On values of cyclotomic polynomials

K. Motose

韓国での Conference における Program と口頭発表 (July 2, 1999) の OHP 原稿。

June 2003 本瀬香

CONFERENCE PROGRAM

June 28, Monday

Morning Session (Emerald-Ruby Room)

- 9: 00 - 9: 20 Welcoming Address, The President of Kyungpook National University, Korea
- 9: 30 - 10:15 "Non-commutative Valuation Rings and Their Global Theories", H. Marubayashi, Naruto University of Education, Japan
- 10:25 - 11:10 "Auslander-Gorenstein Rings", J. Clark, University of Otago, New Zealand
- 11:20 - 12:05 "Multiplier Hopf Algebras of Discrete Type", Yinhuo Zhang, Max-Plack Institute of Mathematics, Germany

Lunch Break

- 1:40 - 2:25 "The Connes Spectrum of a Hopf Algebra Action", J. Osterburg, University of Cincinnati, USA

Afternoon Session (Emerald-Ruby Room)

Time	Room (Emerald)	Room (Ruby)
2:40-3:25	"Semicentral Reduced Rings" G. F. Birkenmeier, Univ. of Southwestern Louisiana, USA	"A Survey on *-Operations" Young Soo Park, Kyungpook National Univ., Korea
3:35-4:00	"The Property (DF) and Simple Unit Regular Rings" M. Kutami and H. Tsunashima, Yamaguchi Univ., Japan	"Poisson Algebras" Sei-Qwon Oh, Chungnam National Univ., Korea
4:05-4:30	"On the Maximal t-Corational Extensions of Modules" S. Morimoto, Hagi Koen Gakuin, Japan	"Hopf Algebra Coaction and its Application to Group Graded Algebra" Guilong Liu, China Univ. of Geoscience, China
4:40-5:05	"Rings in which Nilpotent Elements form an Ideal" Yang Lee, Pusan National Univ., Korea	"Homological Dimensions of Smash Products and the Surjectivity of Trace Maps" Zhixi Wang, Capital Normal Univ., China
5:10-5:35	"When is a Direct Sum of Uniform Modules a Normal CS-Module?" Y. Kuratomi, Yamaguchi Univ., Japan	"A Generalization of Herstein's Famous Theorem" Changlin Fu, University of Science and Technology, China

5:40–6:05	"Relations between Armendariz Rings and Semicommutative Rings" Chan Huh, Pusan National Univ., Korea	"A Characterization of Generalized Chain Conditions for N-Modules" Yong Uk Cho, Silla Univ., Korea

BANQUET will start at 7:00 PM

June 29, Tuesday

Morning Session (Emerald-Ruby Roonm)

- 9:00 - 9:45 "Dual-Bimodules and Nakayama Permutations", Y. Kurata, Yamaguchi University and Kanagawa University, Japan
- 9:55 - 10:40 TBA, F. van Oystaeyen, University of Antwerp, Belgium
- 10:50 - 11:35 "Good Conditions for the Total", F. Kasch, Universitaet Muenchen, Germany
- 11:45 - 12:30 "On Torsion-Free Modules over Pruefer Domains", K. M. Rangaswamy, University of Colorado at Colorado Springs, USA

Lunch Break

Afternoon Session (Emerald-Ruby Room)

- 2:00 - 2:45 "Tilting Theory and Derived Equivalences", D. Happel, TU-Chemnitz, Germany

Time	Room (Emerald)	Room (Ruby)
3:00-3:25	"Tilting Module and Slice" Yanan Lin, Xiamen Univ., China	"Generalized Principally Injective Maximal Ideals" Jin Yong Kim, Nam Kyun Kim, and Sang Bok Nam, Kyung Hee Univ. and Kyungdong Univ., Korea
3:30-3:55	"Cohomologies of Monomial Algebras" Pu Zhang, Univ. of Science and Technology, China	"Rings with Finitely generated Faithful Modules contain Generators" H. Yoshimura, Yamaguchi Univ., Japan
4:05-4:50	"Group Acting on Derived Categories" A. Zimmernann, Univ. de Picardie, France	"Gorenstein Injective Modules over Iwanaga-Gorenstein Rings" O. M. G. Jenda, Auburn Univ., USA
5:00-5:25	Quadratic Bimodule Problem O. Iyama, Kyoto Univ., Japan	"Some Results on Skew Polynomial Rings over a Reduced Ring" Hongkee Kim, Gyeongsang National Univ., Korea
5:30-5:55	"Dualizing Modules for Orders and Artin Algebras" K. Nishida, Shinshu Univ., Japan	"On Regular Rings with Prime Centers" Xianneng Du, Anhui Univ., China

June 30, Wednesday

Morning Session (Emerald-Ruby Room)

- 9:00 - 9:45 "Complete MV-Algebras", Tae Ho Choe, McMaster University, Canada
- 9:55 - 10:40 "Tree Algebras, Hecke Algebras, and Cohen-Macaulay Modules", K. W. Roggenkamp, Universitaet Stuttgart, Germany
- 10:50 - 11:35 "Hopf Algebras over a Finite Field, Using Personal Computers", K. Yokogawa, Okayama Science University, Japan
- 11:45 - 12:30 "Stratification of Rings", V. Dlab, Carleton University, Canada

Lunch Break

Afternoon Session (Emerald-Ruby Room)

Time	Room (Emerald)	Room (Ruby)
3:00-3:25	"Adjacency Algebras of Association Schemes" A. Hanaki, Shinshu Univ., Japan	"On Rings with Skew Differential Operators on Commutative Rings" Y. Hirano, Okayama Univ., Japan
3:30-3:55	"On Linkage of Cohen-Macaulay Modules" Y. Yoshino, Okayama Univ., Japan	"On Inertial Subalgebras of Finite Rings" T. Sumiyama, Aichi Tech., Japan
4:05-4:50	Multipler Hopf Algebras of Discrete type Zhizhong Chen, Northen Jiaotong Univ., China	"Some New Results on Nil Rings" E. R. Puczylowski, Univ. of Warsaw, Poland
5:00-5:25	"On Some Kind of Duality" M. Sato, Yamanashi Univ., Japan	"Remarks on Ore Extensions of Baer and PP Rings" Chan Yong Hong and Tai Keun Kwak, Kyung Hee Univ. and Daejin Univ., Korea
5:30-5:55	"Every Right Self-Injective Right Perfect Ring is QF" Mingyi Wang, Southwest Jiaotong Univ., China	"Self-Duality of QH Rings with Homogeneous Socles and Left Global Dimension at most 2" Y. Baba, Osaka Kyoiku Univ., Japan

BANQUET will start at 6:30 PM

PROBLEM SESSION: 8:00PM at Emerald-Ruby Room

July 1,Thursday : Sightseeing and / or Hiking Excursion

July 2, Friday

Morning Session (Emerald-Ruby Room)

- 9:20 - 10:05 TBA, A. Nakajima, Okayama University, Japan
- 10:15 - 11:00 "Study of Hopficity in Certain Class of Algebras", K. Varadarajan, University of Calgary, Canada
- 11:10 - 11:55 Some recent results on CS-modules and rings, S. K. Jain, Ohio University, USA
- 12:05 - 12:30 "On Values of Cyclotomic Polynomials", K. Motose, Hirosaki University, Japan

Lunch Break

Afternoon Session

Time	Room (Emerald)	Room(Ruby)
2:00-2:45	"On FI-Extending Modules" S. Tariq Rizvi, Ohio State Univ. at Lima, USA	"On Representations of Lie-Admissible Algebras and Lie Algebras of Poisson Algebras" K. I. Beidar, National Cheng Kung Univ., Taiwan
2:55-3:20	"Left Global Dimensions and Inverse Polynomial Modules" Sangwon Park, Dong A Univ., Korea	TBA Miaosen Chen, Zhejiang Normal Univ., China
3:25-4:10	"On Quasi-Frobenius Rings" M. F. Yousif, Ohio State Univ. at Lima, USA	"Hopf Algebras and Azumaya Algebras" R. Alfaro, Univ. of Michigan at Flint, USA
4:20-4:45	Self-duality and H-rings J. Kado, Osaka City Univ., Japan	On wild algebras H. Nagase, Osaka City Univ., Japan
4:50-5:15	"Prime Radicals of Differential Operator Rings" Juncheol Han, Kosin Univ., Korea	"The Module of Differentials of a Noncommutative Ring Extension" H. Komatsu, Okayama Prefectural Univ., Japan

5:20–5:45	"On Generalized Principally Injective Rings" Jianlong Chen and Nanqing Ding Southeast Univ. and Nanjing Univ., China	"A Generalization of Maschke's Theorem" T. Nishinaka, Okayama Shouka Univ., Japan

- 5:50 – 6:15 On generalization of injectivity, Jianlong Chen, Southeast University, China

July 3, Saturday

Morning Session (Emerald-Ruby Room)

• 9:00 - 9:45 "On the Torsion Nilpotence of the Closed Prime Radical of Rings with Relative Krull Dimension", M. L. Teply, University of Wisconsin at Milwaukee, USA

• 9:55 - 10:40 "The Theory of Nakayama, Morita-Azumaya, Harada in a Bottom Current of the Artinian Rings", K. Oshiro, Yamaguchi University, Japan

Time	Room (Emerald)	Room (Ruby)
11:00-11:45	"Noetherian Semigroup Algebras" E. Jespers, Vrije Univ. of Brussel, Belgium	"Slender Modules over Matlis Domains" S. B. Lee, Sangmyung Univ., Korea
11:55-12:20	"On Divisible Envelopes" Seog Hoon Rim, Kyungpook National Univ., Korea	"Factorable Domains" David F. Anderson, Hwankoo Kim*, Jeanam Park, Univ. of Tennessee, Kyungpook National Univ., and Inha Univ., Korea
12:25-12:50	"Distinguished Domains" Dong Je Kwak, Kyungpook National Univ., Korea	"Some Structures of Bicrossproduct Hopf Algebras", Suk Bong Yoon, Kyungpook National Univ., Korea

On values of cyclotomic polynomials

K. Motose

November 5th 2002

1. Definitions

Cyclotomic polynomials are defined by

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

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

Example.

$$\Phi_1(x) = x - 1,\ \Phi_2(x) = x + 1,\ \Phi_3(x) = x^2 + x + 1,$$
$$\Phi_4(x) = x^2 + 1,\ \Phi_5(x) = x^4 + x^3 + x^2 + x + 1,$$
$$\Phi_6(x) = x^2 - x + 1,\ \ldots$$

Möbius' function μ is also defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } p^2 \mid n \text{ for a prime } p, \\ (-1)^r & \text{if } n = p_1 p_2 \ldots p_r \text{ where } p_k \text{ are all} \\ & \text{distinct primes.} \end{cases}$$

Example.

$$\mu(1) = 1,\ \mu(2) = -1,\ \mu(3) = -1,\ \mu(4) = 0,$$
$$\mu(5) = -1, \mu(6) = 1,\ \ldots$$

Fundamental properties

We can now state fundamental properties of cyclotomic polynomials.

1. $x^n - 1 = \prod_{d|n} \Phi_d(x)$ where d runs through positive divisors of n. Thus $n = \sum_{d|n} \varphi(d)$.
2. $\Phi_n(x) \in \boldsymbol{Z}[x]$ and the leading coefficient of $\Phi_n(x)$ is 1.
3. $\Phi_n(x) = \prod_{d|n}(x^d - 1)^{\mu(\frac{n}{d})}$. Thus $\varphi(n) = \sum_{d|n} d\mu(\frac{n}{d})$.
4. $\Phi_n(x)$ is irreducible in $\boldsymbol{Q}[x]$.

1. This formula is equivalent to the definition of cyclotomic polynomials.
2. It is easy to see from the above that $\Phi_n(a)$ is an integer for an integer a. It is important for us.
3. This formula is useful for calculations of cyclotomic polynomials. For example,

$$\Phi_6(x) = \frac{(x^6 - 1)(x - 1)}{(x^3 - 1)(x^2 - 1)} = \frac{x^3 + 1}{x + 1} = x^2 - x + 1$$

4. This is essential for Gauss' theorem which give necessary and sufficient condition that regular polygon can be constructed by using only ruler and compass. Galois groups of cyclotomic fields are determined from this.

We provide an estimation of values of cyclotomic polynomials.

Theorem 1. $\Phi_n(x)$ are strictly increasing functions for $x \geq 2$ and

$$a^{\varphi(n)+1} > \Phi_n(a) > a^{\varphi(n)-1} \quad \text{for } n, a \geq 2.$$

where $\varphi(n)$ is the degree of $\Phi_n(x)$ which is the number of positive integers $k < n$ with $(k, n) = 1$.

Example. $\Phi_6(x) = x^2 - x + 1$ is strictly increasing for $x \geq 1$ and $a^3 > a^2 - a + 1 > a$ for $a \geq 2$.

Fermat's little Theorem. If p is a prime and a is a positive integer with $p \nmid a$, then $a^{p-1} \equiv 1 \bmod p$.

Example. $3^6 \equiv 1 \bmod 7$.

If p is a prime and a is a positive integer with $p \nmid a$, then the least positive integer s such that $a^s \equiv 1 \bmod p$ is called the order of a modulo p. We denote the order of a modulo p by $|a|_p$. It is easy to show that $|a|_p$ is a divisor of m if $a^m \equiv 1 \bmod p$.

Example. We have $|2|_7 = 3$ from

$$2^1 \equiv 2 \bmod 7,\ 2^2 \equiv 4 \bmod 7,\ 2^3 \equiv 1 \bmod 7$$

Let q be a prime divisor of a Mersenne number $2^p - 1$ where p is prime. Then $p = |2|_q$ since p is prime. Thus p is a divisor of $q - 1$ and $q > p$. This shows that there exist infinitely many prime numbers. In fact, starting from 2 we have 3, 7, 127, ... In this argument, $p = |2|_q$ is most important. We can generalized this to the next theorem which is easy to prove, but powerful for us.

Theorem 2. If $p \mid \Phi_n(a)$, then $n = p^e|a|_p$.

Example. 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 $18 = |2|_{19}$. But for number 6 and 2, we cannot find such a prime because $\Phi_6(2) = 3$. This is the only exceptional case in the next theorem.

The next was known before one century more and was found again by many mathematicians, but is not so popular for us. This follows from the above theorem and an estimation cited before.

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

4. Applications to algebra

Cyclotomic polynomials provide some important theorems on algebra.

1. The multiplicative group of a finite field is cyclic.
2. Artin's theorem with respect to the orders of finite (linear) simple groups.
3. Wedderburn's theorem: Finite division rings are commutative.
4. Special case of Dirichlet's theorem: The next arithmetic progression for a natural number d contains infinitely many primes.

$$1,\ 1+d,\ 1+2d,\ \ldots,\ 1+nd,\ \ldots\ .$$

5. There exists a Galois extension over the rational number field such that a given finite abelian group is the Galois group of this extension.
6. Primality tests of big primes.

1. It is easy to prove from Theorem 2 and the next equation for a prime field F_p

$$\prod_{d|p-1} \Phi_d(x) = x^{p-1} - 1 = \prod_{\alpha \in F_p^*} (x - \alpha).$$

Just a modification of Theorem 2 gives the same proof in general.

2. For example, we set the next number $N_n(q)$ for a natural number $n \geq 2$ and a prime power $q = p^r$ where p is prime. This number is the order of the projective special linear group $\mathrm{PSL}(n, q)$

$$N_n(q) = \frac{1}{(n, q-1)} q^{\frac{n(n-1)}{2}} (q^n - 1)(q^{n-1} - 1) \cdots (q^2 - 1)$$

If $N_n(q) = N_{n_0}(q_0)$ for different pairs $(n, q) \neq (n_0, q_0)$, then $N_3(4) = N_4(2) = 20160, N_2(7) = N_3(2) = 168$, and $N_2(5) = N_2(4) = 60$.

3. In the last part of Witt's proof, we have the equation $\Phi_n(q)|q-1$. This contradicts to $\Phi_n(q) > q-1$. However, It is easy to see $n = 1$ from Theorem 2.

4. It is a special case but is used frequently.

5. No comments.

6. For example, the next is an extension of Lucas' or Pepin's test.

Theorem 4. (1) $p > 3$ is prime if and only if there exists an integer c such that $\left(\frac{c}{p}\right) = -1$ and $\Phi_{p-1}(c) \equiv 0 \bmod p$.

(2) $p > 3$ is prime if and only if there exists an integer $c > 1$ such that $(c^3 - c, p) = 1, \gamma = c + \sqrt{c^2 - 1}$, $\left(\frac{2c+2}{p}\right) = \left(\frac{c^2-1}{p}\right) = -1$ and $\Phi_{p+1}(\gamma) \equiv 0 \bmod p\mathcal{O}_\gamma$ where $\mathcal{O}_\gamma$ is the ring of algebraic integers in $\boldsymbol{Q}(\gamma)$

5. Cipher

Pseudo primes are useful for a cipher.

Definition. A composite number n is a a-pseudo prime if and only if $a^{n-1} \equiv 1 \bmod n$

Roughly speaking, every a-pseudo primes is a product of divisors of cyclotomic numbers $\Phi_n(a)'s$ for some n, and conversely. The next is a special case, but useful for a cipher.

Theorem 5. If d is a divisor of $\Phi_n(a)$ and $(d, n) = 1$, then $a^{d-1} \equiv 1 \bmod d$

We shall present a cipher using cyclotomic polynomials. We shall represent by $\boldsymbol{Z}^s$ the direct sum of the ring $\boldsymbol{Z}$ of integers. Let $\mathbf{1}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{n}$ be the elements of $\boldsymbol{Z}^s$ such that $\mathbf{1} = (1, 1, \ldots, 1)$ is the identity of $\boldsymbol{Z}^n$,

$$\boldsymbol{a} = (a_1, a_2, \ldots, a_s), \boldsymbol{b} = (b_1, b_2, \ldots, b_s), \text{ and}$$
$$\boldsymbol{n} = (n_1, n_2, \ldots, n_s)$$

We use the following notations.

$\boldsymbol{a} \equiv \boldsymbol{b} \bmod \boldsymbol{n}$ if and only if $a_k \equiv b_k \bmod n_k$ for every k.
$(\boldsymbol{a}, \boldsymbol{b}) = \mathbf{1}$ if and only if $(a_k, b_k) = 1$ for every k.
$\boldsymbol{a}^{\boldsymbol{n}} = (a_1^{n_1}, a_2^{n_2}, \ldots, a_s^{n_s})$.

We can construct a cipher as follows: For a plain text a, let $\boldsymbol{k} = (k_1, k_2, \ldots, k_s)$ and $\boldsymbol{\ell} = (\ell_1, \ell_2, \ldots, \ell_s)$ be vectors such that k_i and ℓ_i are divisors of $\Phi_{s_i}(a_i)$ with $(k_i, s_i) = 1$ and $\Phi_{t_i}(a_i)$ with $(\ell_i, t_i) = 1$ where $(s_i, t_i) = 1$, respectively. We set $n = \boldsymbol{k}\boldsymbol{\ell}$ and $m = (\boldsymbol{k} - 1)(\boldsymbol{\ell} - 1)$. Then we can see

$$a^m \equiv 1 \bmod n.$$

We choose an enciphering key e with $(e, m) = 1$ and calculate the deciphering key d with $ed \equiv 1 \bmod m$. Then the sender A encipher a with $b \equiv a^e \bmod n$ and A sends b to the receiver B. Then B decipher b using relationship

$$b^d \equiv a^{ed} \equiv a \bmod n.$$

Example To encipher a word "BULLETIN", we first translate "BULLETIN" into this numerical equivalence $\boldsymbol{a} = (2, 3, 4, 4, 5, 6, 7, 8)$. We choose the next vectors $\boldsymbol{k}, \boldsymbol{\ell}$ for $\boldsymbol{a}$.

$$\begin{aligned} \boldsymbol{k} &= (\Phi_5(2), \Phi_5(3), \Phi_5(4), \Phi_5(4), \Phi_5(5), \tfrac{1}{5}\Phi_5(6), \\ &\quad \Phi_5(7), \Phi_5(8)) \\ \boldsymbol{\ell} &= (\Phi_9(2), \Phi_9(3), \tfrac{1}{3}\Phi_9(4), \tfrac{1}{3}\Phi_9(4), \Phi_9(5), \Phi_9(6), \\ &\quad \tfrac{1}{3}\Phi_9(7), \Phi_9(8)) \end{aligned}$$

Then we set

$$\boldsymbol{n} = \boldsymbol{k}\boldsymbol{\ell}, \ \boldsymbol{m} = (\boldsymbol{k} - 1)(\boldsymbol{\ell} - 1)$$

Selecting the enciphering key $\boldsymbol{e} = 291$ with $(\boldsymbol{m}, \boldsymbol{e}) = 1$, we calculate the deciphering key

$$\begin{aligned} \boldsymbol{d} &= (149, 56309, 48749, 48749, 5507069, 13528229, \\ &\quad 60758069, 296710709) \end{aligned}$$

such that $\boldsymbol{ed} \equiv 1 \bmod \boldsymbol{m}$. After this setting, we use the following sequences of steps.

$$\begin{aligned} \boldsymbol{\alpha} &= (B, U, L, L, E, T, I, N) \\ \boldsymbol{a} &= (2, 3, 4, 4, 5, 6, 7, 8) \\ \boldsymbol{b} &= \boldsymbol{a}^{\boldsymbol{e}} \bmod \boldsymbol{n} \\ &= (1318, 72681, 302382, 302382, 11340745, \\ &\quad 10593334, 96832971, 1191412216) \\ \boldsymbol{b}^{\boldsymbol{d}} \bmod \boldsymbol{n} &= (2, 3, 4, 4, 5, 6, 7, 8) \\ \boldsymbol{\alpha} &= (B, U, L, L, E, T, I, N) \end{aligned}$$