Math. J. Okayama Univ. 35(1993), 35-40

ON VALUES OF CYCLOTOMIC POLYNOMIALS

KAORU MOTOSE

It is very important to study values of cyclotomic polynomials, especially, values for integers (cyclotomic numbers) because important theorems were proved using properties of these values, for examples, Wedderburn's theorem for finite division rings, Artin's theorem for the orders of simple groups (see [1], [2]) and Bang's theorem where we shall give a simple proof of his theorem in the section 2 of this paper (see [3], [5, p.221]).

In the Galois theory of commutative rings, I. Kikumasa and T. Nagahara proved that the polynomials $f_n(x) = \sum_{d|n} \mu(d)x^{n/d}$ are strictly increasing functions for $x \geq 1$, where μ is the Möbius function, and they used essentially this property in their paper [4]. We shall show that cyclotomic polynomials $\Phi_n(x)$ have the same property in the section 1 of this paper. For a prime p, the p-part of a natural number m is the largest power of p dividing m.

1. Let $g(x)$ be a real valued and infinitely differentiable function defined on an interval. Then for a natural number n, we define a new function

$$f_n(x) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}x\right).$$

We have the following theorem and corollary.

Theorem 1. (1) *If $g^{(k)}(x) > 0$ for all k, then $f_n^{(k)}(x) > 0$ for all k.* (2) *If $a < g'(x) < a + 1/x$ for $a \geq 1$ then $f_n'(x) > 0$ for $x \geq 1$.*

Proof. We proceed by induction on n. In case (1), let p^s be the p-part of n and $m = n/p^s$. Then we have

$$f_n(x) = \sum_{d|m} \mu(d) g\left(p^s \frac{m}{d}x\right) - \sum_{d|m} \mu(d) g\left(p^{s-1} \frac{m}{d}x\right) = f_m(p^s x) - f_m(p^{s-1}x).$$

Thus it follows from the induction hypothesis that

$$f_n^{(k)}(x) = p^{sk} f_m^{(k)}(p^s x) - p^{(s-1)k} f_m^{(k)}(p^{s-1}x) > 0.$$

In case (2), we get

$$f_n'(x) = \sum_{d|n} \mu(d)\frac{n}{d}g'\left(\frac{n}{d}x\right) = a\phi(n) + \sum_{d|n} \mu(d)\frac{n}{d}(g'\left(\frac{n}{d}x\right) - a)$$
$$> a\phi(n) - \sum_{\mu(\frac{n}{d})=-1} \frac{1}{x} = a\phi(n) - \frac{2^{r-1}}{x} \geq \phi(n) - 2^{r-1} \geq 0.$$

where ϕ is the Euler ϕ function and r is the number of distinct prime divisors of n.

Corollary 1. *The next polynomials are strictly increasing functions for $x \geq 1$.*

$$(1)\ f_n(x) = \sum_{d|n} \mu(d) x^{\frac{n}{d}}$$
$$(2)\ \Phi_n(x) = \prod_{d|n} (x^{\frac{n}{d}} - 1)^{\mu(d)}.$$

Proof. It is sufficient to prove $f_n(e^x)$ and $\log \Phi_n(e^x)$ are strictly increasing functions. The functions e^x and $\log(e^x - 1)$ satisfy the first and the second conditions for $g(x)$ of theorem, respectively.

2. In this section we shall give a simple proof of Bang's theorem. Assume $n \geq 2$ and $a > 1$. Then it follows from Corollary 1 that $\Phi_n(a) > \Phi_n(1) \geq 1$ since $\Phi_n(1)$ is a prime or 1 according as n is a power of a prime or not. However we shall give a much better estimation in the next lemma.

Lemma 1. *We have the next inequality for $a \geq 2$ and $n \geq 2$. We set that r is the number of distinct prime divisors of n, n' is the product of all distinct prime divisors of n and $m = n/n'$.*
In case r is even,

$$a^{\phi(n)} > \Phi_n(a) > \frac{a^m - 1}{a^m} a^{\phi(n)}$$

In case r is odd,

$$\frac{a^m}{a^m - 1} a^{\phi(n)} > \Phi_n(a) > a^{\phi(n)}.$$

Proof. It is easy to see $(1-x^t)(1-x^s) > 1-x^{s-1}$ for $t \geq s > 1$ and $1/2 \geq x > 0$, and so

$$(1-x^{n_1})(1-x^{n_2})\cdots(1-x^{n_k}) > 1-x$$

for $n_1 > n_2 > \ldots > n_k > 1$ and $1/2 \geq x > 0$. It is easy to see that $\Phi_n(a) = \Phi_{n'}(a^m)$ and $\phi(n) = m\phi(n')$. So we may assume n is square free. We set $b = 1/a$. Using the last inequality together with

$$\Phi_n(b) = \frac{\prod_{\mu(d)=1}(1-b^{\frac{n}{d}})}{\prod_{\mu(d)=-1}(1-b^{\frac{n}{d}})},$$

we obtain that in case r is even,

$$\Phi_n(b) = \frac{\prod_{\mu(d)=1}(1-b^{\frac{n}{d}})}{\prod_{\mu(d)=-1}(1-b^{\frac{n}{d}})} < \frac{1-b}{\prod_{\mu(d)=-1}(1-b^{\frac{n}{d}})} < 1,$$

$$\Phi_n(b) > (1-b)\prod_{p|n}\frac{\prod_{s|\frac{n}{p},\mu(s)=-1}(1-b^{ps})}{1-b^p} > 1-b,$$

and in case r is odd,

$$\Phi_n(b) \leq \frac{1}{1-b}\prod_{p|n}\frac{1-b^p}{\prod_{s|\frac{n}{p},\mu(s)=-1}(1-b^{ps})} < \frac{1}{1-b},$$

$$\Phi_n(b) \geq \frac{\prod_{\mu(d)=1}(1-b^{\frac{n}{d}})}{1-b} > 1,$$

where d and p are extended over divisors and prime divisors of n, respectively. Thus we have our result from $\Phi_n(a) = a^{\phi(n)}\Phi_n(b)$.

It is easy to prove the next lemma. We can see this in many text books. In the remainder of this paper, we shall study only cyclotomic numbers and so all small characters represent integers.

Lemma 2. *Let p be prime and let $b \geq 2$. If $b \equiv 1 \bmod p$ in case p is odd and $b \equiv 1 \bmod 4$ in case $p = 2$, then p is the p-part of*

$$\frac{b^p-1}{b-1}.$$

The next lemma shall show that prime divisors of the degree do not so contribute to prime divisors of cyclotomic numbers.

Lemma 3. *Let $a \geq 2$. If p is a prime divisor of n and of $\Phi_n(a)$ where $n \equiv 0 \bmod 4$ in case $p = 2$, then p is the p-part of $\Phi_n(a)$.*

Proof. We obtain that $a^{n/p} \equiv 1 \bmod p$ since $(a^{n/p} - 1)^p \equiv a^n - 1 \equiv 0 \bmod p$. Thus we have also $a^{n/2} \equiv 1 \bmod 4$ in case $p = 2$. It follows from Lemma 2 that p is the p-part of

$$\frac{a^n - 1}{a^{\frac{n}{p}} - 1}$$

with a divisor $\Phi_n(a)$.

The next theorem is a characterization of prime divisors of cyclotomic numbers.

Theorem 2. *We set $n \geq 2$, $a \geq 2$ and $|a|_p$ is the order of $a \bmod p$ for a prime p. Then p is a prime divisor of $\Phi_n(a)$ if and only if $(a, p) = 1$ and $n = p^\gamma |a|_p$ where $\gamma \geq 0$. A prime divisor p of $\Phi_n(a)$ for $n \geq 3$ has the property such that $n = |a|_p$ or p is the p-part of $\Phi_n(a)$ according as $\gamma = 0$ or not.*

Proof. Let p be a prime divisor of $\Phi_n(a)$. Since $\Phi_n(a)$ divides $a^n - 1$ and so $a^n \equiv 1 \bmod p$, we can write $n = p^\alpha |a|_p t$ where $\alpha \geq 0$ and $(p, t) = 1$. If $t \geq 2$, then we have a contradiction $t \equiv 0 \bmod p$ since

$$\frac{a^n - 1}{a^{\frac{n}{t}} - 1}$$

is divisible by $\Phi_n(a)$ and $a^{n/t} \equiv 1 \bmod p$. Thus we obtain $t = 1$.

Conversely we assume $n = p^\gamma |a|_p$. If $p = 2$, then $n = 2^\gamma$ and a is odd. So $\Phi_n(a)$ is even. We may assume p is odd. In case $\gamma \geq 1$, p^γ divides

$$\frac{a^n - 1}{a^{\frac{n}{p^\gamma}} - 1} = \prod_{\gamma \geq \beta \geq 1} \prod_{h | \frac{n}{p^\gamma}} \Phi_{p^\beta h}(a)$$

If p divides $\Phi_{p^\beta d}(a)$ for some divisor d of n/p^γ and $\beta \geq 1$, then we have $(a^d - 1)^{p^\beta} \equiv a^{p^\beta d} - 1 \equiv 0$ and so $a^d - 1 \equiv 0 \bmod p$. But a condition

$|a|_p = n/p^\gamma$ implies $d = n/p^\gamma$. Thus we have p^γ divides

$$\prod_{\gamma\geq\beta\geq 1} \Phi_{p^\beta \frac{n}{p^\gamma}}(a)$$

and so p divides $\Phi_n(a)$ by Lemma 3. In case $\gamma = 0$, it is easy by the same method. The last assertion follows from Lemma 3.

The next is a theorem of A. S. Bang.

Corollary 2. *Let $a \geq 2$ and $n \geq 2$. Then there exists a prime p with $n = |a|_p$ in all except the following pairs: $(n, a) = (2, 2^\gamma - 1)$ or $(6, 2)$.*

Proof. In case $n \geq 3$, we may assume that $p = \Phi_n(a)$ for the largest prime divisor p of n by virtue of Theorem 2. This together with Lemma 1 yields the next inequality.

$$p = \Phi_n(a) > a^{\phi(n)-1} \geq 2^{p-2}$$

This gives the exceptional case $a = 2$ and $n = 6$. In case $n = 2$, we have the exceptional case $2^\gamma = \Phi_2(a) = a + 1$ since our result follows for $a + 1$ with an odd prime divisor.

The next corollary was suggested from Artin's theorem (see [1], [2]).

Corollary 3. *Assume that $\Phi_n(a) = \Phi_m(b)$ where $a, b \geq 2$ and $n, m \geq 3$. Then $n = m$ if and only if $a = b$.*

Proof. Since $\Phi_n(x)$ is strictly increasing for $x \geq 1$ (Corollary 1), we obtain $a = b$ in case $n = m$. Assume $a = b$ and p is the largest prime divisor of $\Phi_n(a) = \Phi_m(b)$. In case $(n, a) = (6, 2)$, it follows from $3 = \Phi_6(2) = \Phi_m(2) > 2^{\phi(m)-1}$ that $m = 6$. In case $(n, a) \neq (6, 2)$, then $n = |a|_p = m$ from Corollary 2.

The next corollary is well known but we shall show some applications to know that Corollary 2 and Theorem 2 are important.

Corollary 4. (1) *There exists a Galois extension over the rational number field such that a given finite abelian group is the Galois group of this extension.*

(2) *The set $\{ns + 1 | s = 1, 2, \ldots\}$ contains infinitely many prime numbers where $n \geq 1$.*

(3) $\Phi_{n-1}(a) \equiv 0 \bmod n$ *if and only if n is a prime and a is a primitive root* mod n *where $a \geq 1$ and $n \geq 2$.*

Proof. (1) Using Corollary 2, we can define inductively distinct prime numbers p_k satisfying $|4|_{p_k} = m_k p_{k-1}$ where $p_0 = 2$ and m_k $(1 \leq k \leq s)$ is the order of a cyclic group appearing in the direct decomposition of a given abelian group. Since Galois group of $\mathbf{Q}(\zeta_k)/\mathbf{Q}$ is a cyclic group of order $p_k - 1$ where $\mathbf{Q}$ is the rational number field and ζ_k is a primitive p_kth root of 1, it is easy to find a cyclic Galois extension field L_k over $\mathbf{Q}$ of degree m_k. The composite field $L_1 L_2 \cdots L_s$ is our object.

(2) Using Corollary 2, we can define inductively distinct prime numbers p_k satisfying $|4|_{p_k} = np_{k-1}$ where $p_0 = 2$.

(3) We may assume $a \geq 2$ and $n \geq 4$. Let p be a prime divisor of n. Then noting $n - 1 = |a|_p$ by Theorem 2 and $|a|_p$ is a divisor of $p - 1$, we obtain that $n = p$ and a is a primitive root mod p. Conversely, if n is a prime and a is a primitive root mod n, then n divides $\Phi_{n-1}(a)$ since $|a|_n = n - 1$ and $a^{n-1} - 1 = \prod_{d|n-1} \Phi_d(a)$.

References

[1] E. Artin: The orders of the linear groups, Comm. Pure Appl. Math. **8**(1955), 355–365.

[2] E. Artin: The order of the classical simple groups, Comm. Pure Appl. Math. **8**(1955), 455–472.

[3] A. S. Bang: Taltheoretiske Undersøgelser, Tidsskrift for Math. **5**(1886), 70–80 and 130–137.

[4] I. Kikumasa and T. Nagahara: Primitive elements of Galois extensions of finite fields, Proc. Amer. Math. Soc., **115**(1992), 593–600.

[5] H. N. Shapiro: Introduction to The Theory of Numbers, 1983. John Wiley & Sons.

Department of Mathematics
Faculty of Science
Hirosaki University
Hirosaki 036, Japan

(*Received August 19,1992*)