Mathematical Journal of Okayama University

Volume 45, *Issue* 1 2003 *Article* 4

JANUARY 2003

On Values of Cyclotomic Polynomials. V

Kaoru Motose*

*Hirosaki University

Math. J. Okayama Univ. **45** (2003), 29–36

ON VALUES OF CYCLOTOMIC POLYNOMIALS. V

Dedicated to emeritus professor Kazuo Kishimoto on his seventieth birthday

Kaoru MOTOSE

In this paper, using properties of cyclotomic polynomial, we shall give a new proof on some fundamental results in finite fields, a new method of factorization of a number, and a suggestion about new cyclic codes.

Cyclotomic polynomials $\Phi_n(x)$ of order n are defined by

$$\Phi_n(x) = \prod_{(k,n)=1} (x - \zeta_n^k)$$

where $\zeta_n = \cos(\frac{2\pi}{n}) + \sqrt{-1}\sin(\frac{2\pi}{n})$ and the product is extended over natural numbers k which are relatively prime to n with $1 \leq k < n$.

The character p represents a prime. All Latin characters mean natural numbers.

1. Basic results

In this section, we shall give some basic results on $\Phi_n(x)$. First, we give a theorem about the order of an element in a commutative ring R of positive characteristic.

Theorem 1. *Let R be a commutative ring of characteristic $\ell > 0$, namely, containing a prime ring $\boldsymbol{Z}/\ell\boldsymbol{Z}$. Assume $\Phi_n(\alpha) = 0$ for $\alpha \in R$. Then $n = \ell^e|\alpha|_\ell$ where $|\alpha|_\ell$ means the order of α and $e \geq 0$.*

Proof. Since $\Phi_n(x)$ divides $x^n - 1$, we have $\alpha^n = 1$. Hence $|\alpha|_\ell$ is a divisor of n and so we can write $n = \ell^e|\alpha|_\ell \cdot t$ where ℓ does not divide t. We set $s = \ell^e|\alpha|_\ell$ and assume $t > 1$. Then $\alpha^s = 1$ and noting $\Phi_n(x)g(x) = \frac{x^{st}-1}{x^s-1} = (x^s)^{t-1} + \cdots + (x^s)^2 + x^s + 1$ for some $g(x) \in \boldsymbol{Z}[x]$, we have a contradiction that ℓ divides t from the next equation

$$0 = \Phi_n(\alpha)g(\alpha) = (\alpha^s)^{t-1} + (\alpha^s)^{t-2} + \cdots + (\alpha^s)^2 + \alpha^s + 1 = t.$$

□

Example 1. In this theorem, it is an important case such that ℓ is prime and $R = \boldsymbol{F}_\ell$. Since $\Phi_{18}(2) = 3 \cdot 19$, we have $18 = 3^2 \cdot |2|_3 = |2|_{19}$. For the numbers 18 and 2, we can find a prime 19 with $18 = |2|_{19}$.

This paper was financially supported by the Grant-in-Aid for Scientific Research from Japan Society for the Promotion of Science (Subject No. 1164003).

Mathematical Journal of Okayama University, Vol. 45 [2003], Iss. 1, Art. 4

From this result, we can prove a special case of Dirichlet theorem with respect to arithmetic progressions, namely, the set $\Delta = \{ns + 1 \mid s = 1, 2, \cdots\}$ contains infinite primes. Setting $p_0 = 1$, let p_k be a prime divisor of $\Phi_{p_{k-1}n}(p_{k-1}n)$ for $k = 1, 2, \cdots$ and set $R_k = \boldsymbol{Z}/p_k\boldsymbol{Z}$. Then it follows from the above theorem that $p_k \in \Delta$ for $k = 1, 2, \cdots$.

We have an easy estimation for values of cyclotomic polynomials (see also [1, Lemma 1]).

Lemma 1. *$(a+1)^{\varphi(n)} \geq \Phi_n(a) > (a-1)^{\varphi(n)}$ for $n \geq 2, a \geq 2$ where $\varphi(n)$ is the number of positive integers $k < n$ with $(k, n) = 1$.*

Proof. It is trivial that $\Phi_n(a) > 0$ for $a > 1$ from the formula

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

where μ is Möbius function. Thus we have for $a > 1$

$$\Phi_n(a) = \prod_{1 \leq k < n, (k,n)=1} |a - \zeta_n^k|.$$

Our result follows from drawing the unit circle and two concentric circles with the same centre $(a, 0)$ and distinct radiuses $a - 1, a + 1$. $\square$

Example 2. $(a+1)^2 > \Phi_6(a) = a^2 - a + 1 > (a-1)^2$ for $a \geq 2$.

Lemma 2 follows from the above lemma and it is necessary for Bang's theorem. For the numbers 18 and 2, we can find a prime 19 with $18 = |2|_{19}$. But for number 6 and 2, we cannot find such a prime because $\Phi_6(2) = 3$. Lemma 2 or Corollary 1 shows that this is the only exceptional case in Theorem 2.

Lemma 2. *Assume that a prime p is a divisor of n and $p = \Phi_n(a)$ for $n \geq 2$ and $a \geq 2$. Then we have $n = 6$ and $a = 2$.*

Proof. If $a \geq 3$, then we obtain a contradiction $p > 2^{p-1}$ from the next inequality

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

Thus we have $a = 2$ and p is odd because $2^n \equiv 1 \bmod p$. If $e \geq 2$ where $n = p^e m$ and $m = |2|_p > 1$, then $p = \Phi_n(2) = \Phi_{pm}(2^{p^{e-1}})$ and $2^{p^{e-1}} \geq 4$. We have the same contradiction as the above. Thus we have $n = p|2|_p$ and $p > 2$. Moreover, we have $3p + 1 > 2^p$ from the next inequality

$$p = \Phi_{pm}(2) = \frac{\Phi_m(2^p)}{\Phi_m(2)} > \left(\frac{2^p - 1}{2 + 1}\right)^{\varphi(m)} \geq \frac{2^p - 1}{3}.$$

Thus $p = 3$ and we obtain an exceptional case $n = 3|2|_3 = 6$. $\square$

The next corollary follows from the above lemma.

Corollary 1. *If $\Phi_n(a)$ is a divisor of n for $n \geq 3$ and $a \geq 2$, then we have $n = 6$ and $a = 2$.*

Proof. If p and q are prime divisors of $\Phi_n(a)$, then p and q are the maximal prime divisor of n by Theorem 1 and little Fermat theorem. Hence we have $p = q$ and $\Phi_n(a)$ is a power of a prime p. On the other hand, we set $b = a^{\frac{n}{p}}$. Then $b \equiv 1 \bmod p$ in case $p > 2$ and $b \equiv 1 \bmod 4$ in case $p = 2$ because a is odd and $n = 2^e \geq 4$ from Theorem 1. In any case, $\Phi_p(b) = \frac{b^p-1}{b-1}$ has a divisor p but has not a divisor p^2. Thus $\Phi_n(a) = p$ because $\Phi_n(a)$ is a divisor of $\frac{a^n-1}{a^{\frac{n}{p}}-1} = \Phi_p(a^{\frac{n}{p}}) = \Phi_p(b)$. Hence our result follows from Lemma 2. □

The following theorem is a basic result about value of cyclotomic polynomials.

Theorem 2 (Bang)**.** *If $n \geq 3, a \geq 2$ and $(n, a) \neq (6, 2)$, then there exists a prime p with $n = |a|_p$.*

Proof. There exists a prime divisor p of $\Phi_n(a)$ since $\Phi_n(a) > 1$. We may assume from Theorem 1 that p is a divisor of n and p is the maximal divisor of n. Hence, p is the only prime divisor of $\Phi_n(a)$, equivalently, $\Phi_n(a)$ is a power of p. Hence $\Phi_n(a) = p$ by the same method as in Corollary 1. We have our result from Lemma 2. □

2. Some fundamental results on finite fields

The next proposition shows that the multiplicative group of a finite field is cyclic.

Proposition 1. *Let G be a finite subgroup of the multiplicative group of a field K. Then G is cyclic.*

Proof. We set $m = |G|$. Then G is contained in the set of roots of $x^m - 1$ in K which has at most m elements. Thus, we obtain $x^m - 1 = \prod_{\alpha \in G}(x - \alpha)$. Hence, $\Phi_m(x)$ has a root $\beta \in G$ since $\Phi_m(x)$ divides $x^m - 1$. If K is of characteristic $p > 0$, then p is not a divisor of m because $x^m - 1$ has no multiple roots, and so $m = |\beta|_p$ by Theorem 1. If K is of characteristic zero, then our assertion is trivial. □

The next theorem is well known. However, it is very fundamental for cyclotomic polynomials and we shall show this for completeness.

Theorem 3. *Let p be a prime and let q be a power of a prime p. If p is not a divisor of n, then $\Phi_n(x) \in \boldsymbol{F}_q[x]$ is the product of irreducible polynomials of the same degree $|q|_n$.*

Mathematical Journal of Okayama University, Vol. 45 [2003], Iss. 1, Art. 4

Proof. Let $f(x)$ be an arbitrary irreducible factor of $\Phi_n(x) \in \boldsymbol{F}_q[x]$ and let ζ be a root of $f(x)$. Then ζ is a root of $\Phi_n(x)$. Thus $n = |\zeta|_p$ by Theorem 1 and so we may assume $\zeta \in \boldsymbol{F}_{q^{|q|_n}}$ from Proposition 1. Since $\boldsymbol{F}_q(\zeta) = \boldsymbol{F}_{q^{\deg f(x)}}$ is a subfield of $\boldsymbol{F}_{q^{|q|_n}}$, $\deg f(x)$ is a divisor of $|q|_n$. On the other hand $|q|_n$ is a divisor of $\deg f(x)$ because $q^{\deg f(x)} \equiv 1 \bmod n$ by $\zeta \in \boldsymbol{F}_q(\zeta)^* = \boldsymbol{F}^*_{q^{\deg f(x)}}$. Thus we have $\deg f(x) = |q|_n$. □

Concerning factorizations of cyclotomic polynomials modulo a prime, we should be use Berlekamp and McEliece's algorithm, and should pay attention to results of G. Stein [see 3].

Example 3. If follows from $4 = |2|_{15}$ that $\Phi_{15}(x) \bmod 2 = x^8 + x^7 + x^5 + x^4 + x^3 + x + 1 = (x^4 + x^3 + 1)(x^4 + x + 1)$.

We shall give an alternative proof of the next well-known theorem. This means that there exist finite fields of arbitrary prime power orders.

Proposition 2. *Let p be a prime and let q be a power of p. For an arbitrary n, There exists an irreducible polynomial of degree n in $\boldsymbol{F}_q[x]$.*

Proof 1. It follows from $n = |q|_{q^n-1}$ that $\Phi_{q^n-1}(x) \in \boldsymbol{F}_q[x]$ has an irreducible factor of degree n. □

Proof 2. In case $n \geq 3$ and $(n, q) \neq (6, 2)$, then we can find a (prime) divisor r of $\Phi_n(q)$ with $n = |q|_r$. Hence $\Phi_r(x) \in \boldsymbol{F}_q[x]$ has an irreducible factor of degree n. In case $n = 2$, $\Phi_{q+1}(x) \in \boldsymbol{F}_q[x]$ has an irreducible factor of degree 2 because $2 = |q|_{q+1}$. In case $n = 6$ and $q = 2$, we obtain $\Phi_9(x) = \Phi_3(x^3) = x^6 + x^3 + 1 \bmod 2$ is irreducible from $6 = |2|_9$. □

In this proposition, the smallest prime divisor r of $\Phi_n(q)$ with $r \nmid n$ is best. Unfortunately, if we can not find a proper divisor, then we set $r = \Phi_n(q)$.

Example 4. Proof 1 is very simple and it is practical to find a primitive polynomial. For example, $\Phi_{2^4-1}(x) = \Phi_{15}(x) \bmod 2 = (x^4+x^3+1)(x^4+x+1)$ (see Example 3). These polynomials are primitive polynomials of order $2^4 - 1 = 15$. The class of x is a generator of $\boldsymbol{F}_{2^4}$. However, if we would like to find an irreducible polynomial of degree n, Proof 2 is very useful. For example, $\Phi_5(x) \bmod 2 = x^4 + x^3 + x^2 + x + 1$ is irreducible because $4 = |2|_5$ by $\Phi_4(2) = 5$.

3. A method of a factorization of a number

Let n be a number, let m be the product of distinct prime divisors of n, let p be a fixed prime divisor of m and let $m' = \frac{m}{p}$. We can see easily the next equation

$$\Phi_n(x) = \Phi_m(x^{\frac{n}{m}}) \text{ and } \Phi_m(x) = \prod_{d|m'} \Phi_p(x^d)^{\mu(\frac{m'}{d})}.$$

The above equation and next lemma show us that factorizations of cyclotomic numbers $\Phi_n(a)$, especially $\Phi_p(a)$ of a prime order p are essential in factorizations of numbers.

Proposition 3. *For a natural number n, let a and m be natural numbers such that $(am, n) = 1$ and $a^m \equiv 1 \bmod n$. Then $n = \prod_{d|m}(n, \Phi_d(a))$, where (s, t) means the greatest common divisor of two numbers s and t.*

Proof. We set $s_d = (n, \Phi_d(a))$, where d is a divisor of m. If p is a common prime divisor of s_d and $s_{d'}$, then $d = |a|_p = d'$ from Theorem 1 because p is not a divisor of both d and d'. Thus we can see $(s_d, s_{d'}) = 1$ for distinct divisors d, d' of m. Hence we have

$$n = (n, a^m - 1) = (n, \prod_{d|m} \Phi_d(a)) = \prod_{d|m}(n, \Phi_d(a)).$$

□

If we use Proposition 3 to see a factor of a number, we should find m for numbers n and a, and the factorization of m. So, we can only use this in case n is a small number and m is a product of small primes.

Example 5. Setting $a = 2$ for the number $n = 1111111111$, we have $1111111111 = 11 \cdot 41 \cdot 271 \cdot 9091$ for $m = 54540 = 2^2 \cdot 3^3 \cdot 5 \cdot 101$.

Lemma 3. *Let n be a divisor of $\Phi_m(a)$ and $(m, n) = 1$. If $m > \sqrt{n}$, then n is prime.*

Proof. Let p be a minimum prime divisor of n. Then p is a divisor of $\Phi_m(a)$ and so $m = |a|_p$ is a divisor of $p - 1$. Thus $n = p$ is prime because

$$p > |a|_p = m > \sqrt{n}.$$

□

Example 6. $\Phi_6(6) = \Phi_5(2) = 31$ and $6 > \sqrt{31}$ implies that 31 is prime by the above lemma but $\sqrt{31} > 5$ shows that the converse of the above lemma does not hold.

Pocklington's theorem is easily proved using the values of cyclotomic polynomials.

Proposition 4 (Pocklington)**.** *Let n, f and r be natural numbers such that $n - 1 = fr$ with $(f, r) = 1$, where the factorization of f is well known, every* *divisor ℓ of r is larger than c and $fc \geq \sqrt{n}$. If there exists a number $a > 1$ such that*

$$(1)\ a^{n-1} \equiv 1 \bmod n \textit{ and } (2)\ (a^{\frac{n-1}{q}} - 1, n) = 1$$

for every prime divisor q of f, then n is prime.

Proof. It follows from the condition (2) that

$$n = \prod_{d|f} (n, \Phi_d(a^r)) = (n, \Phi_f(a^r))$$

and so n is a divisor of $\Phi_f(a^r)$. On the other hand $n = \prod_{\ell|r}(n, \Phi_\ell(a^f))$. Let p be the smallest divisor of n. Then $f = |a^r|_p$ is a divisor of $p-1$ and $\ell = |a^f|_p$ is a divisor of $p-1$ for some ℓ. Thus $f\ell$ is a divisor of $p-1$ and $p > f\ell > fc \geq \sqrt{n}$. □

Example 7. We can see $n = \Phi_{17}(976)$ is prime from this theorem and program by Yuji Kida written in UBASIC. His program found numbers $a = 3, f = 2^4 \cdot 17 \cdot 61 \cdot 73 \cdot 977 \cdot 7177 \cdot 12433 \cdot 13049$, and $c = 131071$ and showed $n = \Phi_{17}(976)$ is prime.

4. A suggestion about cyclic codes

In this section, we consider cyclic codes like a Golay code. A generator polynomial of the Golay code is one of two factors in $\Phi_{23}(x) \bmod 2$. We choose one of two factors in cyclotomic polynomials over finite fields and we use this as generator polynomials of cyclic codes. For this purpose, we should find a pair (ℓ, r) such that r is a power of a prime and ℓ is a divisor of $\Phi_{\frac{\varphi(\ell)}{2}}(r)$. If we find such a pair, $\Phi_\ell(x)$ over $\boldsymbol{F}_r$ is factorized into two irreducible polynomials.

Example 8. We find a pair (ℓ, r) satisfying the above conditions where $\ell \leq 50,\ r \leq 10$.

$$\begin{aligned}
&r = 2;\ \ell = 7, 17, 23, 41, 47\\
&r = 3;\ \ell = 11, 23, 37, 47\\
&r = 4;\ \ell = 3, 5, 7, 11, 13, 19, 23, 29, 37, 47\\
&r = 5;\ \ell = 4, 11, 19, 21, 29, 41\\
&r = 7;\ \ell = 3, 6, 8, 31, 47\\
&r = 8;\ \ell = 17, 23, 41, 47\\
&r = 9;\ \ell = 4, 5, 7, 10, 11, 17, 19, 23, 29, 31, 34, 43, 47
\end{aligned}$$

A special case of our consideration can be written in the quadratic residues. This is showed in Lemma 4. We shall represent Legendre symbol by $\left(\frac{a}{p}\right)$.

Lemma 4. *Let p be an odd prime and let q, r be natural numbers such that $p = 2q + 1 > r > 1$. Then clearly $|r|_p > 1$ and*

(1) $\left(\frac{r}{p}\right) = 1$ *if and only if $|r|_p$ is a divisor of q.*

(2) *If q, r are odd primes, then $\left(\frac{-p}{r}\right) = 1$ if and only if $|r|_p = q$. In particular, if $q \equiv -1 \bmod r$, then $|r|_p = q$.*

(3) *If q is an odd prime, then $q \equiv -1 \bmod 4$ if and only if $|2|_p = q$.*

Proof. The assertion (1) follows from $r^q = r^{\frac{p-1}{2}} \equiv \left(\frac{r}{p}\right) \bmod p$.

The assertion (2) is clear from

$$\left(\frac{r}{p}\right) = (-1)^{\frac{p-1}{2}\frac{r-1}{2}}\left(\frac{p}{r}\right) = (-1)^{q\frac{r-1}{2}}\left(\frac{p}{r}\right) = \left(\frac{-p}{r}\right).$$

The (3) follows from that (1) and the next equation

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{q\frac{q+1}{2}} = (-1)^{\frac{q+1}{2}}.$$

□

It follows from this lemma that for a prime r, the cyclotomic polynomial $\Phi_p(x) \bmod r$ factorizes two irreducible polynomials $f(x), g(x)$ of same degree q. This fact suggests that $(p, q+1, d)$ code over $\boldsymbol{F}_r$ with generator polynomial $g(x)$ of degree q where $q + 1$ is the dimension of a code subspace C of the vector space $\boldsymbol{F}_r^p$, and d is the minimum distance of C.

Example 9.

q	p	r	d	$g(x)$
3	7	2	3	$x^3+x+1,\ x^3+x^2+1$
5	11	3	5	$x^5-x^3+x^2-x-1,\ x^5+x^4-x^3+x^2-1$
11	23	2	7	$x^{11}+x^9+x^7+x^6+x^5+x+1$
11	23	2	7	$x^{11}+x^{10}+x^6+x^5+x^4+x^2+1$
23	47	2	11	$x^{23}+x^{19}+x^{18}+x^{14}+x^{13}+x^{12}+x^{10}+x^9$ $+x^7+x^6+x^5+x^3+x^2+x+1$
23	47	2	11	$x^{23}+x^{22}+x^{21}+x^{20}+x^{18}+x^{17}+x^{16}+x^{14}$ $+x^{13}+x^{11}+x^{10}+x^9+x^5+x^4+1$

Concerning computations in this paper, we used some programs written in UBASIC and a personal computer IBM Intellistation E Pro. The program language UBASIC was designed by Professor Yuji Kida, Rikkyo University, Tokyo, Japan.

Acknowledgements. The author would like to express great thanks to the referee for useful suggestions and corrections.

Mathematical Journal of Okayama University, Vol. 45 [2003], Iss. 1, Art. 4

References

[1] K. Motose, *On value of cyclotomic polynomials*, Math. J. Okayama Univ. **35**(1993), 35–40.

[2] R. Lidl and H. Niederwriter, *Finite fields*, Encyclopedia of Mathematics and Applications, **20**, Cambridge University Press, London, 1984.

[3] G. Stein, *Factoring cyclotomic polynomials over large finite fields, Finite fields and applications*, London Math. Soc. Lecture Note Ser., 233 (Glasgow, 1995), Cambridge Univ. Press, Cambridge, 1996, 349–354.

Kaoru Motose
Department of Mathematical System Science
Faculty of Science and Technology
Hirosaki University
Hirosaki 036-8561, Japan
e-mail address: skm@cc.hirosaki-u.ac.jp

(*Received December 3, 2002*)
(*Revised July 9, 2003*)