김일성종합대학학보
(자연과학)
주체105(2016)년 제62권 제12호

JOURNAL OF **KIM IL SUNG** UNIVERSITY
(NATURAL SCIENCE)
Vol. 62 No. 12 JUCHE105(2016).

씨수들의 제곱에 관한 일반화된 원분수의 특성

김정향, 최충혁

경애하는 **김정은**동지께서는 다음과 같이 말씀하시였다.

《우리는 가까운 앞날에 전반적인 과학기술분야에서 세계를 디디고 올라설수 있다는 배심을 가지고 첨단돌파의 기적들을 련이어 창조하여야 합니다.》(《조선로동당 제7차대회에서 한 중앙위원회사업총화보고》 단행본 40페지)

일반화된 원분수들에 대한 연구는 와링의 문제와 계차모임, 2진렬생성과 부호리론, 암호학 등에서 널리 리용되는 수론의 오랜 연구분야[2, 3]이며 씨수들에 관한 위수가 24이하의 원분수들은 여러가지 종류의 지표합들에 의해 계산되였다.

선행연구[1]에서는 $4k+1$ 모양인 $t(\geq 2)$ 개의 씨수들에 관하여 위수가 2^{t-1} 인 와이트맨의 일반화된 원분수의 계산공식을 얻었다. 또한 선행연구[2]에서는 씨수들의 제곱들에 관한 일반화된 원분수들을 새롭게 정의하고 위수가 2인 일반화된 원분수들을 구하였으며 그것의 여러 분야에서의 응용에 대하여 언급하였다.

우리는 $t-1$개의 $4k+3$모양의 씨수들의 제곱과 1개의 $4k+1$모양의 씨수의 제곱에 관한 위수가 2^{t-1}인 일반화된 원분수의 특성을 밝히고 그것의 계산공식을 새롭게 얻는다.

n을 2이상의 자연수라고 하고 D_0을 환 Z_n의 가역원소군 Z_n^*의 지표가 d인 부분군이라고 하자. Z_n^*에서 D_0의 왼쪽합동류들을 $\{D_0, \cdots, D_{d-1}\}$이라고 하자.

n이 합성수일 때 D_i들을 위수가 d인 일반화된 원분클라스라고 부르며 $0 \leq i,\ j \leq d-1$에 대하여 $(i,\ j) = |(D_i + [1]) \bigcap D_j|$를 위수가 d인 원분수라고 부른다.[2]

$p \equiv 3 \pmod 4$를 씨수, g를 p^k의 원시뿌리라고 할 때 $C_i := [g]^i \langle [g^2] \rangle$, $i = 0,\ 1$은 $Z_{p^k}^*$의 위수가 2인 일반화된 원분클라스이다.

$Z_{p^k}^*$의 위수가 2인 일반화된 원분수 $(i,\ j)^{(p^k)} = |(C_i + 1) \bigcap C_j|$, $i,\ j = 0, 1$들은 다음의 명제에 의하여 구할수 있다.

명제[1] $(0,\ 0)^{(p^k)} = (1,\ 0)^{(p^k)} = (1,\ 1)^{(p^k)} = p^{k-1}(p-3)/4$, $(0,\ 1)^{(p^k)} = p^{k-1}(p+1)/4$

론문에서는 $p_1, \cdots, p_t$를

$$p_i \equiv 3 \pmod 4,\ p_t \equiv 1 \pmod 4\ (1 \leq i \leq t-1),\ \gcd(\varphi(p^i),\ \varphi(p^j)) = 2\ (i \neq j)$$

를 만족시키는 서로 다른 씨수, g를 $p_1^{k_1}, \cdots, p_t^{k_t}$의 공통원시뿌리라고 한다.

$Z_n^* = Z_{p_1^{k_1} \cdots p_t^{k_t}}^*$에서 $[g]$에 의해 생성된 순환부분군 $W^{(t)}$에 의해 얻어지는 위수가 4이상인 일반화된 원분수를 $p_1^{k_1}, \cdots, p_t^{k_t}$에 의한 원분수라고 부른다. Z_n^*에서 $[g]$의 위수는 $d = \varphi(p_1^{k_1}) \cdots \varphi(p_t^{k_t})/2^{t-1}$이므로 $p_1^{k_1}, \cdots, p_t^{k_t}$에 의한 원분수들은 위수가 2^{t-1}인 일반화된 원분수이다.

$k\geq 1$에 대하여 $([1],\cdots,[1])\in Z_2^k$을 δ_k로 표시한다.

환동형넘기기 $Z_n\cong Z_{p_1^{k_1}}\times\cdots\times Z_{p_t^{k_t}}$, $[x]_n\mapsto([x]_{p_1^{k_1}},\cdots,[x]_{p_t^{k_t}})$에 의한

$$([g],[1],\cdots,[1]),\ ([1],[g],\cdots,[1]),\cdots,([1],\cdots,[1],[g])$$

의 원상을 각각 $[y_1]$, $[y_2]$, $\cdots$, $[y_t]$라고 하면 다음의 보조정리가 성립된다.

보조정리 1　$y_i^2\in W^{(t)}$, $1\leq i\leq t$

보조정리 2　$C_\alpha:=[y_1]^{a_1}\cdots[y_{t-1}]^{a_{t-1}}W^{(t)}$, $\alpha=([a_1],\cdots,[a_{t-1}],[0])\in Z_2^t/\langle\delta_t\rangle$들은 위수 2^{t-1}인 원분클라스들이다.

일반화된 원분클라스들은 $C_\alpha=:y_\alpha W^{(t)}$, $\alpha=([a_1],\cdots,[a_{t-1}],[0])\in Z_2^t/\langle\delta_t\rangle$의 모양을 가지며 원분수들을 $(\alpha,\beta):=|(C_\alpha+1)\bigcap C_\beta|$, $\alpha,\beta\in Z_2^t/\langle\delta_t\rangle$로 표시한다.

보조정리 3　$\sigma=([1],\cdots,[1],[0])\in Z_2^t/\langle\delta_t\rangle$일 때 $[-1]\in C_\sigma$이다.

정리 1　$\alpha,\beta\in Z_2^t/\langle\delta_t\rangle$일 때 $(\alpha,\beta)=(\beta+\sigma,\alpha+\sigma)$, $(\alpha,\beta)=(\alpha,\alpha+\beta)$가 성립된다.

증명 일반화된 원분수의 정의로부터 $\mathrm{sol}_{\alpha,\beta}:=\{([u],[v])\in Z_d^2\mid y_\alpha[g]^u+[1]=y_\beta[g]^v\}$으로 놓으면 $(\alpha,\beta)=|\mathrm{sol}_{\alpha,\beta}|$이다.

$([u],[v])\in\mathrm{sol}_{\alpha,\beta}$라고 하면 $[y_1\cdots y_{t-1}g^x]=[-1]$인 x가 존재하므로 $y_\alpha[g]^u+[1]=y_\beta[g]^v$의 량변에 $[y_1\cdots y_{t-1}g^x]$을 곱하면 $y_{\alpha+\sigma}[g]^{u+x}-[1]=y_{\beta+\sigma}[g]^{v+x}$을 얻는다. 즉

$$y_{\beta+\sigma}[g]^{v+x}+[1]=y_{\alpha+\sigma}[g]^{u+x}\text{이며 }([v+x],[u+x])\in\mathrm{sol}_{\beta+\sigma,\alpha+\sigma}.$$

이 결과로부터 $([v'],[u'])\in\mathrm{sol}_{\beta+\sigma,\alpha+\sigma}$이면 $([u'-x],[v'-x])\in\mathrm{sol}_{\alpha,\beta}$임을 알수 있고 결국 $|\mathrm{sol}_{\alpha,\beta}|=|\mathrm{sol}_{\beta+\sigma,\alpha+\sigma}|$이다. 따라서 $(\alpha,\beta)=(\beta+\sigma,\alpha+\sigma)$이다.

보조정리 1에 의하여 $y_\alpha^2\in W^{(t)}$이다. 즉 $y_\alpha^2=[g]^k$인 웅근수 k가 존재한다.

$([u],[v])\in\mathrm{sol}_{\alpha,\beta}$라고 하면 $y_\alpha[g]^u+[1]=y_\beta[g]^v$의 량변에 $y_\alpha[g]^{-k-u}$을 곱하여 $y_\alpha^2[g]^{-k}+y_\alpha[g]^{-k-u}=y_\alpha y_\beta[g]^{v-k-u}$ 즉 $y_\alpha[g]^{-k-u}+[1]=y_{\alpha+\beta}[g]^{v-k-u}$을 얻게 된다.

그러므로 $([-k-u],[v-k-u])\in\mathrm{sol}_{\alpha,\alpha+\beta}$이다.

거꾸로 $([u'],[v'])\in\mathrm{sol}_{\alpha,\alpha+\beta}$이면 $([-k-u'],[v'-u'])\in\mathrm{sol}_{\alpha,\beta}$라는것을 곧 알수 있다. 따라서 $|\mathrm{sol}_{\alpha,\beta}|=|\mathrm{sol}_{\alpha,\alpha+\beta}|$이며 즉 $(\alpha,\beta)=(\alpha,\alpha+\beta)$이다.(증명끝)

따름　$\alpha,0=([0],\cdots,[0])\in Z_2^t/\langle\delta_t\rangle$일 때 $(\alpha,\alpha)=(\alpha,0)$, $(0,0)=(\sigma,\sigma)=(\sigma,0)$이다.

정리 2　$\sigma=([1],\cdots,[1],[0])$, $\alpha=(\underbrace{[1],\cdots,[1]}_{r},[0],\cdots,[0])\in Z_2^t/\langle\delta_t\rangle$, $1\leq r\leq t-1$이라고 하면 $(0,\sigma)+3(0,\sigma+\alpha)=(0,0)^{(r)}(0,\sigma')^{(t-r)}$이 성립된다. 여기서 $\sigma'=([1],\cdots,[1],[0])\in Z_2^{t-r}/\langle\delta_{t-r}\rangle$이며 $(0,0)^{(r)}$, $(0,\sigma')^{(t-r)}$은 각각 $p_1^{k_1},\cdots,p_r^{k_r}$, $p_{r+1}^{k_{r+1}},\cdots,p_t^{k_t}$에 의한 일반화된 원분수이다.

증명 먼저 $C_0\bigcup C_\alpha=\psi^{-1}(W^{(r)}\times W^{(t-r)})$임을 밝히자. 여기서 ψ는

$$Z_n\cong Z_{p_1^{k_1}\cdots p_r^{k_r}}\times Z_{p_{r+1}^{k_{r+1}}\cdots p_t^{k_t}},\ [x]_n\mapsto([x]_{p_1^{k_1}\cdots p_r^{k_r}},[x]_{p_{r+1}^{k_{r+1}}\cdots p_t^{k_t}})$$

로 주어지는 환동형넘기기이다.

$([g]^l,[g]^m)\in W^{(r)}\times W^{(t-r)}$에 대하여 $l\equiv m\pmod 2$라고 하자.

이때 명제에 의해 $s \equiv l \pmod{\varphi(p_i^{k_i})}\ (1 \le i \le r),\ s \equiv m \pmod{\varphi(p_i^{k_i})}\ (r+1 \le i \le t)$ 의 풀이 s가 존재하면 $g^s \equiv g^l \pmod{p_1^{k_1} \cdots p_r^{k_r}},\ g^s \equiv g^m \pmod{p_{r+1}^{k_{r+1}} \cdots p_t^{k_t}}$ 이므로

$$\psi^{-1}([g]^l,\ [g]^m) = [g]_n^s \in W^{(t)} = C_0 .$$

한편 $l \equiv m+1 \pmod 2$ 이면 $s \equiv l-1 \pmod{\varphi(p_i^{k_i})}\ (1 \le i \le r),\ s \equiv m \pmod{\varphi(p_i^{k_i})}\ (r+1 \le i \le t)$ 인 s가 존재하며 이 경우 $g^s \equiv g^{l-1} \pmod{p_1^{k_1} \cdots p_r^{k_r}},\ g^s \equiv g^m \pmod{p_{r+1}^{k_{r+1}} \cdots p_t^{k_t}}$ 로 된다.

따라서 $\psi([y_1 \cdots y_r]_n) = ([g],\ [1])$ 임을 고려하면 $\psi([y_1 \cdots y_r g^s]_n) = ([g]^l,\ [g]^m)$ 이고

$$\psi^{-1}([g]^l,\ [g]^m) = [y_1 \cdots y_r]_n [g]_n^s \in [y_1 \cdots y_r]_n W^{(t)} = C_\alpha .$$

우의 두 사실로부터 $C_0 \cup C_\alpha \supset \psi^{-1}(W^{(r)} \times W^{(t-r)})$ 이다.

반대로 $[y_1]_n^a \cdots [y_r]_n^a [g]_n^s \in C_0 \cup C_\alpha,\ 0 \le a \le 1$ 에 대하여

$$\psi([y_1]_n^a \cdots [y_r]_n^a [g]_n^s) = ([g]^{a+s},\ [g]^s) \in W^{(r)} \times W^{(t-r)}$$

이다. 따라서 $C_0 \cup C_\alpha = \psi^{-1}(W^{(r)} \times W^{(t-r)})$ 이고

$$C_\sigma \cup C_{\alpha+\sigma} = y_\sigma (C_0 \cup C_\alpha) = y_\sigma \psi^{-1}(W^{(r)} \times W^{(t-r)}) = \psi^{-1}(W^{(r)} \times y_{\sigma'} W^{(t-r)})$$

이다. 여기서 $\sigma'' = ([1], \cdots, [1],\ [0]) \in Z_2^r / \langle \delta_r \rangle$ 이다.

ψ가 환준동형이므로 $(C_\sigma \cup C_{\alpha+\sigma}) + [1] = \psi^{-1}((W^{(r)} + [1]) \times (y_{\sigma'} W^{(t-r)} + [1]))$ 로 된다.

정리 1에 의하여 $(0,\ \alpha+\sigma) = (\alpha+\sigma+\sigma,\ 0+\sigma) = (\alpha,\ \sigma) = (\alpha,\ \alpha+\sigma)$ 이므로

$$\begin{aligned}(0,\ \sigma) + 3(0,\ \alpha+\sigma) &= (0,\ \sigma) + (0,\ \alpha+\sigma) + (\alpha,\ \sigma) + (\alpha,\ \alpha+\sigma) = \\ &= |(C_0 \cup C_\alpha) \cap ((C_\sigma \cup C_{\alpha+\sigma}) + [1])| = \\ &= |\psi^{-1}(W^{(r)} \times W^{(t-r)}) \cap \psi^{-1}((W^{(r)} + [1]) \times (y_{\sigma'} W^{(t-r)} + [1]))| = \\ &= |W^{(r)} \cap (W^{(r)} + [1])| \cdot |W^{(t-r)} \cap (y_{\sigma'} W^{(t-r)} + [1])| = (0,\ 0)^{(r)} (0,\ \sigma')^{(t-r)}\end{aligned}$$

이 성립된다.(증명끝)

보조정리 4 p가 씨수, $[g]$가 $Z_{p^k}^*$의 생성원소일 때 위수 1인 일반화된 원분수는 $(0,0)^{(1)} = p^k - 2p^{k-1}$을 만족시킨다.

보조정리 5 $\gcd(a,\ m) = d$ 일 때 $aZ_m = dZ_m$ 이 성립된다.

정리 3 $\alpha = ([1], \cdots, [1], [0]) \in Z_2^t / \langle \delta_t \rangle$ 라고 하면

$$(0,\ 0) = p_t^{k_t - 1}\left(\frac{p_t - 3}{4}(0,\ 0)^{(t-1)} + \frac{1}{2}\left(\prod_{i=1}^{t-1} \frac{p_i^{k_i-1}(p_i-3)}{4} + \prod_{i=1}^{t-1} \frac{p_i^{k_i-1}(p_i+1)}{4}\right)\right),$$

$$(0,\ \alpha) = p_t^{k_t - 1}\left(\frac{p_t + 1}{4}(0,\ 0)^{(t-1)} - \frac{3}{2}\left(\prod_{i=1}^{t-1} \frac{p_i^{k_i-1}(p_i-3)}{4} + \prod_{i=1}^{t-1} \frac{p_i^{k_i-1}(p_i+1)}{4}\right)\right)$$

이 성립된다. 여기서 $(0,\ 0)^{(t-1)}$은 $p_1^{k_1}, \cdots, p_{t-1}^{k_{t-1}}$에 의해 일반화된 원분수이다.

정리 4 $0 < r_1 + r_2 < t$ 이고

$$\alpha = (\underbrace{[1], \cdots, [1]}_{r_1},\ \underbrace{[0], \cdots, [0]}_{r_2},\ \underbrace{[1], \cdots, [1]}_{r_3},\ \underbrace{[0], \cdots, [0]}_{r_4}) \in Z_2^t / \langle \delta_t \rangle,$$

$$\beta = (\underbrace{[0], \cdots, [0]}_{r_1},\ \underbrace{[1], \cdots, [1]}_{r_2},\ \underbrace{[1], \cdots, [1]}_{r_3},\ \underbrace{[0], \cdots, [0]}_{r_4}) \in Z_2^t / \langle \delta_t \rangle$$

이라고 하면 $2(\alpha,\ \beta+\sigma)+(0,\ \alpha+\sigma)+(0,\ \beta+\sigma)=(\gamma_1,\ 0)^{(r_1+r_2)}(\gamma_2,\ \sigma')^{(r_3+r_4)}$ 가 성립된다. 여기서

$$\sigma=([1],\ \cdots,\ [1],\ [0])\in Z_2^t/\langle\delta_t\rangle,\ \ \sigma'=([1],\cdots,\ [1],\ [0])\in Z_2^{r_3+r_4}/\langle\delta_{r_3+r_4}\rangle,$$

$$\gamma_1=(\underbrace{[1],\cdots,\ [1]}_{r_1},\ \underbrace{[0],\cdots,\ [0]}_{r_2})\in Z_2^{r_1+r_2}/\langle\delta_{r_1+r_2}\rangle,\ \ \gamma_2=(\underbrace{[1],\cdots,\ [1]}_{r_3},\ \underbrace{[0],\cdots,\ [0]}_{r_4})\in Z_2^{r_3+r_4}/\langle\delta_{r_3+r_4}\rangle.$$

증명 $C_0':=\langle[g]\rangle$ 를 $Z^*_{p_1^{k_1}\cdots p_{r_1+r_2}^{k_{r_1+r_2}}}$ 의 순환부분군, $C_0''=\langle[g]\rangle$ 를 $Z^*_{p_{r_1+r_2+1}^{k_{r_1+r_2+1}}\cdots p_t^{k_t}}$ 의 순환부분군이라고 하자.

이때 $C'_{\gamma_1}=y_{\gamma_1}W^{(r_1+r_2)}$, $C''_{\gamma_2}=y_{\gamma_2}W^{(t-r_1-r_2)}$ 라고 놓으면

$$C_\alpha\cup C_\beta\cong C'_{\gamma_1}\times C''_{\gamma_2},\ C_{\alpha+\sigma}\cup C_{\beta+\sigma}\cong C'_{\gamma_1}\times C''_{\gamma_2+\sigma}$$

로 된다는것을 정리 2의 증명에서와 같이 밝힐수 있다.

따라서 정리 1에 의하여

$$2(\alpha,\ \beta+\sigma)+(0,\ \alpha+\sigma)+(0,\ \beta+\sigma)=(\alpha,\ \beta+\sigma)+(\beta,\ \alpha+\sigma)+(\alpha,\ \sigma)+(\beta,\ \sigma)=$$
$$=(\alpha,\ \beta+\sigma)+(\beta,\ \alpha+\sigma)+(\alpha,\ \alpha+\sigma)+(\beta,\ \beta+\sigma)=|((C_\alpha\cup C_\beta)+[1])\cap(C_{\alpha+\sigma}\cup C_{\beta+\sigma})|=$$
$$=|(C'_{\gamma_1}+[1])\cap C'_{\gamma_1}|\cdot|(C''_{\gamma_2}+[1])\cap C''_{\gamma_2+\sigma}|=(\gamma_1,\ \gamma_1)^{(r_1+r_2)}(\gamma_2,\ \gamma_2+\sigma')^{(r_3+r_4)}=$$
$$=(\gamma_1,\ 0)^{(r_1+r_2)}(\gamma_2,\ \sigma')^{(r_3+r_4)}$$

이 성립된다.(증명끝)

정리 2, 3, 4를 리용하여 임의의 $\alpha,\ \beta\in Z_2^t/\langle\delta_t\rangle$ 에 대하여 위수가 2^{t-1} 인 일반화된 원분수들을 모두 구할수 있다. 사실 $\alpha,\ \beta\in Z_2^t/\langle\delta_t\rangle$ 가 주어졌을 때 [1]과 [0]의 위치를 적당히 바꾸면 모두 정리 2, 3, 4에서와 같은 모양으로 바꿀수 있다.

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.

주체105(2016)년 8월 5일 원고접수

Characteristics of Generalized Cyclotomic Numbers with Respect to Prime Powers

Kim Jong Hyang, Choe Chung Hyok

We find out characteristics of generalized cyclotomic numbers with respect to some prime powers and propose a method to calculate them, where one prime is congruent to 1 and the others are congruent to 3 modulo 4.

Key words: prime, cyclotomic number