Canad. Math. Bull. Vol. 19 (4), 1976

A GENERALIZATION OF THE CYCLOTOMIC POLYNOMIAL

BY
K. NAGESWARA RAO*

ABSTRACT. In this paper, the cyclotomic polynomial is generalized and several of its properties based on the Möbius inversion are derived. It is deduced that a polynomial whose roots are the roots of a cyclotomic polynomial multiplied by those of another cyclotomic polynomial is the product of cyclotomic polynomials. Character sums and finite Fourier series are employed for the latter result.

1. **Preliminaries.** Let $n \geq 1$ be any integer. To each integer n associate a non-empty set $A(n)$ of positive divisors of n satisfying the following conditions:

I. If $d \in A(m)$ and $m \in A(n)$ imply that $d \in A(n)$ and $m/d \in A(n/d)$ and vice versa.
II. If $d \in A(n)$ then $n/d \in A(n)$.
III. $1 \in A(n)$.
IV. $A(mn) = A(m) \times A(n) = \{ab \mid a \in A(m), b \in A(n)\}$ whenever $(m, n) = 1$.
V. For every prime power of p^k, there exists a positive integer t so that

$$A(p^k) = \{1, p^t, p^{2t}, \ldots, p^{rt}\},$$

$rt = k$, and $p^t \in A(p^{2t})$, $p^{2t} \in A(p^{3t})$, etc.

Following Narkiewicz [9] the number p^t is called the primitive element of $A(p^k)$ associated with the prime p. (Also see McCarthy [4].)

If m is any integer, then the A-greatest common divisor (A-g.c.d.) of m and n is defined as the largest member of $A(n)$ that divides m and is denoted by $(m, n)_A$. The number of integers m, $0 \leq m < n$ such that $(m, n)_A = 1$ is denoted by $\phi_A(n)$ which generalizes Euler's totient.

Let ρ be any primitive nth root of unity, $d_1, d_2, \ldots, d_r$ be all the elements of $A(n)$. Then let $C(d_i)$ stand for the set of all elements $\{\rho^m\}$, $0 \leq m < n$ which are such that $(m, n)_A = n/d_i$.

Let μ_A be the Möbius function associated with the set $A(n)$ which is multiplicative and is defined for prime power values by

$$\mu_A(p^\alpha) = \begin{cases} -1 & \text{if } p^\alpha \text{ is primitive} \\ 0 & \text{otherwise} \end{cases}$$

Received by the editors February 24, 1976 and, in revised form, June 4, 1976.
* Supported in part by NSF Institutional Grant for Science GU 3615; IBM No. 4122.

https://doi.org/10.4153/CMB-1976-069-8 Published online by Cambridge University Press

Also, let the generalized Ramanujan's sum $C_A(m, n)$ be defined by

$$C_A(m,n)=\sum_{(x,n)_A=1}\exp(2\pi imx/n)$$

Let $Q_A^{(n)}(x)\equiv Q^{(n)}(x)=\pi(x-\delta)$ where the product runs over all elements δ of $C(n)$. If $A(n)$ is the set of all positive divisors of n then $Q^{(n)}(x)$ reduces to the cyclotomic polynomial. For an extensive literature on the cyclotomic polynomial, see Apostol [1].

The object of the paper is to obtain several of the properties involving $Q^{(n)}(x)$. In particular, it is shown that a monic polynomial $Q^{(d_1,\ldots,d_k)}(x)$, whose roots are given by $x=x_1\cdot x_2\cdots x_k$, where x_i $(i=1,\ldots,k)$ runs over all the roots of $Q^{(d_i)}(x)=0$, is the product of the polynomials $Q^{(d)}(x)$, where d runs over all the elements of $A(n)$.

2. **Main results.**

THEOREM 1.

$$Q^{(n)}(x)=\prod_{d\in A(n)}(x^d-1)^{\mu_A(n/d)}$$

Proof. It is clear that $x^n-1=\prod_{d\in A(n)}Q^{(d)}(x)$. Now by applying Möbius inversion (see McCarthy [3]), we get the result.

REMARK 1. From Theorem 1 it follows that the coefficients of $Q^{(n)}(x)$ are rational integers.

REMARK 2. The polynomial $Q^{(n)}(x)$ is irreducible over the rational field if $A(n)$ is the set of all positive divisors of n.

We now obtain some lemmas:

LEMMA 1. *If* $f(n)=\prod[1-e(T,n)]$ & $f(1)=1$ *and* $g(n)=\prod[1-e(x,n)]$ & $g(1)=1$ *where in the first product* T *runs from* 1 *to* $n-1$ *and in the second* x *ranges over all the elements* mod n *such that* $(x,n)_A=1$ *then* $g(n)=\prod_{\omega\in A(n)}[f(n/\omega)]^{\mu_A(\omega)}$.

Proof. Clearly $f(n)=\prod_{\omega\in A(n)}g(\omega)$. Now by applying the inversion principle for products, the result is obtained.

Note:

$$g(n)=\begin{cases}Q^{(n)}(1) & \text{if } n>1\\ 1 & \text{if } n=1\end{cases}$$

LEMMA 2. $\log g(n)=\Lambda_A(n)$, *where* $g(n)$ *is the function defined above and* $\Lambda_A(n)$ *is given in*

$$\Lambda_A(n)=\begin{cases}\log p^t & \textit{if } n \textit{ is the power of a prime and } p^t \textit{ is its primitive}\\ 0 & \textit{otherwise}\end{cases}$$

https://doi.org/10.4153/CMB-1976-069-8 Published online by Cambridge University Press

It is well known that $f(n)=n$, then by the above Lemma 1, $g(n)=\prod_{\omega\in A(n)}(n/\omega)^{\mu_A(\omega)}$. If n has canonical representation given by $n=p_1^{a_1}\cdots p_r^{a_r}$ and $p_i^{t_i}$ is the primitive for $p_i^{a_i}$ $(i=1,\ldots,r)$ then

$$g(n)=\left(\frac{n}{1}\right)\prod_{1}^{r}\left(\frac{p_i^{t_i}}{n}\right)\prod_{\substack{i\neq j\\ i,j=1}}^{r}\left(\frac{n}{p_i^{t_i}p_j^{t_j}}\right)\prod_{\substack{i\neq j\neq k\\ i,j,k=1}}^{r}\left(\frac{p_i^{t_i}p_j^{t_j}p_k^{t_k}}{n}\right)\cdots$$

where $p_i^{t_i}$ are primitives. (Vacuous products are to be taken as 1.) But this is clearly given by

$$g(n)=\begin{cases}p_1^{t_1}=p^t & \text{if } r=1\\ 1 & \text{otherwise.}\end{cases}$$

This completes the proof of the lemma.

LEMMA 3. $Q^{(1)}(1)=0$.
Since $Q^{(1)}(x)=x-1$, *the result follows.*

Lemmas 2 and 3 yield the following result.

THEOREM 2.

$$Q^{(n)}(1)=\begin{cases}p^t & \textit{if } n=p^k \textit{ and } p^t \textit{ is the primitive}\\ 0 & \textit{if } n=1\\ 1 & \textit{otherwise}\end{cases}$$

THEOREM 3.

$$Q^{(n)}(x)=x^{\phi_A(n)}Q^{(n)}(x^{-1})$$

Proof. Clearly the degree of $Q^{(n)}(x)$ is $\phi_A(n)$. Also, if $\delta\in C(n)$ then $\delta^{-1}\in C(n)$ and hence $Q^{(n)}(x)=0$, $Q^{(n)}(x^{-1})=0$ have the same roots.

THEOREM 4. *If* $(m,p^\alpha)=1$, *then* $Q^{(mp^\alpha)}(x)=Q^{(mp^t)}(x^{p^{\alpha-t}})$.

Proof. The result follows from

$$\prod_{d\in A(mp^\alpha)}[x^{mp^\alpha/d}-1]^{\mu_A(d)}=\prod[(x^{p^{\alpha-t}})^{mp^t/d}-1]^{\mu_A(d)}$$

THEOREM 5.

$$Q^{(p^tm)}(x)Q^{(m)}(x)=Q^{(m)}(x^{p^t}) \quad \textit{whenever} \quad (m,p^t)=1.$$

Proof. Consider

$$\prod_{d\in A(mp^t)}[x^{mp^t/d}-1]^{\mu_A(d)}\cdot\prod_{\delta\in A(m)}[x^{m/\delta}-1]^{\mu_A(\delta)}$$

$$=\prod_{D\in A(m)}[x^{mp^t/D}-1]^{\mu_A(D)}\cdot\prod_{\substack{\Delta\in A(mp^t)\\ \Delta\notin A(m)}}[x^{mp^t/\Delta}-1]^{\mu_A(\Delta)}\cdot\prod_{\delta\in A(m)}[x^{m/\delta}-1]^{\mu_A(\delta)}$$

https://doi.org/10.4153/CMB-1976-069-8 Published online by Cambridge University Press

But

$$\prod_{\substack{\delta p^t \in A(mp^t)\\ \delta \notin A(p^t)}} [x^{mp^t/\delta p^t}-1]^{\mu_A(\delta p^t)} \cdot \prod_{\delta \in A(m)} [x^{m/\delta}-1]^{\mu_A(\delta)}$$

$$= \prod_{\substack{\delta p^t \in A(mp^t)\\ \delta \notin A(p^t)}} [x^{m/\delta}-1]^{-\mu_A(\delta)} \cdot \prod_{\delta \in A(m)} [x^{m/\delta}-1]^{\mu_A(\delta)} = 1$$

Let

$$P_i(m, n) = \begin{cases} 1 & \text{if } (m, n)_A \in C(d_i) \\ 0 & \text{otherwise.} \end{cases}$$

It is easy to see that $P_i(m, n)$ is multiplicative in n and also in m, n; i.e., $P_i(m, n_1 n_2) = P_i(m, n_1)P_i(m, n_2)$ whenever $(n_1, n_2) = 1$; also $P_i(m_1 m_2, n_1 n_2) = P_i(m_1, n_1)P_i(m_2, n_2)$ whenever $(m_1 n_1, m_2 n_2) = 1$. Also, it is an A-even function (mod n), i.e., $P_i(m, n) = P_i(g, n)$ where $g = (m, n)_A$.

THEOREM 6. *The function $P_j(m, n)$ has the representation given by*

$$P_i(m, n) = \frac{1}{n} \sum_{d \in A(n)} C_A\left(\frac{n}{d}, d_i\right) C_A(m, d).$$

Proof. Since $P_i(m, n)$ is A-even (mod n) it admits a representation given by

$$P_i(m, n) = \sum_{\omega \in A(n)} a_\omega C_A(m, \omega)$$

where

$$a_\omega = \frac{1}{n} \sum_{d \in A(n)} P_i\left(\frac{n}{d}, n\right) C_A\left(\frac{n}{\omega}, d\right).$$

(cf. McCarthy [3], Theorem 6). (See Cohen [2].) Using the definition of $P_i(m, n)$ we have $a_\omega = (1/n)C_A(n/\omega, d_i)$.

The Cauchy product $h(m, n)$ of $P_i(m, n)$ and $P_j(m, n)$ is defined by the relation:

$$h(m, n) = \sum_{m \equiv a+b \pmod n} P_i(a, n)P_j(b, n)$$

where the summation runs over all a and b (mod n) such that $m \equiv a + b \pmod n$. We now have the following:

LEMMA 4. *If $f(m, n)$ and $g(m, n)$ are two A-even functions* (mod n) *having the representations given by*

$$f(m, n) = \sum_{d \in A(n)} \alpha_d C_A\left(m, \frac{n}{d}\right)$$

$$g(m, n) = \sum_{d \in A(n)} \beta_d C_A\left(m, \frac{n}{d}\right)$$

https://doi.org/10.4153/CMB-1976-069-8 Published online by Cambridge University Press

then the Cauchy product $\ell(m, n)$ *of* $f(m, n)$, *and* $g(m, n)$ *is given by*

$$\ell(m, n) = \sum_{m \equiv a+b \pmod n} f(a, n) g(b, n)$$
$$= n \sum_{d \in A(n)} \alpha_d \beta_d C_A\left(m, \frac{n}{d}\right)$$

Proof. The result is a direct conseauence of the orthogonality relation:

$$\sum_{m \equiv a+b \pmod n} C_A(a, d_i) C_A(b, d_j) = \begin{cases} nC_A(m, d) & \text{if } d_i = d_j = d \\ 0 & \text{if } d_i \neq d_j \end{cases}$$

(cf. McCarthy [3], Theorem 3.)

THEOREM 7. *The number of solutions* $\{a, b\}$ *of the congruence:* $m \equiv a + b \pmod n$, *such that* $(a, n)_A = n/d_i$ *and* $(b, n)_A = n/d_j$ *is*

$$\frac{1}{n} \sum_{\omega \in A(n)} C_A\left(\frac{n}{\omega}, d_i\right) C_A\left(\frac{n}{\omega}, d_j\right) C_A(m, \omega)$$

Proof. By Lemma 4, the Cauchy product $h(m, n)$ of $P_i(m, n)$ and $P_j(m, n)$ is the expression given in the theorem. But this Cauchy product by definition is $\sum_{m \equiv a+b \pmod n} P_i(a, n) P_j(b, n)$ which is the number of solutions of the congruence stated above.

REMARK 3. Since $C_A(m, n)$ is A-even (mod n) it follows that the number of solutions of the congruences: $m \equiv a + b \pmod n$ such that $(a, n)_A = n/d_i$ and $(b, n)_A = n/d_j$ and $m' \equiv a + b \pmod n$ are the same whenever $(m, n)_A = (m', n)_A$. The same thing can also be interpreted as follows: Let $C(d_i) \otimes C(d_j)$ stand for the set of elements obtained by multiplying each element of $C(d_i)$ with each element of $C(d_j)$. If any element of $C(d_k)$ appears γ times in the product set then every element of $C(d_k)$ must repeat the same number of times. Or equivalently $C(d_i) \otimes C(d_j)$ can be represented as a linear combination of $C(d_1), \ldots, C(d_r)$. If $A(n)$ is the set of all positive divisors of n, the above discussion in substance reduces to the result of Vaidyanathaswamy [10].

THEOREM 7'. *The number of solutions of the congruence* $m \equiv x_1 + \cdots + x_s \pmod n$ *where* s_i *of the* x*'s are such that* $(x_i, n)_A = n/d_i$ *and* $\sum s_i = s$, *is equal to*

$$\frac{1}{n} \sum_{\omega \in A(n)} \left[\prod_i \left[C_A\left(\frac{n}{\omega}, d_i\right) \right]^{s_i} \cdot C_A(m, \omega) \right]$$

Proof. The result mentioned is the Cauchy product of s_1 functions $P_1(m, n)$, s_2 functions $P_2(m, n), \ldots$ so that $\sum s_i = s$.

This generalizes some of the results of Rao [7] and [8] and McCarthy [5].

THEOREM 8. *If* $Q^{(d_1,\ldots,d_k)}(x)$ *is a monic polynomial whose roots are* $\{x_1x_2\cdots x_k\}$, *where* x_i *runs over all the roots of* $Q^{(d_i)}(x)=0$, *then* $Q^{(d_1,\ldots,d_k)}(x)=\prod_{d\in A(n)}[Q^{(d)}(x)]^{\gamma(d_1,\ldots,d_k,d)}$ *where*

$$\gamma(d_1,\ldots,d_k,d)=\frac{1}{n}\sum_{\omega\in A(n)} C_A\left(\frac{n}{\omega},d_1\right)\cdots C_A\left(\frac{n}{\omega},d_k\right)C_A(d,\omega).$$

Proof. This is a direct consequence of Theorem 7′ since each root of $Q^{(d)}(x)$ is repeated $\gamma(d_1,\ldots,d_k,d)$ times in $\{(x_1x_2\cdots x_k)\}$. This generalizes a result of Menon [6].

When $A(n)$ is the set of all positive divisors of n denote $Q^{(n)}(x)$ by $P_n(x)$ the cyclotomic polynomial and $C_A(m,n)$ by $C(m,n)$, the Ramanujan's Sum. We now deduce that a polynomial whose roots are the roots of a cyclotomic polynomial multiplied by those of another cyclotomic polynomial is the product of cyclotomic polynomials. Precisely,

THEOREM 8′. *If* $P_{d_1,d_2}(x)$ *is the monic polynomial whose roots are the roots of* $P_{d_1}(x)$ *multiplied by those of* $P_{d_2}(x)$ *then*:

$$P_{d_1,d_2}(x)=\prod_{d/n}[P_d(x)]^{\Gamma(d_1,d_2,d)}$$

where

$$\Gamma(d_1,d_2,d)=\frac{1}{n}\sum_{\omega/n} C\left(\frac{n}{\omega},d_1\right)C\left(\frac{n}{\omega},d_2\right)C(d,\omega).$$

The author is grateful to the referee for his useful suggestions.

REFERENCES

1. Tom M. Apostol, *The resultant of the cyclotomic polynomials* $F_m(ax)$ *and* $F_n(bx)$. Math. Comp. **29** (1975), 1–6.

2. Eckford Cohen, *A class of arithmetical functions*. Proc. Nat. Acad. Sci. USA, **41** (1955), 939–944.

3. Paul J. McCarthy, *Regular arithmetical convolutions*. Port. Math. **27** (1968), 1–13.

4. Paul J. McCarthy, *Arithmetical functions and distributivity*. Canad. Math. Bull. **13** (1970), 491–496.

5. Paul J. McCarthy, *Regular arithmetical convolutions and the solution of linear congruences*. Colloq. Math **22** (1971), 215–222.

6. P. K. Menon, *On Vaidyanathaswamy's class division of the residue classes modulo N*. J. Indian Math. Soc. **26** (1962), 167–186.

7. K. Nageswara Rao, *Unitary class division of integers mod n and related arithmetical identities*. J. Indian Math. Soc. **30** (1966), 195–205.

8. K. Nageswara Rao, *On a congruence equation and related arithmetical identities*. Monatsh. Math. **71** (1967), 24–31.

9. W. Narkiewicz, *On a class of arithmetical convolutions*. Colloq. Math. **10** (1963), 81–94.

10. R. Vaidyanathaswamy, *A remarkable property of integers mod N and its bearing on group theory*. Proc. Ind. Acad. Sci. **5A** (1937), 63–75.

DEPT. OF MATHEMATICS
NORTH DAKOTA STATE UNIVERSITY
FARGO, NORTH DAKOTA 58102 USA