

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>](http://www.numdam.org/item?id=RSMUP_1972__47__57_0)

© Rendiconti del Seminario Matematico della Università di Padova, 1972, tous droits réservés.

L'accès aux archives de la revue « Rendiconti del Seminario Matematico della Università di Padova » (<http://rendiconti.math.unipd.it/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

*Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques*
<http://www.numdam.org/>

A POLYNOMIAL RELATED TO THE CYCLOTOMIC POLYNOMIAL

L. CARLITZ *)

1. Let

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

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

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

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

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

Also it follows at once from (1.2) that

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

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

Supported in part by NSF grant GP-17031.

where

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

and

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

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

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

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

$$(1.8) \quad k = (m, n)^*.$$

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

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

where

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

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*

$$(2.1) \quad x + y \equiv (\text{mod } p^e) \quad (p \nmid xy),$$

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

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

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

$$(2.3) \quad x + y \equiv a \pmod{n} \quad ((x, n) = (y, n) = 1).$$

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

$$(2.4) \quad f(a, mn) = f(a, m)f(a, n).$$

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

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

with

$$(2.6) \quad k = \prod_{j=1} p_j^{e_j}, \quad r = \prod_{j=1} p_j^{f_j}.$$

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 $(\text{mod } k)$. Let $k = rs$. Then $\gamma = \alpha\beta = \varepsilon^{x+y}$ is a primitive r -th root of unity if and only if

$$x + y \equiv as \pmod{k},$$

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 $\phi(d)$ times, where

$$(2.7) \quad d = (m, n), \quad M = [m, n] = mn/d.$$

It suffices to prove this when

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

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

$$(3.1) \quad m = km', \quad n = kn',$$

so that

$$(3.2) \quad (m', n')^* = 1.$$

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

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

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,

$$(3.4) \quad d = (m', n'), \quad M = [m', n'].$$

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

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

Making use of the formula

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

we get

$$\begin{aligned} H_{m,n} &= \prod_{rst=k} F_M(x^s)^{\mu(t)\psi(st, k)\varphi(d)} \\ &= \prod_{su=k} F_M(x^s)^{\varphi(d)e(s, u, k)} \end{aligned}$$

where

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

Put

$$(3.7) \quad k = \Pi p^e, \quad k^* = \Pi p^{e-1}.$$

It follows from (2.5) and (3.6) that

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

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

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

where $s = \Pi p^f$.

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

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

Then

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

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

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

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

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

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

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

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.