Journal of Integer Sequences, Vol. 18 (2015),
Article 15.3.6

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 φ is Euler's totient function. In this note, we extend his result to values of cyclotomic polynomials.

1 Introduction

Let φ 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 Φ_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:

$$n^{\frac{d(n)}{2}} \mid \varphi(\Phi_1(a^n, b^n))$$

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*

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

where

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

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 Φ_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

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

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

$$\Phi_k(a^n, b^n) = \prod_{e|n} \Phi_{ke}(a, b) \tag{1}$$

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

2 Proof

Let n be an integer relatively prime to a prime p, and let $\mathrm{ord}_p(n)$ 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*

$$\begin{aligned} &(a) \quad v_p(\Phi_k(a,b)) \neq 0 \text{ if and only if } k = p^{v_p(k)}\mathrm{ord}_p(ab^{-1}),\\ &(b) \quad \text{if } v_p(k) \neq 0 \text{ then } v_p(\Phi_k(a,b)) \leq 1 \text{ (except } k = p = 2). \end{aligned}$$

Proof. See Roitman [4]. $\square$

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

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

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 $P_{kd}^{(1)}$. But this contradicts to the fact that $P_n^{(1)}$ is prime to p if the largest prime p of n is a factor of $V_n^{(1)}$ (see Birkhoff-Vandiver [1, Theorem 4]).

Next we have that the primitive factors $P_d^{(k)}$ are pairwise relatively prime. Indeed, if p is a factor of $P_{d_1}^{(k)}$ and $P_{d_2}^{(k)}$ 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 $V_{d_1}^{(k)}$ and $V_{d_2}^{(k)}$. This is a contradiction.

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

$$k^2 n \mid \varphi\big(P_d^{(k)}\big)\varphi\big(P_{\frac{n}{d}}^{(k)}\big) \tag{3}$$

for each d such that $n \neq d^2$. Thus, it is now clear that the factor $\prod_{d|n} \varphi(P_d^{(k)})$ of $\varphi(V_n^{(k)})$ 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 $d \mid n$. In this case we have

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

Thus, (3) implies that $kn \big|\ \varphi\big(P_{\frac{6}{k}}^{(k)}\big)\varphi\big(P_{\frac{nk}{6}}^{(k)}\big)$ for $k = 3, 6$. When $k = 2$, we combine (3) with the fact that $2^3 + 1 \mid V_n^{(2)}$. If $k = 1$ then $P_3^{(1)} = 7$ and so

$$n^2 \big|\ \varphi(P_3^{(1)} P_{\frac{n}{3}}^{(1)})\varphi\big(P_{\frac{n}{6}}^{(1)}\big)$$

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

[1] G. D. Birkhoff and H. S. Vandiver, On the integral divisors of $a^n - b^n$, *Ann. of Math.* **5** (1904), 173–180.

[2] N. G. Gunderson, Some theorems on the Euler ϕ-function, *Bull. Amer. Math. Soc.* **49** (1943), 278–280.

[3] A. Rotkiewicz, On the numbers $\varphi(a^n \pm b^n)$, *Proc. Amer. Math. Soc.* **12** (1961), 419–421.

[4] M. Roitman, On Zsigmondy primes, *Proc. Amer. Math. Soc.* **125** (1997), 1913–1919.

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.