International J. of Math. Sci. & Engg. Appls. (IJMSEA)
ISSN 0973-9424, Vol. 9 No. III (September, 2015), pp. 11-17

VALUES OF CYCLOTOMIC POLYNOMIALS

O. RATNABALA DEVI[1] AND TH. ROJITA CHANU[2]
[1,2] Department of Mathematics,
Manipur University, Imphal-795003, Manipur, India
E-mail: [1] ord2007mu@yahoo.com, [2] rojitachanu@gmail.com

Abstract

In this paper, we study about the prime divisors of the values of cyclotomic polynomials and some properties of cyclotomic polynomials. We also give an improved version of a result given by Motose in 1995.

1. Introduction

Let a and m be two positive integers. The smallest positive integer d satisfying

$$a^d \equiv 1(mod\ m)$$

is called order of a modulo m, denoted by $|a|_m$.

Motose have extensively studied the values of cyclotomic polynomials. In a paper appeared in 1993 [5], he proved that the cyclotomic polynomials $Q_n(x)$ are strictly increasing for $x \geq 1$. Later in 2004 [8] and 2005 [9], this result was subsequently corrected for $x \geq 2$ and $x \geq 3/2$. He also studied about the characterization of prime divisors of values of cyclotomic polynomials. In another paper [6], he gave new proof for the existence of

---

Key Words : *Cyclotomic polynomial, Zsigmondy prime, Mersenne numbers, Fermats number.*

primitive root modulo all primes, odd prime power using cyclotomic polynomials. He also showed that for $a \in \mathbb{N}$, $Q_n(a)$ of distinct degrees are almost relatively prime. The result was extended in 2006 to the case of cyclotomic polynomials and obtained that the greatest common divisor of two cyclotomic polynomials in $\mathbb{Z}[x]$ is either 1 or a prime number [10]. In another paper [7] appeared in 2003, he gave new proof on some fundamental results in finite fields and a new method for the factorization of a number using the properties of cyclotomic polynomials. His works produced excellent properties about cyclotomic polynomials realizing it as an important tool of proving some well known results of finite fields, Ramanunjan's sums and Fibbonacci polynomials. Interestingly, the sequence of numbers generated by the cyclotomic polynomials $Q_n(2)$ are observed to contain the Mersenne numbers 2^p-1 and the Fermat numbers $2^{2^m}+1$ [2]. In this paper, we try to study the divisor of $Q_n(x^m)$ with some conditions on m and n. Further, we study about the multiple prime divisor of the values of $Q_n(x^m)$.

2. Preliminaries

We state below an important result given by Guerrier [3].

Theorem 2.1 : If p is any prime, $p \nmid n$ and $|p|_n = d$, then $Q_n(x)$ factors modulo p into product of $\varphi(n)/d$ distinct irreducible factors each of degree d and $Q_{p^r n}(x) = Q_n(x)^{\varphi(p^r)} (mod\ p)$ for any positive integer r where ϕ is the Euler's ϕ function.

Cheng *et al.* [1] gave a formula for the resultant of cyclotomic polynomials. In proving the formula, they used an important lemma which is the factorization of $Q_n(x^m)$ in $\mathbb{Z}[x]$ and is given as follows:

Lemma 2.2 : For positive integers m and n.

$$Q_n(x^m) = \prod_{[d,m]=mn} Q_d(x)$$

From the above theorem, they deduced the following result:

Lemma 2.3 : Let (m, n)=1. Then

$$Q_n(x^m) = \prod_{d|m} Q_{nd}(x)$$

Motose [7] gave a result about the order of an element in a commutative ring R of positive characteristic which is given as follows:

Theorem 2.4 : Let R be a commutative ring of characteristic $p>0$, namely, containing a prime ring $\mathbb{Z}/p\mathbb{Z}$. Assume $Q_n(a)=0$ for $a \in R$. Then, $n = p^e|a|_p$ where $e \geq 0$.

McDaniel [4] proved the following theorem:

Theorem 2.5 : Let a, r and m be positive integers with $(m, \varphi(m))=1$. If $|a|_m = n$ and $a^{\varphi(m)} \equiv 1 \pmod{m^r}$, then $a^n \equiv 1 \pmod{m^r}$.

Using this theorem, he gave a corollary that whenever $|a|_p = n$ and $a^{p-1} \equiv 1 \pmod{p^r}$ for some odd prime p, and positive integer a and r, then p^r divides $Q_n(a)$.

Motose [6] gave a corollary which is stated as:

Lemma 2.6 : Assume $n, a \geq 2$ and $(n, Q_n(a))=1$. Then, $Q_n(a)$ divides properly $Q_n(a^k)$ for $k \geq 2$ and $(k, n)=1$.

3. Main results

First of all, we give a result on the multiple prime divisor of $Q_n(a^{p^k})$.

Theorem 3.1 : Let p be a prime and $m = np^k, p \nmid n$ and $|a|_p = n$. Then, $p^{k+1}|Q_n(a^{p^k})$.

Proof : By definition, $|a|_p = n$ implies

$$\Rightarrow p \nmid a^d - 1 \qquad for \qquad d < n$$

$$\Rightarrow p \nmid Q_d(a) \qquad for \qquad d < n$$

Also $a^n \equiv 1 \pmod{p}$. And

$$a^n - 1 = \prod_{d|n} Q_d(a)$$

Therefore, $p|Q_n(a)$. Using Theorem 2.1, we have

$$Q_{p^k n}(a) \equiv Q_n(a)^{\varphi(p^k)} (mod\ p)$$

for any positive integer k which implies that $p|Q_{p^k n}(a)$ for any positive integer k. Also from theorem 2.3 we have

$$Q_n(a^{p^k}) = Q_n(a)Q_{np}(a)...Q_{np^k}(a).$$

Hence, $p^{k+1}|Q_n(a^{p^k})$. □

Motose [6] proved the following theorem in 1995.

Theorem 3.2 : Assume $k \geq 2$. Then, $p^k|Q_n(a)$ for some n iff $a^{p-1} \equiv 1 (\text{mod } p^k)$.

It is evident from the following examples that the above theorem is not always true.

Example 3.3 : Let a=7, and n=2. Then, $Q_2(7)$=8. So, in this case k=3 and p=2. But $7 \not\equiv 1(mod\ 2^3)$.

Example 3.4 : Let a=11, and n=2. Then, $Q_2(11)$=12. For this case k=2 and p=2. But $11 \not\equiv 1(mod\ 2^2)$.

For any two positive integers a and n greater than 1, a Zsigmondy prime for the pair a and n is a prime p such that $p \nmid a$ and $|a|_p = n$. Roitman [11] proved that if a, n are integers greater than 1, and p be a prime factor of $Q_n(a)$, then p is a non Zsigmondy prime for the pair a and n iff $p|n$. And, in this case p is the largest prime factor of n, and $n = p^f m$, where m is a positive integer dividing $p-1$. Moreover, $p^2 \nmid Q_n(a)$ unless $p = n$ =2. So, it clarifies that the above Theorem 3.2 does not hold for $p = n$ =2. However, if we assume p to be an odd prime and n to be $|a|_p$, then the result is true.

Now, we give an improved version of the above Theorem 3.2 which is given as follows:

Theorem 3.5 : Let p be an odd prime and $|a|_p = n$. Then, $p^k|Q_n(a)$ iff $a^{p-1} \equiv 1(\text{mod } p^k)$.

Proof : Let $p^k|Q_n(a)$. Then $p^k|a^n$-1. So, by definition of $|a|_p$, $n|p$-1. Hence, $a^{p-1} \equiv 1(\text{mod } p^k)$.

Conversely, let $a^{p-1} \equiv 1(\text{mod } p^k)$. Then, using Theorem 2.5 we have $a^n \equiv 1(\text{mod } p^k)$. Also, we have $a^n - 1 = \prod_{d|n} Q_d(a)$. Since $|a|_p$=n, $p|Q_n(a)$ but $p \nmid Q_d(a)$ for $d < n$ because, if $p|Q_d(a)$ for $d < n$, then $p|x^d - 1$ for $d < n$ which is a contradiction to the definition of order. So, $p^k|Q_n(a)$. □

Proposition 3.6 : If a is an odd positive integer and $n \geq 2$, then $Q_{2^n}(a)$ is twice an odd number.

Proof : Let a=$2k$+1 for some k. Then,

$$\begin{aligned} Q_{2^n}(a) &= a^{2^{n-1}} + 1 \\ &= (2k+1)^{2^{n-1}} + 1 \\ &= (2k)^{2^{n-1}} + ... + 2^{n-1}.2k + 1 + 1 \\ &= 2(2k_1 + 1), \quad for \quad some \quad k_1. \end{aligned}$$

□

Example 3.7 : Let a=5, and n=2. Then $Q_4(5)$=26=2×13.

Theorem 3.8 : Let (m, n)=1, where m and n are positive integers. Then, $Q_n(x^d)$ divides $Q_n(x^m)$ iff $d|m$.

Proof : Let $d|m$, then (d,n)=1. So, from lemma 2.3 we have

$$Q_n(x^d) = \prod_{e|d} Q_{ne}(x)$$

and

$$Q_n(x^m) = \prod_{f|m} Q_{nf}(x)$$

Since $d|m$, $e|m$. Hence, $Q_n(x^d)|Q_n(x^m)$.

Conversely, let $Q_n(x^d)|Q_n(x^m)$. Since the roots of $Q_n(x^d)$ are the d^{th} roots of the n^{th} roots of unity, the roots of $Q_n(x^d)$ are nd^{th} roots of unity including all the primitive nd^{th} roots of unity. This implies that $Q_{nd}(x)|Q_n(x^d)$. Also

$$Q_n(x^m) = \prod_{s|m} Q_{ns}(x)$$

implies that

$$Q_{nd}(x) \;\; divides \;\; \prod_{s|m} Q_{ns}(x).$$

Since $Q_n(x)$ is irreducible over $\mathbb{Z}$,

$$\begin{aligned} Q_{nd}(x) &= Q_{ns}(x) \;\; for \;\; some \;\; s \\ \Rightarrow nd &= ns \\ \Rightarrow d &= s \end{aligned}$$

which implies $d|m$. □

Example 3.9 : $Q_3(2^4)$=13× 21 and $Q_3(2^2)$=21 i.e. $Q_3(2^2)$ divides $Q_3(2^4)$.

The corollary given below generalizes the Lemma 2.6 of Motose [6].

Corollary 3.10 : Let $n, a \geq 2$ and (m,n)=1, where m, a and n are positive integers. Then, $Q_n(a^d)|Q_n(a^m)$ iff $d|m$.

Motose [7] have shown the following theorem 3.11 in 2003.

Theorem 3.11 : For a natural number n, let a and m be natural numbers such that (am,n)=1 and $a^m \equiv 1 (\text{mod } n)$. Then, n=$\prod_{d|n}(n, Q_d(a))$, where (s,t) means the greatest common divisor of two numbers s and t.

We now give two different forms of the Theorem 3.11.

Theorem 3.12 : For a natural number n, let a and m be natural numbers such that (am,n)=1, $a^m \equiv 1 (\text{mod } n)$ and m=$m_1 m_2$. Then,

(i) $n = \prod_{d|m_1}(n, Q_d(a^{m_2}))$

(ii) if $(m_1, m_2) = 1, n = \prod_{d|m_1}\prod_{e|m_2}(n, Q_{de}(a))$

such that $(n, Q_d(a^{m_2}))$ and $(n, Q_{d'}(a^{m_2}))$ are relatively prime for distinct d and d'.

Proof : (i) We have

$$\begin{aligned} n &= (n, a^{m_1 m_2} - 1) \\ &= (n, (a^{m_2})^{m_1} - 1) \\ &= (n, \prod_{d|m_1} Q_d(a^{m_2})) \end{aligned}$$

Suppose p is a common prime divisor of $(n, Q_d(a^{m_2}))$ and $(n, Q_{d'}(a^{m_2}))$, where d, d' are distinct divisors of m_1. Then, p divides n, $Q_d(a^{m_2})$ and $Q_{d'}(a^{m_2})$. This implies $d = p^f |a^{m_2}|_p$ and $d' = p^{f'} |a^{m_2}|_p$ for some f and f'. But we have (n, m_1)=1. So, $d = |a^{m_2}|_p$ and $d' = |a^{m_2}|_p$. Hence, for distinct d and d', $(n, Q_d(a^{m_2}))$ and $(n, Q_{d'}(a^{m_2}))$ are relatively prime. Therefore,

$$n = \prod_{d|m_1}(n, Q_d(a^{m_2}))$$

(ii) If $(m_1, m_2) = 1$, then applying lemma 2.3 to (i) we get

$$n = \prod_{d|m_1}(n, \prod_{e|m_2} Q_{de}(a))$$

Proceeding the same line of proof as in (i) one can show that $(n, Q_{de}(a))$ and $(n, Q_{d'e'}(a))$ are relatively prime for distinct de and $d'e'$. So,

$$n = \prod_{d|m_1}\prod_{e|m_2}(n, Q_{de}(a))$$

□

Acknowledgments

Authors are much thankful for financial assistance by CSIR under SRF scheme.

References

[1] Cheng C. C., Mckay J. H. and Wang S. S., Resultants of cyclotomic polynomials, Proc. Amer. Math. Soc., 123(4) (1995), 1053-1059.

[2] Gallot Y., Cyclotomic polynomials and prime numbers, http://perso.orange.fr/yves.gallot/papers/cyclotomic.pdf, (2001).

[3] Guerrier W. J., The factorization of the cyclotomic polynomials mod p, Amer. Math. Monthly, 75(1) (1968), 46.

[4] McDaniel W. L., On multiple prime divisors of cyclotomic polynomials, Mathematics of Computation. 28(127) (1974), 847-850.

[5] Motose K., On values of cyclotomic polynomials, Math. J. Okayama Univ., 35(1) (1993), 35-40.

[6] Motose K., On values of cyclotomic polynomials II, Math. J. Okayama Univ., 37 (1995), 27-36.

[7] Motose K., On values of cyclotomic polynomials V, Math. J. Okayama Univ., 45 (2003), 29-36.

[8] Motose K., On values of cyclotomic polynomials VII, Bull. Fac. Sci. Tech. Hirosaki Univ., 7 (2004), 1-8.

[9] Motose K., Ramanunjan's sums and cyclotomic polynomials, Math. J. Okayama Univ., 47 (2005), 65-74.

[10] Motose K., On euclidean algorithm, Math. J. Okayama Univ., 48 (2006), 1-7.

[11] Roitman M., On Zsigmondy primes, Proc. Amer. Math. Soc., 125(1) (1997), 1913-1919.