A Note on a Theorem of Rotkiewicz

Gombodorj Bayarmagnai
Department of Mathematics
National University of Mongolia
Baga Toirog
Ulaanbaatar 14200
Mongolia
bayarmagnai@smcs.num.edu.mn

Abstract

In 1961, Rotkiewicz presented a generalisation of the well-known fact that $n$ divides $\varphi(a^n - 1)$ for all positive integers $n$ and $a > 1$, where $\varphi$ is Euler’s totient function. In this note, we extend his result to values of cyclotomic polynomials.

1 Introduction

Let $\varphi$ be the Euler’s totient function. It is well known that $n \mid \varphi(a^n - 1)$ for all positive integers $n$ and $a > 1$ (see, e.g., Gunderson [2]). Let $\Phi_k$ be the homogeneous cyclotomic polynomial of order $k$, and let $d(n)$ be the number of divisors of $n$. Rotkiewicz [3] generalized the above result as follows:

$$n^\frac{d(n)}{2} \mid \varphi(\Phi_k(a^n, b^n))$$

for all positive integers $a, b$ ($a > b$) and $n$. In this note we extend this result to values of cyclotomic polynomials.

Theorem 1. Let $n$ and $k$ be relatively prime positive integers. For all positive integers $a, b$ ($a > b$) we have

$$k^n a^{\frac{d(n)}{2}} \mid \varphi(\Phi_k(a^n, b^n)),$$

where

$$\alpha = \begin{cases} 
    d(n) - 1, & \text{if } a = 2b \text{ and } ke = 6 \text{ for some } e \mid n; \\
    d(n), & \text{otherwise}.
\end{cases}$$

1
Note that the case of $k = 2$ was discussed in Rotkiewicz [3, Theorem 2].

Fix positive integers $a, b$ ($a > b$) and $k$, and define a sequence $(V_n^{(k)})_{n \geq 1}$ by setting $V_n^{(k)} = \Phi_k(a^n, b^n)$. Since $\Phi_k$ is homogeneous, we may assume without loss of generality that $a$ and $b$ are relatively prime.

For convenience, we recall the notion of arithmetic primitive factor introduced in Birkhoff-Vandiver [1] in the following way. A prime of $V_n^{(k)}$ is called a primitive prime factor of the term if it does not divide any $V_m^{(k)}$ for proper divisors $m$ of $n$. We consider the arithmetic primitive factor of $V_n^{(k)}$ given by the product

$$P_n^{(k)} = \prod p^{v_p(V_n^{(k)})},$$

where $p$ runs through all primitive prime factors of the term. Here, $v_p(n)$ denotes the exponent of $p$ in the decomposition of $n$. If $n$ and $k$ are relatively prime then it follows from the identity

$$\Phi_k(a^n, b^n) = \prod \Phi_{ke}(a, b)$$

that $P_n^{(k)}$ divides $\Phi_{kn}(a, b)$.

2 Proof

Let $n$ be an integer relatively prime to a prime $p$, and let $\text{ord}_p(n)$ be the order of $n$ modulo $p$. We now state the following useful lemma.

**Lemma 2.** Let $p$ be a prime not dividing $b$. Then

(a) $v_p(\Phi_k(a, b)) \neq 0$ if and only if $k = p^{v_p(b)} \text{ord}_p(ab^{-1})$,

(b) if $v_p(k) \neq 0$ then $v_p(\Phi_k(a, b)) \leq 1$ (except $k = p = 2$).

**Proof.** See Roitman [4].

**Proof of Theorem.** Let $d$ be a divisor of $n$. The identity (1) implies that every primitive prime of $V_{kd}^{(1)}$ is a factor of $P_d^{(k)}$. Hence, by Zsigmondy’s theorem, $P_d^{(k)} \neq 1$ if

$$(kd, a, b) \neq (6, 2, 1).$$

Under the condition (2), we claim that $P_d^{(k)}$ has a prime factor not dividing $kd$. Suppose that $p$ is a prime of $kd$ dividing $\Phi_{kd}(a, b)$. Then Lemma 2(a) implies that $kd/p^{v_p(kd)} < p$ and so $p$ is the largest prime of $kd$. Thus, by Lemma 2(b), $p$ is the greatest common divisor of $kd$ and $\Phi_{kd}(a, b)$. Hence, if the claim is not true, then it follows that $P_d^{(k)}$ equals the largest prime
of $kd$. Moreover, it also equals the primitive factor $P^{(1)}_{kd}$. But this contradicts to the fact that $P^{(1)}_{n}$ is prime to $p$ if the largest prime $p$ of $n$ is a factor of $V^{(1)}_{n}$ (see Birkhoff-Vandiver [1, Theorem 4]).

Next we have that the primitive factors $P^{(k)}_{d}$ are pairwise relatively prime. Indeed, if $p$ is a factor of $P^{(k)}_{d_1}$ and $P^{(k)}_{d_2}$ then we may apply Lemma 2(a) to conclude that $d_1/d_2$ is a power of $p$. Hence, $p$ is not a primitive factor of one of $V^{(k)}_{d_1}$ and $V^{(k)}_{d_2}$. This is a contradiction.

Assume that (2) holds for each factor $d$ of $n$. Let $q$ be a prime factor of $P^{(k)}_{d}$ not dividing $kd$. Then it follows from Lemma 2(a) that $kd|q - 1$. Hence we obtain

$$k^2n \mid \phi(P^{(k)}_{d}) \phi(P^{(k)}_{d'})$$

for each $d$ such that $n \neq d^2$. Thus, it is now clear that the factor $\prod_{d|n} \phi(P^{(k)}_{d})$ of $\phi(V^{(k)}_{n})$ is divisible by $k^{d(n)}n^{\frac{d(n)}{2}}$.

It remains to consider only the case $(kd,a,b) = (6,2,1)$ with $d | n$. In this case we have

$$P^{(k)}_{\frac{6}{k}} = \begin{cases} 1, & \text{if } k \text{ is } 1 \text{ or } 2; \\ 3, & \text{otherwise.} \end{cases}$$

Thus, (3) implies that $kn|\phi(P^{(k)}_{\frac{6}{k}})\phi(P^{(k)}_{\frac{6}{k}})$ for $k = 3, 6$. When $k = 2$, we combine (3) with the fact that $2^3 + 1 | V^{(2)}_{n}$. If $k = 1$ then $P^{(1)}_{3} = 7$ and so

$$n^2 \mid \phi(P^{(1)}_{3} P^{(1)}_{\frac{6}{k}}) \phi(P^{(1)}_{\frac{6}{k}})$$

as in the previous case. This completes the proof.

3 Acknowledgment

The author would like to thank the referee for carefully reading the paper and for some suggestions.

References


2010 *Mathematics Subject Classification*: Primary 11A25; Secondary 11B83.

*Keywords*: Euler’s totient function, primitive factor, cyclotomic polynomial.

Received November 25 2014; revised versions received February 4 2015; February 13 2015; February 14 2015. Published in *Journal of Integer Sequences*, February 14 2015.

Return to *Journal of Integer Sequences* home page.