I} & f_{m-1} \cdot \mathbf{I} & \cdots \\ & f_m \cdot \mathbf{I} & \cdots \\ & & \ddots \end{vmatrix}.$$

As the above detail suggests, we can think of $\operatorname{Res}(f(x^t), g(x^t))$ 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, 8**]) 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:

$$\operatorname{Res}(f(x^t), g(x^t)) = |\operatorname{Res}(f, g) \cdot \mathbf{I}| = \operatorname{Res}(f, g)^t. \qquad \square$$

We now proceed with the proof of Theorem 1. The following lemmas cover the two cases when $n/m$ is and is not the power of a prime.

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

*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 $\Phi_m$ and $\Phi_n$ share a root over the field $\mathbf{Z}/p\mathbf{Z}$. However, by Theorem 2, we know that $u(x), v(x) \in \mathbf{Z}[x]$ exist such that

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

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

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

*Proof.* If $a = b$, then $\operatorname{Res}(\Phi_a, \Phi_b) = \operatorname{Res}(\Phi_{ap^i}, \Phi_{bp^i}) = 0$, 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 $\operatorname{Res}(\Phi_{ap^i}(x), \Phi_{bp^i}(x)) = \operatorname{Res}(\Phi_{ap^{i-1}}(x^p), \Phi_{bp^{i-1}}(x^p))$, and by Theorem 8, this is $\operatorname{Res}(\Phi_{ap^{i-1}}(x), \Phi_{bp^{i-1}}(x))^p$.

For $i = 1$, we consider

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

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 $\operatorname{Res}(\Phi_{ap}, \Phi_b) = \operatorname{Res}(\Phi_a, \Phi_{bp}) = 1$. So, our previous equations imply

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

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

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

*Proof.* This follows by using Lemma 10 on all the primes $p$ dividing $c$. □

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

*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, $\mathrm{Res}\,(\Phi_1, \Phi_{p^i}) = \Phi_{p^i}(1)$, 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:

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

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

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

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

We now suppose $m = p^k$. In this case, $\mathrm{Res}\,(\Phi_{p^k}(x), \Phi_{p^{i+k}}(x)) = \mathrm{Res}\,(\Phi_p(x^{p^{k-1}}), \Phi_{p^{i+1}}(x^{p^{k-1}})) = \mathrm{Res}\,(\Phi_p(x), \Phi_{p^{i+1}}(x))^{p^{k-1}}$, which by the 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 $\mathrm{Res}\,(\Phi_{cp^k}(x), \Phi_{cp^{i+k}}(x)) = \mathrm{Res}\,(\Phi_{p^k}(x), \Phi_{p^{i+k}}(x))^{\phi(c)}$ which by the previous case becomes $p^{\phi(p^k)\phi(c)} = p^{\phi(m)}$ as desired. □

## REFERENCES

**1.** Tom M. Apostol, *Resultants of cyclotomic polynomials*, Proc. Amer. Math. Soc. **24** (1970), 457–462.

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

**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, A.K. Peters, Natick, MA, 2002.

**4.** Istvan Kovacs, Daniel S. Silver and Susan G. Williams, *Determinants of commuting-block matrices*, Amer. Math. Month. **106** (1999), 950–952.

**5.** Emma T. Lehmer, *A numerical function applied to cyclotomy*, Bull. Amer. Math. Soc. **36** (1930), 291–298.

**6.** Stéphane Louboutin, *Resultants of cyclotomic polynomials*, Publ. Math. Debrecen **50** (1997), 75–77.

**7.** James H. McKay and Stuart Sui Sheng Wang, *A chain rule for the resultant of two polynomials*, Arch. Math. (Basel) **53** (1989), 347–351.

**8.** John R. Silvester, *Determinants of block matrices*, Math. Gazette **84** (2000), 460–467. 8

Washington & Lee University, 204 West Washington Street, Lexington, VA 24450
**Email address: dresdeng@wlu.edu**