김일성종합대학학보 주체107(2018)년
수 학 제64권 제4호

$8k+5$ 모양의 두 씨수의 제곱들에 관한 일반화된 원분수들사이관계

최 충 혁

원분수 및 일반화된 원분수들은 수론의 오래고도 중요한 한가지 주제로서 와링의 문제, 계차모임, 2진렬생성, 부호리론, 암호학 등과 련관되여있다.

선행연구[2]에서는 기껏 하나의 씨수가 $4k+1$의 형태를 가지는 씨수들에 관한 위수가 2의 제곱인 일반화된 원분수계산공식을 구하였으며 선행연구[1]에서는 2개의 $4k+1$ 모양의 씨수들의 제곱들에 관한 위수 2의 제곱인 일반화된 원분수들의 성질들이 연구되였으나 계산공식을 완전히 얻지는 못하였다.

론문에서는 2개의 $8k+5$ 모양의 씨수들의 제곱에 관한 일반화된 원분수들사이의 몇가지 관계식에 대하여 론의한다.

p_1, p_2를 $8k+5$ 모양의 씨수, k_1, k_2들을 $\gcd(\varphi(p_1^{k_1}),\ \varphi(p_2^{k_2}))=4$를 만족시키는 정의옹근수, $n=p_1^{k_1}p_2^{k_2}$라고 하고 g를 $p_1^{k_1}$, $p_2^{k_2}$의 공통원시뿌리라고 하면 가역원소군 Z_n^*에서 g의 위수는 $d=\mathrm{ord}_n(g)=\mathrm{lcm}(\mathrm{ord}_{p_i^{k_1}}(g),\ \mathrm{ord}_{p_2^{k_2}}(g))=\varphi(p_1^{k_1})\varphi(p_2^{k_2})/4$으로 된다.

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

명제 1[1] 환동형넘기기 $\varphi: Z_n \cong Z_{p_1^{k_1}} \times Z_{p_2^{k_2}}$, $a \mapsto (a,\ a)$에 의한 $(g,\ 1)$의 원상을 y라고 하면 $y,\ y^2,\ y^3 \notin W,\ y^4 \in W$이다.

명제 2[1] $C_i := y^i W,\ i \in Z_4$들은 가역원소군 Z_n^*의 서로 다른 합동류들 즉 위수 4인 원분클라스들이다.

명제 3[1] $p_1 \equiv p_2 \equiv 5 \pmod 8$일 때 원분수행렬은 $\begin{pmatrix} A & B & C & D \\ B & D & E & E \\ C & E & C & E \\ D & E & E & B \end{pmatrix}$로 되며 이 행렬에 관하여 다음의 식들이 성립된다.

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

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

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

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

명제 3으로부터 $p_1^{k_1}$, $p_2^{k_2}$에 관한 일반화된 원분수들의 계산공식을 얻으려면 A, B, C, D, E들을 구해야 하지만 주어진 3개의 식만으로는 불충분하다.

이제 A, B, C, D, E 사이에 성립되는 관계식들을 더 찾아보자.

보조정리 1 $\displaystyle\sum_{\substack{g^a+yg^b+1=y^2g^c\\ a,\ b,\ c\in Z_d}} 1 = AE+B^2+CD+DE+p_1^{k_1-1}p_2^{k_2-1}\frac{(p_1+p_2-10)d}{16}$

증명 $\displaystyle\sum_{g^a+yg^b+1=y^2g^c} 1 = \sum_{\substack{g^a+yg^b+1=y^2g^c\\ g^a+1\in Z_n^*}} 1 + \sum_{\substack{g^a+yg^b+1=y^2g^c\\ g^a+1\notin Z_n^*}} 1$ 이므로 $\displaystyle\sum_{\substack{g^a+yg^b+1=y^2g^c\\ g^a+1\in Z_n^*}} 1$ 과 $\displaystyle\sum_{\substack{g^a+yg^b+1=y^2g^c\\ g^a+1\notin Z_n^*}} 1$ 을 구하자.

명제 2에 의하여 $C_i\ (i\in Z_4)$ 들이 Z_n^* 의 서로 다른 합동류전부를 이루므로

$$\sum_{\substack{g^a+yg^b+1=y^2g^c\\ g^a+1\in Z_n^*}} 1 = \sum_{g^a+1=g^x}\ \sum_{yg^{b-x}+1=y^2g^{c-x}} 1 + \sum_{g^a+1=yg^x}\ \sum_{g^{b-x}+1=yg^{c-x}} 1 + \sum_{g^a+1=y^2g^x}\ \sum_{y^3g^{b-x}+1=g^{c-x}} 1 + \sum_{g^a+1=y^3g^x}\ \sum_{y^2g^{b-x}+1=y^3g^{c-x}} 1 =$$

$$=(0,\ 0)(1,\ 2)+(0,\ 1)(0,\ 1)+(0,\ 2)(3,\ 0)+(0,\ 3)(2,\ 3)=AE+B^2+CD+DE$$

이다. 한편 $\displaystyle\sum_{\substack{g^a+yg^b+1=y^2g^c\\ g^a+1\notin Z_n^*}} 1 = \sum_{\substack{g^a+yg^b+1=y^2g^c\\ g^a+1\in p_1Z_n\cap p_2Z_n}} 1 + \sum_{\substack{g^a+yg^b+1=y^2g^c\\ g^a+1\in p_1Z_n-p_2Z_n}} 1 + \sum_{\substack{g^a+yg^b+1=y^2g^c\\ g^a+1\in p_2Z_n-p_1Z_n}} 1$ 이므로 이 등식의 오른변에 있는 3개의 합들을 각각 계산해보자.

g 가 p_i 들의 공통원시뿌리이므로 $g^a+1\in p_iZ_n$ 이기 위해서는 a 가 $(p_i-1)/2$ 의 홀수배일것이 필요충분하므로 $g^a+1\in p_1Z_n\cap p_2Z_n$ 이기 위해서는 a 가 $(p_1-1)/2$ 과 $(p_2-1)/2$ 의 홀수배일것이 필요충분하다.

결국 $g^a+1\in p_1Z_n\cap p_2Z_n$, $g^a+1\in p_1Z_n-p_2Z_n$, $g^a+1\in p_2Z_n-p_1Z_n$ 인 a 의 개수는 각각 $p_1^{k_1-1}p_2^{k_2-1}$, $p_1^{k_1-1}p_2^{k_2-1}(p_2-5)/4$, $p_1^{k_1-1}p_2^{k_2-1}(p_1-5)/4$ 이다.

a 를 $g^a+1\in p_1Z_n\cap p_2Z_n$ 인 수라고 하면 $g^a+yg^b+1=y^2g^c$ 인 $b,\ c$ 에 대하여 $g^{b+1}\equiv g^{c+2}\ (\mathrm{mod}\ p_1),\ g^b\equiv g^c\ (\mathrm{mod}\ p_2)$ 가 만족되여야 한다. p_i 들의 공통원시뿌리이므로 이 식들은 $b-c\equiv 1\ (\mathrm{mod}\ p_1-1),\ b-c\equiv 0\ (\mathrm{mod}\ p_2-1)$ 과 동등하며 $\gcd(p_1-1,\ p_2-1)=4$ 이므로 이 합동식을 만족시키는 $b,\ c$ 는 존재하지 않는다. 즉 $\displaystyle\sum_{\substack{g^a+yg^b+1=y^2g^c\\ g^a+1\in p_1Z_n\cap p_2Z_n}} 1 = 0$ 이다.

다음으로 $\displaystyle\sum_{\substack{g^a+yg^b+1=y^2g^c\\ g^a+1\in p_1Z_n-p_2Z_n}} 1 = \sum_{s=1}^{k_1}\ \sum_{\substack{p_1^s\|g^a+1\\ p_2\nmid g^a+1}}\ \sum_{g^a+yg^b+1} 1$ 을 구하자.

$s<k_1$ 이라고 할 때 $p_1^s\,\|\,g^a+1$ 이기 위해서는 a 가 $\varphi(p_1^s)/2$ 의 홀수배이지만 $\varphi(p_1^{s+1})/2$ 의 홀수배는 아니며 $p_2\nmid g^a+1$ 이기 위해서는 a 가 $(p_2-1)/2$ 의 홀수배가 아닐것이 필요충분하다는것을 고려하면 다음의 식이 성립된다.

$$|\{a\,|\,p_1^s\,\|\,(g^a+1),\ p_2\nmid(g^a+1)\}|=p_1^{k_1-s-1}p_2^{k_2-1}(p_1-1)(p_2-5)/4$$

a 를 우의 조건을 만족시키는 수라고 하면 $g^a+1=p_1^sQ$, $p_1\nmid Q$, $[g^a+1]_{p_2^{k_2}}=[g^t]_{p_2^{k_2}}$ 로 쓸수 있으며 따라서 다음의 식이 성립된다.

$$g^a+yg^b+1=y^2g^c \Leftrightarrow \begin{cases} p_1^sQ+g^{b+1}\equiv g^{c+2}(\mathrm{mod}\ \ p_1^{k_1}) & (1)\\ g^b+g^t\equiv g^c(\mathrm{mod}\ \ p_2^{k_2}) & (2)\end{cases}$$

식 (1)의 풀이가 존재하려면 분명히 $p_1^s\,\|\,(g^{c-b+1}-1),\ \varphi(p_1^s)\,|\,(c-b+1),\ \varphi(p_1^{s+1})\nmid(c-b+1)$

이며 $b, c\in Z_d$ 임을 고려하면 $c-b+1=\varphi(p_1^s)k,\ p_1\nmid k,\ 0\le k\le d/\varphi(p_1^s)-1=p_1^{k-s}\varphi(p_2^{k_2})/4-1$ 로 쓸수 있다. 이 식을 리용하여 식 (2)를 다시 쓰면

$$1+g^{-b+t}\equiv g^{\varphi(p_1^s)k-1}\ (\mathrm{mod}\ \ p_2^{k_2}) \tag{3}$$

이 얻어지는데 $\gcd(\varphi(p_1^{k_1}),\ \varphi(p_2^{k_2}))=4$ 이므로 이 합동식이 풀이 b 를 가지려면 $[1+g^{-b+t}]_{p_2^{k_2}}\in g^{-1}\langle g^4\rangle$ 이 성립되여야 한다. 여기서 $\langle g^4\rangle$ 은 군 $Z^*_{p_2^{k_2}}$ 의 부분군이다. 따라서 $|(1+Z^*_{p_2^{k_2}})\cap g^{-1}\langle g^4\rangle|=|\{k\,|\,0\le 4k-1\le\varphi(p_2^{k_2})-1,\ (p_2-1)\nmid(4k-1)\}|=\varphi(p_2^{k_2})/4$ 임을 밝힐수 있으며 $[1+g^{-b+t}]_{p_2^{k_2}}\in g^{-1}\langle g^4\rangle$ 이 성립되는 b 의 값은 mod $\varphi(p_2^{k_2})$ 에 관하여 $\varphi(p_2^{k_2})/4$ 개 존재한다.

이제 $1+g^{-b+t}=g^{4\upsilon-1}$ 이라고 하면 식 (3)은 $\varphi(p_1^s)k\equiv 4\upsilon\,(\mathrm{mod}\,\varphi(p_2^{k_2}))$ 과 동등하며 이 식을 만족시키는 k 는 $\mathrm{mod}\,\varphi(p_2^{k_2})/4$ 에 관하여 유일하다. $k\,\mathrm{mod}\,\varphi(p_2^{k_2})/4$ 의 값이 주어졌을 때 $p_1\nmid k$ 라는 조건을 고려하면 $0\le k\le p_1^{k-s}\varphi(p_2^{k_2})/4-1$ 인 k 는 $p_1^{k_1-s}-p_1^{k_1-s-1}$ 개 존재한다. 이 k 들중의 하나를 식 (1)에 넣고 정돈하면 $g^{b+1}\cdot(g^{\varphi(p_1^s)k}-1)/p_1^s\equiv Q\ \ (\mathrm{mod}\ \ p_1^{k_1-s})$ 이다.

g 가 $p_1^{k_1-s}$ 의 원시뿌리이고 $p_1\nmid(g^{\varphi(p_1^s)k}-1)/p_1^s,\ Q$ 이므로 이것을 만족시키는 b 는 $\mathrm{mod}\,\varphi(p_1^{k_1-s})$ 에 관하여 유일하다. 또한 $k\,\mathrm{mod}\,\varphi(p_2^{k_2})/4$ 이 주어진 $\varphi(p_1^{k_1-s})=p_1^{k_1-s}-p_1^{k_1-s-1}$ 개의 k 의 값 매개에 대하여 얻어지는 b mod $\varphi(p_1^{k_1-s})$ 의 값은 서로 다르게 된다.

결국 $\varphi(p_2^{k_2})/4$ 개의 $b\,\mathrm{mod}\,\varphi(p_2^{k_2})$ 의 값들중의 하나가 선택되면 $p_1^{k_1-s}-p_1^{k_1-s-1}$ 개의 k 와 $b\,\mathrm{mod}\,\varphi(p_1^{k_1-s})$ 의 값들이 각각 결정되게 된다. 여기서 $b\,\mathrm{mod}\,\varphi(p_1^{k_1-s})$ 가 취하는 서로 다른 $p_1^{k_1-s}-p_1^{k_1-s-1}$ 개 값들가운데서 $b\,\mathrm{mod}\,\varphi(p_2^{k_2})$ 의 값과의 차가 $\gcd(\varphi(p_1^{k_1}),\ \varphi(p_2^{k_2}))=4$ 의 배수로 되는것은 $(p_1^{k_1-s}-p_1^{k_1-s-1})/4$ 개뿐이다. 그러므로 $\varphi(p_2^{k_2})/4$ 개의 $b\,\mathrm{mod}\,\varphi(p_2^{k_2})$ 의 값들중의 하나가 선택되면 $(p_1^{k_1-s}-p_1^{k_1-s-1})/4$ 개의 $b\,\mathrm{mod}\,\varphi(p_1^{k_1-s})\varphi(p_2^{k_2})/4$ 과 c 의 값이 결정되게 된다. 따라서 하나의 a 가 선택되였을 때 식 (1), (2)를 만족시키는 $(b,\ c)$ 의 개수는

$$\varphi(p_2^{k_2})/4\cdot(p_1^{k_1-s}-p_1^{k_1-s-1})/4\cdot d/[\varphi(p_1^{k_1-s})\varphi(p_2^{k_2})/4]=d/4$$

로 되며 $\sum\limits_{\substack{p_1^s\|g^a+1\\ p_2\nmid g^a+1}}\ \sum\limits_{g^a+yg^b+1} 1=p_1^{k_1-s-1}p_2^{k_2-1}\dfrac{(p_1-1)(p_2-5)}{4}\cdot\dfrac{d}{4}$ 이다.

$s=k_1$ 인 경우 우의 합을 계산해보자.

우와 마찬가지로 $|\{a\,|\,p_1^{k_1}\,\|\,(g^a+1),\ p_2\nmid(g^a+1)\}|=p_2^{k_2-1}(p_2-5)/4$ 임을 밝힐수 있다.

또한 $g^a+yg^b+1=y^2g^c\Leftrightarrow\begin{cases}g^{b+1}\equiv g^{c+2}\ (\mathrm{mod}\ p_1^{k_1})\\ g^b+g^t\equiv g^c\ (\mathrm{mod}\ p_2^{k_2})\end{cases}\Leftrightarrow\begin{cases}\varphi(p_1^{k_1})\,|\,(c-b+1)\\ 1+g^{b-t}\equiv g^{c-t}\ (\mathrm{mod}\ p_2^{k_2})\end{cases}$ 라는것도 쉽게 말할수 있다.

$c-b+1=\varphi(p_1^{k_1})k$ 라고 하면 $0\le k\le\varphi(p_2^{k_2})/4-1$ 이고 마지막련립합동식의 2번째 식은 $1+g^{-b+t}\equiv g^{\varphi(p_1^{k_1})k-1}\,(\mathrm{mod}\,p_2^{k_2})$ 으로 된다. 역시 우와 류사하게 이 식은 $[1+g^{-b+t}]_{p_2^{k_2}}\in g^{-1}\langle g^4\rangle$ 인 b 에 대하여서만 성립되며 이 식을 만족시키는 b 의 값은 $\mathrm{mod}\,\varphi(p_2^{k_2})$ 에 관하여

$\varphi(p_2^{k_2})/4$ 개 존재하고 $k \bmod \varphi(p_2^{k_2})/4$ 의 값은 유일하게 얻어지므로 $(b,\ c)$ 의 개수는 $\frac{\varphi(p_2^{k_2})}{4}\cdot\frac{d}{\varphi(p_2^{k_2})}=\frac{d}{4}$ 이며 $\sum_{\substack{p_1^{k_1}|g^a+1 \\ p_2\nmid g^a+1}}\sum_{g^a+yg^b+1} 1 = p_2^{k_2-1}\frac{(p_2-5)}{4}\cdot\frac{d}{4}$ 이다. 따라서

$$\sum_{\substack{g^a+yg^b+1=y^2g^c \\ g^a+1\in p_1Z_n-p_2Z_n}} 1 = \sum_{s=1}^{k_1}\sum_{\substack{p_1^s\|g^a+1 \\ p_2\nmid g^a+1}}\sum_{g^a+yg^b+1} 1 = \sum_{s=1}^{k_1} p_1^{k_1-s-1}p_2^{k_2-1}\frac{(p_1-1)(p_2-5)}{4}\cdot\frac{d}{4}+p_2^{k_2-1}\frac{(p_2-5)}{4}\cdot\frac{d}{4}=$$

$$=p_2^{k_2-1}\frac{(p_1-1)(p_2-5)d}{16}\cdot\frac{p_1^{k_1-1}-1}{p_1-1}+p_2^{k_2-1}\frac{(p_2-5)}{4}\cdot\frac{d}{4}=p_1^{k_1-1}p_2^{k_2-1}\frac{(p_2-5)d}{16}$$

가 성립되며 우와 류사하게 $\sum_{\substack{g^a+yg^b+1=y^2g^c \\ g^a+1\in p_2Z_n-p_1Z_n}} 1 = p_1^{k_1-1}p_2^{k_2-1}\frac{(p_1-5)d}{16}$ 가 성립된다. 그러므로

$$\sum_{g^a+yg^b+1=y^2g^c} 1 = \sum_{\substack{g^a+yg^b+1=y^2g^c \\ g^a+1\in Z_n^*}} 1 + \sum_{\substack{g^a+yg^b+1=y^2g^c \\ g^a+1\notin Z_n^*}} 1 = AE+B^2+CD+DE+p_1^{k_1-1}p_2^{k_2-1}(p_1+p_2-10)d/16$$

이다.(증명끝)

보조정리 2 $\sum_{\substack{g^a+yg^b+1=y^2g^c \\ a,\ b,\ c\in Z_d}} 1 = BC+DE+CE+E^2+p_1^{k_1-1}p_2^{k_2-1}\frac{(p_1+p_2-2)d}{16}$

정리 1 $AE+B^2+CD-BC-CE-E^2=p_1^{k_1-1}p_2^{k_2-1}d/2$

보조정리 3 $\sum_{\substack{g^a+yg^b+1=yg^c \\ a,\ b,\ c\in Z_d}} 1 = B^2+D^2+2E^2+p_1^{k_1-1}p_2^{k_2-1}\frac{p_1+p_2-2}{16}$

$$\sum_{\substack{g^a+yg^b+1=yg^c \\ a,\ b,\ c\in Z_d}} 1 = 2AC+2C^2+p_1^{k_1-1}p_2^{k_2-1}\frac{(p_1-1)(p_2-5)^2}{64}+p_1^{k_1-1}p_2^{k_2-1}\frac{(p_1-5)^2(p_2-1)}{64}+p_1^{k_1-1}p_2^{k_2-1}\frac{(p_1-1)(p_2-1)}{4}$$

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

참 고 문 헌

[1] 김장룡 등; 조선민주주의인민공화국 과학원통보, 1, 10, 주체107(2018).

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

주체107(2018)년 6월 5일 원고접수

Relationship between the Generalized Cyclotomic Numbers with Respect to the Powers of Two Primes of the Form $8k+5$

Choe Chung Hyok

We find out some relationships between the generalized cyclotomic numbers with respect to the powers of two primes, where both the primes are congruent to 5 modulo 8.

Key words: cyclotomic number, generalized cyclotomic number