김일성종합대학학보
(자연과학)
주체106(2017)년 제63권 제12호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 63 No. 12 JUCHE106(2017).

$8k+5$ 형태의 두 씨수의 제곱들에 관한 일반화된 원분수행렬

김장룡, 최충혁

씨수들에 관한 위수 24까지의 원분수들은 각이한 형태의 지표합들에 의하여 계산된다.

선행연구[1]에서는 잉여계차모임을 구하기 위하여 두 씨수들의 적에 관한 위수가 2와 4인 일반화된 원분수들을, 선행연구[2]에서는 몇개의 씨수들의 제곱들에 관한 위수가 2인 일반화된 원분수들을 연구하였다.

론문에서는 2개의 $8k+5$ 모양의 씨수들의 제곱에 관한 일반화된 원분수행렬을 구하고 그것의 성질에 대하여 연구한다.

n을 1보다 큰 정의옹근수라고 하고 D_0을 환 $\boldsymbol{Z}_n$의 가역원소군 $\boldsymbol{Z}_n^*$의 지표가 d인 부분군이라고 하자. 그리고 $\{D_0, \cdots, D_{d-1}\}$을 $\boldsymbol{Z}_n^*$에서 D_0의 왼쪽 합동류들이라고 하자.

n이 씨수일 때 D_i들을 위수 d인 고전적원분클라스, $0 \le i, j \le d-1$에 대하여 $|(D_i+[1]) \bigcap D_j|$들을 고전적원분수들이라고 부른다.[2]

n을 1보다 큰 정의옹근수, a를 n과 서로 소인 옹근수라고 하자.

$\boldsymbol{Z}_n^*$에서 $[a]$의 위수가 $\varphi(n)$ (φ: 오일러함수)일 때 a를 n의 원시뿌리라고 부른다.[2]

p_1, p_2를 $8k+5$ 형태의 씨수, k_1, k_2들을 $\gcd(\varphi(p_1^{k_1}), \varphi(p_2^{k_2})) = 4$를 만족시키는 정의옹근수들이라고 할 때 $n = p_1^{k_1} p_2^{k_2}$이고 g를 $p_1^{k_1}$, $p_2^{k_2}$의 공통원시뿌리라고 하면 $\boldsymbol{Z}_n^*$에서 g의 위수는 $d = \mathrm{ord}_n(g) = \mathrm{lcm}(\mathrm{ord}_{p_1^{k_1}}(g), \mathrm{ord}_{p_2^{k_2}}(g)) = \varphi(p_1^{k_1})\varphi(p_2^{k_2})/4$로 된다.

W를 $\boldsymbol{Z}_n^*$에서 g에 의해 생성된 순환부분군이라고 하면 $d = \varphi(p_1^{k_1})\varphi(p_2^{k_2})/4 = |\boldsymbol{Z}_n^*|/4$이므로 이 부분군은 $\boldsymbol{Z}_n^*$의 지표가 4인 부분군이다.

이제 $y \in \boldsymbol{Z}_n$을 환동형넘기기 $\varphi: \boldsymbol{Z}_n \cong \boldsymbol{Z}_{p_1^{k_1}} \times \boldsymbol{Z}_{p_2^{k_2}}$, $a \mapsto (a, a)$에 의한 $(g, 1)$의 원상 즉 $\varphi(y) = (g, 1)$이라고 하면 y, y^2, $y^3 \notin W$, $y^4 \in W$가 성립되며 $C_i := y^i W$, $i \in \boldsymbol{Z}_4$들은 $\boldsymbol{Z}_n^*$의 서로 다른 합동류들 즉 위수가 4인 원분클라스들이다.

이제 $i, j \in \boldsymbol{Z}$에 대하여 원분수 (i, j)를 $i+1$행, $j+1$렬성분으로 하는 행렬인 원분수행렬을 구하기 위하여 $A_{i,j} := \{(s, t) \in \boldsymbol{Z}_d^2 \mid y^i g^s + 1 = y^j g^t\}$이라고 하자.

정리 1 $i, j \in \boldsymbol{Z}_4$, $(i, j) = (-i, j-i)$

정리 2 $i, j \in \boldsymbol{Z}_4$, $(i, j) = (j, i)$

증명 $-1 \in C_0$이므로 $-1 = g^x$인 $x \in \boldsymbol{Z}_d$가 존재한다.

$(s, t) \in A_{i,j}$이면 $y^i g^s + 1 = y^j g^t$이므로 $y^j g^{t-x} + 1 = y^i g^{s-x}$이다.

따라서 $(t-x, s-x) \in A_{j,i}$이며 거꾸로 $(t-x, s-x) \in A_{j,i}$이면 $(s, t) \in A_{i,j}$이므로 넘기기 $A_{i,j} \to A_{j,i}$, $(s, t) \mapsto (t-x, s-x)$는 1：1넘기기이며 $|A_{i,j}| = |A_{j,i}|$이다.(증명끝)

따름 $p_1^{k_1}$, $p_2^{k_2}$에 관한 원분수행렬은

$$\begin{pmatrix} A & B & C & D \\ B & D & E & E \\ C & E & C & E \\ D & E & E & B \end{pmatrix} \qquad (*)$$

로 된다. 여기서 $A=(0,\ 0),\ B=(0,\ 1),\ C=(0,\ 2),\ D=(0,\ 3),\ E=(1,\ 2)$ 이다.

정리 3 $p_1^{k_1}$, $p_2^{k_2}$ 에 관한 행렬 (*)의 성분들사이에는 다음의 관계식들이 성립된다.

① $A+B+C+D=p_1^{k_1-1}p_2^{k_2-1}((p_1-2)(p_2-2)+3)/4$

② $B+D+2E=p_1^{k_1-1}p_2^{k_2-1}((p_1-2)(p_2-2)-1)/4$

③ $2C+2E=p_1^{k_1-1}p_2^{k_2-1}((p_1-2)(p_2-2)-1)/4$

증명 ① 행렬 (*)로부터 $A+B+C+D=|(C_0+1)\cap \boldsymbol{Z}_n^*|$ 이다. 이때 $p_i\,|\,(g^x+1)$, $i=1,\ 2$ 이기 위해서는 x 가 $(p_i-1)/2$ 의 홀수배일것이 필요충분하므로 $g^x+1\in(C_0+1)\cap \boldsymbol{Z}_n^*$ 인 $x\ (0\le x\le d-1)$ 는 $(p_1-1)/2$ 이나 $(p_2-1)/2$ 의 홀수배가 되지 말아야 한다.

$\mathrm{lcm}((p_1-1)/2,\ (p_2-1)/2)=(p_1-1)(p_2-1)/8$ 이므로 $(p_1-1)/2$ 과 $(p_2-1)/2$ 의 공통홀수배는 $(p_1-1)(p_2-1)/8$ 의 홀수배이며 $|(C_0+1)\cap \boldsymbol{Z}_n^*|=p_1^{k_1-1}p_2^{k_2-1}((p_1-2)(p_2-2)+3)/4$ 이다.

② 우와 마찬가지로 $B+D+2E=|(C_1+1)\cap \boldsymbol{Z}_n^*|$ 으로 된다. 또한 $yg^x+1\in(C_1+1)\cap \boldsymbol{Z}_n^*$ 이기 위해서는 $p_1\nmid(g^{x+1}+1),\ p_2\nmid(g^x+1)$ 일것이 필요충분하며 $p_1\,|\,(g^{x+1}+1)$ 이기 위해서는 $x+1$ 이 $(p_1-1)/2$ 의 홀수배일것이, $p_2\,|\,(g^x+1)$ 이기 위해서는 x 가 $(p_2-1)/2$ 의 홀수배일것이 필요충분하므로 $|(C_1+1)\cap \boldsymbol{Z}_n^*|=p_1^{k_1-1}p_2^{k_2-1}((p_1-2)(p_2-2)-1)/4$ 로 된다.

③ 원분수행렬 (*)로부터 $2C+2E=|(\boldsymbol{Z}_n^*+1)\cap C_2|$ 라는것을 알수 있다.

$y^2g^x\in(\boldsymbol{Z}_n^*+1)\cap C_2$ 이기 위해서는 $p_1\nmid(g^{x+2}-1),\ p_2\nmid(g^x-1)$ 일것이 필요충분하다.

한편 $p_1\,|\,(g^{x+2}-1)$ 은 $(p_1-1)\,|\,(x+2)$ 일 때 또 그때에만, $p_2\,|\,(g^x-1)$ 은 $(p_2-1)\,|\,x$ 일 때 또 그때에만 성립되며 $p_1-1,\ p_2-1$ 이 4의 배수들이므로 이 두 조건을 동시에 만족시키는 x 는 존재하지 않는다. 따라서 $|(\boldsymbol{Z}_n^*+1)\cap C_2|=p_1^{k_1-1}p_2^{k_2-1}((p_1-2)(p_2-2)-1)/4$ 로 된다.(증명끝)

참 고 문 헌

[1] J. Cao et al.; Finite Fields Appl., **18**, 634, 2012.

[2] C. Ding et al.; Finite Fields Appl., **4**, 140, 1998.

주체106(2017)년 8월 5일 원고접수

Generalized Cyclotomic Number Matrix with Respect to the Powers of Two Prime Numbers of the Form $8k+5$

Kim Jang Ryong, Choe Chung Hyok

We study the generalized cyclotomic number matrix with respect to powers of two prime numbers, where both prime numbers are congruent to 5 with respect to modulo 8.

Key words: generalized cyclotomic number, generalized cyclotomic class