RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

L. CARLITZ

A polynomial related to the cyclotomic polynomial

Rendiconti del Seminario Matematico della Università di Padova, tome 47 (1972), p. 57-63

<http://www.numdam.org/item?id=RSMUP_1972__47__57_0>

REND. SEM. MAT. UNIV. PADOVA, Vol. 47 (1972)

A POLYNOMIAL RELATED TO THE CYCLOTOMIC POLYNOMIAL

L. CARLITZ *)

1. Let

$$F_n(x)=\prod_{\substack{k=1\\(k,n)=1}}^{n}(x-e^{2\pi ki/n}) \tag{1.1}$$

denote the cyclotomic polynomial. In a recent paper [1] Apostol has determined the resultant $R(F_m, F_n)$ of the cyclotomic polynomials $F_m(x)$, $F_n(x)$; see also Diederichsen [3].

For $m, n\geq 1$ put

$$G_{m,n}(x)=\prod_{\alpha,\beta}(\alpha x-\beta), \tag{1.2}$$

where α runs through the primitive m-th roots of unity and β runs through the primitive n-th roots of unity. Clearly

$$G_{m,n}(1)=R(F_m, F_n). \tag{1.3}$$

Also it follows at once from (1.2) that

$$G_{m,n}(x)=c_{m,n}H_{m,n}(x). \tag{1.4}$$

---

*) Indirizzo dell'A.: Dept. of Mathematics - Duke University - Durham, North Carolina 27706, U.S.A.

Supported in part by NSF grant GP-17031.

where

$$H_{m,n}(x)=\prod_{\alpha,\beta}(x-\alpha\beta) \tag{1.5}$$

and

$$c_{m,n}=\prod_{\alpha}\alpha^{\varphi(n)}=\begin{cases}-1 & (m=2,\ n=1,\ 2)\\ 1 & (\text{otherwise}).\end{cases} \tag{1.6}$$

In (1.5), as in (1.2), α runs through the primitive m-th roots of unity while β runs through the primitive n-th roots of unity.

Let k denote the greatest common divisor of m and n such that

$$\left(k, \frac{m}{k}\right)=1, \quad \left(k, \frac{n}{k}\right)=1. \tag{1.7}$$

We may call k the *unitary* greatest common divisor of m and n and write

$$k=(m,\ n)^*. \tag{1.8}$$

(We remark that Eckford Cohen [2] has defined a similar function that is denoted by $(m,\ n)_*$). We shall show that, for $k=1$,

$$H_{m,n}(x)=(F_M(x))^{\varphi(d)} \tag{1.9}$$

where

$$d=(m,\ n), \qquad M=[m,\ n]=mn/d.$$

The general case ($k\geq 1$) is given in Theorem 1 below.

Apostol's result is an easy corollary of the theorem. Indeed a slightly more general result is given in (3.12).

2. We shall require several lemmas.

LEMMA 1. *The number of solutions of*

$$x+y\equiv(\mathrm{mod}\ p^e) \qquad (p\nmid xy), \tag{2.1}$$

where p is a prime and $e>1$, is equal to

$$\begin{cases} p^{e-1}(p-2) & (p\nmid a) \\ p^{e-1}(p-1) & (p/a). \end{cases} \tag{2.2}$$

LEMMA 2. *Let $f(a, n)$ denote the number of solutions of*

$$x+y\equiv a(\mathrm{mod}\, n) \qquad ((x, n)=(y, n)=1). \tag{2.3}$$

Then, for $(m, n)=1$,

$$f(a, mn)=f(a, m)f(a, n). \tag{2.4}$$

The proof of these two lemmas is almost immediate.

LEMMA 3. *Let α, β independently run through the primitive k-th roots of unity. Let r denote an arbitrary divisor of k. Then the primitive r-th roots of unity occur $\psi(r, k)$ times among the products $\alpha\beta$, where*

$$\psi(r, k)=\prod_{f_j<e_j} p_j^{e_j-1}(p_j-1) \prod_{f_j=e_j} p_j^{e_j-1}(p_j-2), \tag{2.5}$$

with

$$k=\prod_{j=1} p_j^{e_j}, \qquad r=\prod_{j=1} p_j^{f_j}. \tag{2.6}$$

PROOF. Let ε denote a fixed primitive k-th root of unity and put $\alpha=\varepsilon^x$, $\beta=\varepsilon^y$, where x, y run through reduced residue systems (mod k). Let $k=rs$. Then $\gamma=\alpha\beta=\varepsilon^{x+y}$ is a primitive r-th root of unity if and only if

$$x+y\equiv as(\mathrm{mod}\, k),$$

where $(a, r)=1$. For fixed a, s, the number of solutions of this congruence is $f(as, k)$ as defined in Lemma 2. Now apply Lemmas 1 and 2 and (2.5) follows at once.

LEMMA 4. *Let $(m, n)^*=1$, where $(m, n)^*$ is defined by (1.7) and (1.8). Let α run through the primitive m-th roots of unity and β through the primitive n-th roots of unity. Then $\gamma=\alpha\beta$ runs through the primitive M-th roots of unity $\varphi(d)$ times, where*

$$d=(m, n), \qquad M=[m, n]=mn/d. \tag{2.7}$$

It suffices to prove this when

$$m=p^e, \qquad n=p^f \qquad (e>f\geq 0),$$

where p is prime. Then if α is a primitive p^e-th root of unity and β is a primitive p^f-th root, it is clear that $\gamma=\alpha\beta$ is a primitive p^e-th root. Moreover each γ will occur exactly $\varphi(p^f)$ times.

3. Given $m, n\geq 1$, define $k=(m, n)^*$ by means of (1.7) and (1.8) and put

$$m=km', \qquad n=kn', \tag{3.1}$$

so that

$$(m', n')^*=1. \tag{3.2}$$

Then by (1.5) and (3.1) we have

$$H_{m,n}(x)=\prod\{x-\alpha(k)\alpha(m')\beta(k)\beta(n')\},$$

where $\alpha(k)$, $\beta(k)$ independently run through the primitive k-th roots of unity while $\alpha(m')$, $\beta(n')$ run through the primitive m'-th and n'-th roots, respectively. Applying Lemmas 3 and (4) we get

$$H_{m,n}(x)=\prod_{r|k}\prod\{x-\gamma(r)\alpha(M)\}^{\psi(r,k)\varphi(d)}, \tag{3.3}$$

where in the inner product $\gamma(r)$ runs through the primitive r-th roots of unity and $\alpha(M)$ runs through the primitive M-th roots,

$$d=(m', n'), \qquad M=[m', n']. \tag{3.4}$$

Since $(r, M)=1$, $\gamma(r)\alpha(M)$ runs through the primitive rM-th roots of unity. Hence (3.3) becomes

$$H_{m,n}(x)=\prod_{r|k}(F_{rM}(x))^{\psi(r,k)\varphi(d)}. \tag{3.5}$$

Making use of the formula

$$F_{rM}(x)=\prod_{st=r}(F_M(x^s))^{\mu(t)},$$

we get

$$H_{m,n}=\prod_{rst=k}F_M(x^s)^{\mu(t)\psi(st,\,k)\varphi(d)}$$

$$=\prod_{su=k}F_M(x^s)^{\varphi(d)e(s,\,u,\,k)}$$

where

$$e(s,\,u,\,k)=\sum_{t\mid u}\mu(t)\psi(st,\,k). \tag{3.6}$$

Put

$$k=\prod p^e, \qquad k^*=\prod p^{e-1}. \tag{3.7}$$

It follows from (2.5) and (3.6) that

$$e(s,\,u,\,k)=0 \text{ if } k^*\nmid s. \tag{3.8}$$

Moreover, when $k^*\mid s$, we get

$$e(s,\,u,\,k)=\prod_{f<e}p^{e-1}\cdot\prod_{e=f}p^{e-1}(p-2), \tag{3.9}$$

where $s=\prod p^f$.

We may now state the following

THEOREM 1. *Let k be the greatest common divisor of m and n such that*

$$\left(k,\frac{m}{k}\right)=\left(k,\frac{n}{k}\right)=1$$

and put

$$M=\left[\frac{m}{k},\frac{n}{k}\right], \qquad d=\left(\frac{m}{k},\frac{n}{k}\right).$$

Then

$$H_{m,n}(x)=\prod_{su=k} F_M(x^s)^{\varphi(d)e(s,u,k)}, \tag{3.10}$$

where the product is restricted to those s that are divisible by k^* *and* $e(s, u, k)$ *is evaluated by* (3.9). *In particular, if* $k=1$, *then*

$$H_{m,n}(x)=(F_M(x))^{\varphi(d)}, \tag{3.11}$$

where $M=[m, n]$, $d=(m, n)$.

It is easily verified that

$$\sum_{su=k} e(s, u, k)=\varphi(k).$$

Hence (3.10) implies

$$H_{m,n}(1)=p^{\varphi(d)\varphi(k)}=p^{\varphi(dk)},$$

provided $M=p^a$. Thus if $m>n\geq 1$ and $m=np^a$ then

$$H_{m,n}(1)=p^{\varphi(n)} \tag{3.11}$$

in agreement with Apostol [1].

It may be of interest to mention that if ζ denotes a k^*-th root of unity (not necessarily primitive) then we have

$$H_{m,n}(\zeta)=p^{\varphi(n)}, \tag{3.12}$$

where again $m=np^a$.

REFERENCES

[1] Apostol, T. M.: *Resultants of cyclotomic polynomials*, Proceedings of the American Mathematical Society, vol. 24 (1970), 457-462.

[2] ECKFORD, COHEN: *Arithmetical functions associated with the unitary divisors of an integer,* Mathematische Zeitschrift, vol. 74 (1960), 66-80.

[3] DIEDERICHSEN, F. E.: *Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz,* Abh. Math. Sem. Hansischen Univ., vol. 13 (1964), 357-412.

Manoscritto pervenuto in redazione il 24 settembre 1971.