Publ. Math. Debrecen
50 / 1-2 (1997), 75–77

Resultants of cyclotomic polynomials

By STÉPHANE LOUBOUTIN (Caen)

Abstract. We give a simple proof of a result of Apostol and Diederichsen.

Notations. When x and y are positive integers we let (x,y) be the greatest common divisor of x and y. We set $\zeta_x = \exp(2i\pi/x)$, we let $\phi(x)$ be the number of positive integers less than or equal to x which are prime to x, and we let $\rho(F_m,F_n)$ denote the resultant of any two cyclotomic polynomials $F_m(X)$ and $F_n(X)$ with $m > n \geq 1$. Finally, two algebraic integers α and β are called equivalent when there exists an algebraic unit ε such that $\alpha = \varepsilon\beta$. Note that two positive rational integers which are equivalent are equal (since any rational number which is an algebraic integer is a rational integer.)

Theorem (Tom M. Apostol and F.-E. Diederichsen). *If* $m > n > 1$ *then*

$$\rho(F_m,F_n) = \begin{cases} p^{\phi(n)} & \text{if } n \text{ divides } m \text{ and } m/n \text{ is a power of a prime } p, \\ 1 & \text{otherwise.} \end{cases}$$

We first explain our simple idea which is easy to remember. In principle, a reader who understands this simple idea will be able to reconstruct our proof of the Theorem. We start from

$$(*) \qquad \rho(F_m,F_n) = \prod_{\substack{u=1\\(m,u)=1}}^{m} \prod_{\substack{v=1\\(n,v)=1}}^{n} (1-\zeta_{mn}^{mv-nu})$$

and note that $\rho(F_m,F_n)$ is a positive integer. Thus, if $\rho(F_m,F_n)$ is equivalent to some positive integer N then $\rho(F_m,F_n) = N$. Now, $1-\zeta_x^y$

Mathematics Subject Classification: Primary 11C08; Secondary 11A99.

(with $(x, y) = 1$) is most often equivalent to 1 (i.e. is an algebraic unit), except when x is a power of some prime p, in which case $(1-\zeta_x^y)^{\phi(x)}$ is equivalent to p. Hence, we will first determine under which condition on m and n there may exist u and v in $(*)$ such that $mn/(mn, mv-nu)$ is a power of some prime. Then we will count the u's and v's in $(*)$ for which $mn/(mn, mv-nu)$ is a power of some prime.

Lemma 1. *Let x and y be coprime positive integers. Then, $1-\zeta_x^y$ is associated to $1-\zeta_x$. Moreover, $1-\zeta_x$ is associated to 1, except if x is a power of some prime p, in which case $(1-\zeta_x)^{\phi(x)}$ is associated to p.*

Proof. For the first point, we let z be such that $yz \equiv 1 \pmod{x}$ and note that $(1-\zeta_x^y)/(1-\zeta_x) = \sum_{k=0}^{y-1} \zeta_x^k$ and its inverse $(1-\zeta_x)/(1-\zeta_x^y) = (1-\zeta_x^{yz})/(1-\zeta_x^y) = \sum_{k=0}^{z-1} \zeta_x^{ky}$ are both algebraic integers. Second, let $N \geq 2$ be an integer. Since $\prod_{1\neq d\mid N} F_d(X) = (X^N-1)/(X-1)$, then $N = \prod_{1\neq d\mid N} F_d(1)$. Hence, $F_N(1) = p$ if N is a power of some prime p, and $F_N(1) = 1$ otherwise. The proof of Lemma 1 is now straightforward. □

Lemma 2. *Let $m > n > 1$ and u and v be positive integers with $(m, u) = 1$ and $(n, v) = 1$. Then, $mn/(mn, mv-nu)$ is the power of some prime p if and only if there exits $a \geq 1$ such that $m = np^a$ and N divides $p^a v - u$, where N is defined by means of $n = Np^b$ with $(p, N) = 1$. In that case, $mn/(mn, mv-nu) = p^{a+b}$ and there are exactly $\phi(m)\phi(n)/\phi(N)$ couples (u, v) with $1 \leq u \leq m$, $(m, u) = 1$, $1 \leq v \leq n$, $(n, v) = 1$ such that N divides $p^a v - u$.*

Proof. Set $d = (m, n)$, define $M > N \geq 1$ by means of $m = dM$ and $n = dN$ and assume throughout this proof that $(m, u) = (n, v) = 1$. Then $mn/(mn, mv-nu) = MN(d/(d, Mv-Nu))$. Hence, if $mn/(mn, mv-nu)$ is a power of some prime p then $N = 1$, i.e. n divides m, and M is a power of p, i.e. there exists $a \geq 1$ such that $m = np^a$. Conversely, if $m = np^a$ and $n = p^b N$ with $(p, N) = 1$ and $a \geq 1$, then $mn/(mn, mv-nu) = p^a(n/(n, p^a v-u)) = p^{a+b}(N/(N, p^a v-u))$ is a power of p if and only if N divides $p^a v-u$, in which case $mn/(mn, mv-nu) = p^{a+b}$. Finally, the last point of Lemma 2 is easily proved once we note that for each u prime to n we have $\phi(p^{a+b}) = \phi(n)/\phi(N)$ possible choices for v. □

Proof of the Theorem. If m is not equal to n times some power of a prime, then according to the Lemmas all the terms which appear in $(*)$ are associated to 1, hence $\rho(F_m, F_n)$ is associated to 1, which implies $\rho(F_m, F_n) = 1$. Now, assume that there exists some prime p such that $m = np^a$. Then, according to the Lemmas there are exactly $\phi(m)\phi(n)/\phi(N)$ terms in $(*)$ which are not associated to 1, each of which is associated to $1 - \zeta_{p^{a+b}}$, so that their product is associated to p^k with $k = \phi(m)\phi(n)/\phi(N)\phi(p^{a+b}) = \phi(n)$. Hence, $\rho(F_m, F_n)$ is associated to $p^{\phi(n)}$, which implies $\rho(F_m, F_n) = p^{\phi(n)}$. □

References

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

[2] F.-E. Diederichsen, Über die Ausreduktion ganzzahlinger Gruppendarstellungen bei arithmetischer Äquivalenz, *Abh. Math. Sem. Univ. Hamburg* **13** (1940), 357–412.

[3] R. Sivaramakrishnan, Classical Theory of Arithmetic Functions, Textbooks in Pure and Applied Mathematics, Vol. 126, *Marcel Dekker*, *New York and Basel*, 1989.

STÉPHANE LOUBOUTIN
UNIVERSITÉ DE CAEN, U.F.R. SCIENCES
DÉPARTEMENT DE MATHÉMATIQUES
ESPLANADE DE LA PAIX
14032 CAEN CEDEX, FRANCE
E-mail: louboutin@math.unicaen.fr

(Received October 16, 1995)