김일성종합대학학보 주체108(2019)년
수 학 제65권 제3호

$8k+5$와 같은 형태의 두 씨수의 제곱들에 관한 일반화된 원분수의 계산

최 충 혁

원분수 및 일반화된 원분수들에 대한 연구는 수론의 오래고도 중요한 한가지 주제이다.[1－4] 선행연구[3, 4]에서는 기껏 1개의 씨수가 $4k+1$과 같은 형태를 가지는 씨수들 또는 이러한 씨수들의 제곱들에 관한 위수가 2의 제곱인 일반화된 원분수들의 계산공식이 밝혀졌다. 또한 선행연구[2]에서는 2개의 $4k+1$과 같은 형태의 씨수들의 제곱들에 관한 위수가 2의 제곱인 일반화된 원분수들의 성질들이, 선행연구[1]에서는 $8k+5$와 같은 형태의 2개의 씨수들의 제곱에 관한 일반화된 원분수들사이의 몇가지 관계식이 밝혀졌다. 그러나 이 경우에 일반화된 원분수들의 계산공식은 밝혀지지 않았다. 그러므로 이 론문에서는 $8k+5$와 같은 형태의 2개의 씨수들의 제곱에 관한 일반화된 원분수들을 계산하는 공식을 얻으려고 한다.

n을 1보다 큰 정의 옹근수라고 하고 D_0을 환 $\mathbf{Z}_n$의 가역원소군 $\mathbf{Z}_n^*$에서의 지표가 d인 부분군이라고 하자. 그리고 $\{D_0, \cdots, D_{d-1}\}$을 $\mathbf{Z}_n^*$에서의 D_0의 왼쪽합동류들이라고 하자. 이때 n이 씨수이면 D_i들을 위수가 d인 고전적원분클라스, $0\le i, j\le d-1$인 임의의 i, j에 대하여 $|(D_i+[1])\cap D_j|$들을 고전적원분수라고 부른다.[3] 또한 n이 합성수이면 D_i들을 위수가 d인 일반화된 원분클라스, $0\le i, j\le d-1$인 임의의 i, j에 대하여 $|(D_i+[1])\cap D_j|$들을 일반화된 원분수라고 부른다.[3]

n이 1보다 큰 정의 옹근수이고 a는 n과 서로 소인 옹근수라고 하자. 이때 $\mathbf{Z}_n^*$에서의 $[a]$의 위수가 $\varphi(n)$이면 즉 $[a]$가 군 $\mathbf{Z}_n^*$의 생성원소이면 a를 n의 원시뿌리라고 부른다.[3] 여러개 정의 옹근수들의 원시뿌리로 되는 옹근수를 그 정의 옹근수들의 공통원시뿌리라고 부른다.

론문에서 p_1, p_2가 $8k+5$와 같은 형태의 씨수들이고 k_1, k_2가

$$\gcd(\varphi(p_1^{k_1}),\ \varphi(p_2^{k_2}))=4$$

인 정의 옹근수들이라고 하자. 그리고 $n:=p_1^{k_1}p_2^{k_2}$이라고 하고 g를 $p_1^{k_1}, p_2^{k_2}$의 공통원시뿌리라고 하자. 그러면 가역원소군 $\mathbf{Z}_n^*$에서 g의 위수 d는 다음과 같이 계산된다.

$$d=\mathrm{ord}_n(g)=\mathrm{lcm}(\mathrm{ord}_{p_i^{k_1}}(g),\ \mathrm{ord}_{p_2^{k_2}}(g))=\frac{\varphi(p_1^{k_1})\varphi(p_2^{k_2})}{4}$$

이제 W를 가역원소군 $\mathbf{Z}_n^*$에서 g에 의하여 생성된 순환부분군이라고 하자. 그러면

$$d=\frac{\varphi(p_1^{k_1})\varphi(p_2^{k_2})}{4}=\frac{|\mathbf{Z}_n^*|}{4}$$

이므로 이 부분군은 $\mathbf{Z}_n^*$에서의 지표가 4인 부분군이다.

명제 1 환동형넘기기

$$\varphi:\mathbf{Z}_n\to\mathbf{Z}_{p_1^{k_1}}\times\mathbf{Z}_{p_2^{k_2}}$$
$$a\mapsto(a,\ a)$$

에 의한 $(g,\ 1)$ 의 원상을 y 라고 하면 $y,\ y^2,\ y^3 \notin W,\ y^4 \in W$ 로 된다. 또한 $C_i := y^i W\ (i \in \mathbf{Z}_4)$ 들은 가역원소군 $\mathbf{Z}_n^*$ 의 서로 다른 합동류들 즉 위수가 4인 원분클라스들이다.[2]

명제 2 $p_1 \equiv p_2 \equiv 5 \pmod 8$ 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 다음의 식들이 성립한다.[1, 2]

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

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

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

4) $AE+B^2+CD-BC-CE-E^2=p_1^{k_1-1}p_2^{k_2-1}\dfrac{d}{2}$

5) $2AC+2C^2-B^2-D^2-2E^2=-p_1^{2(k_1-1)}p_2^{2(k_2-1)}\dfrac{p_1+p_2-2}{4}$

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

명제 2에서 얻어진 관계식들을 리용하여 일반화된 원분수들을 구해보자.

정리 $M=\dfrac{(p_1-2)(p_2-2)-1}{4}$ 라고 하자. 이때

$$p_1p_2=a^2+4b^2,\quad a\equiv 1 \pmod 4$$

을 만족시키는 옹근수 $a,\ b$ 가 존재하여

$$A=\frac{p_1^{k_1-1}p_2^{k_2-1}}{8}(3a+2M+5),\ \ B=\frac{p_1^{k_1-1}p_2^{k_2-1}}{8}(-a+4b+2M+1)$$
$$C=\frac{p_1^{k_1-1}p_2^{k_2-1}}{8}(-a+2M+1),\ \ D=\frac{p_1^{k_1-1}p_2^{k_2-1}}{8}(-a-4b+2M+1)$$
$$E=\frac{p_1^{k_1-1}p_2^{k_2-1}}{8}(a+2M-1)$$

이 성립한다.

증명 명제 2로부터 $A,\ B,\ C,\ D,\ E$ 들사이에 성립하는 다음의 련립방정식이 얻어진다.

$$\begin{cases} A+B+C+D=p_1^{k_1-1}p_2^{k_2-1}(M+1) \\ B+D+2E=p_1^{k_1-1}p_2^{k_2-1}M \\ 2C+2E=p_1^{k_1-1}p_2^{k_2-1}M \\ AE+B^2+CD-BC-CE-E^2=p_1^{2(k_1-1)}p_2^{2(k_2-1)}\dfrac{(p_1-1)(p_2-1)}{8} \\ 2AC+2C^2-B^2-D^2-2E^2=-p_1^{2(k_1-1)}p_2^{2(k_2-1)}\dfrac{p_1+p_2-2}{4} \end{cases}$$

그러므로

$$A_1:=\frac{A}{p_1^{k_1-1}p_2^{k_2-1}},\ B_1:=\frac{B}{p_1^{k_1-1}p_2^{k_2-1}},\ C_1:=\frac{C}{p_1^{k_1-1}p_2^{k_2-1}},\ D_1:=\frac{D}{p_1^{k_1-1}p_2^{k_2-1}},\ E_1:=\frac{E}{p_1^{k_1-1}p_2^{k_2-1}}$$

로 놓으면 우의 련립방정식을 다음과 같이 고쳐쓸수 있다.

$$\begin{cases} A_1+B_1+C_1+D_1=M+1 \\ B_1+D_1+2E_1=M \\ 2C_1+2E_1=M \\ A_1E_1+B_1^2+C_1D_1-B_1C_1-C_1E_1-E_1^2=\dfrac{(p_1-1)(p_2-1)}{8} \\ 2A_1C_1+2C_1^2-B_1^2-D_1^2-2E_1^2=-\dfrac{p_1+p_2-2}{4} \end{cases} \qquad (*)$$

이 련립방정식 (*)의 넷째 식과 다섯째 식으로부터 다음의 식이 얻어진다.

$$-2A_1C_1-2C_1^2+B_1^2+D_1^2+2E_1^2+2(A_1E_1+B_1^2+C_1D_1-B_1C_1-C_1E_1-E_1^2)=\frac{p_1p_2-1}{4}$$

그리고 련립방정식 (*)의 첫 3개의 식을 리용하여 우의 식을 다시 변형하면 다음과 같이 쓸수 있다.

$$\frac{p_1p_2-1}{4}=-2A_1C_1-2C_1^2+3B_1^2+D_1^2+(A_1-C_1)(A_1+C_1-1)-(B_1+D_1)(B_1-D_1)=$$

$$=A_1^2-2A_1C_1-3C_1^2-(A_1-C_1)+2B_1^2+2D_1^2=(A_1-C_1)^2-(A_1-C_1)+(B_1-D_1)^2$$

따라서 다음의 식이 성립한다.

$$p_1p_2=4(A_1-C_1)^2-4(A_1-C_1)+1+4(B_1-D_1)^2=[2(A_1-C_1)-1]^2+4(B_1-D_1)^2$$

그러므로 $a:=2(A_1-C_1)-1,\ b:=B_1-D_1$ 로 놓으면 우의 식을 다음과 같이 간단히 쓸수 있다.

$$p_1p_2=a^2+4b^2$$

그리고 련립방정식 (*)의 첫 3개의 식들을 고려하면 다음의 식이 얻어진다.

$$A_1=\frac{3a+2M+5}{8},\ B_1=\frac{-a+4b+2M+1}{8},\ C_1=\frac{-a+2M+1}{8},$$

$$D_1=\frac{-a-4b+2M+1}{8},\ E_1=\frac{a+2M-1}{8}$$

그러므로

$$A=\frac{p_1^{k_1-1}p_2^{k_2-1}}{8}(3a+2M+5),\ B=\frac{p_1^{k_1-1}p_2^{k_2-1}}{8}(-a+4b+2M+1)$$

$$C=\frac{p_1^{k_1-1}p_2^{k_2-1}}{8}(-a+2M+1),\ D=\frac{p_1^{k_1-1}p_2^{k_2-1}}{8}(-a-4b+2M+1)$$

$$E=\frac{p_1^{k_1-1}p_2^{k_2-1}}{8}(a+2M-1)$$

이다. 또한 련립방정식 (*)의 둘째 식과 셋째 식에 의하여 M 은 짝수이고 $B_1+D_1=2C_1$ 이 성립한다는것이 나온다. 그러므로 첫째 식은 $A_1+3C_1=M+1$ 과 같이 변형된다. 이로부터 A_1 과 C_1 의 짝홀성은 다르다는것을 알수 있다. 따라서 $a=2(A_1-C_1)-1\equiv 1 \pmod 4$ 이다.(증명끝)

선행연구[5]에 의하면 p_1, p_2가 $\gcd(p_1-1,\ p_2-1)=4$인 경우

$$p_1p_2=a^2+4b^2,\ a\equiv 1\ (\text{mod}\ 4)$$

을 만족시키는 쌍 $(a,\ |b|)$는 2개 존재한다. 그러므로 정리 1을 리용하여 위수가 4인 일반화된 원분수들을 유일하게 결정할수는 없다. 여기서 a가 취할수 있는 2개의 값은 여러개의 공통원시뿌리들가운데서 어느것을 g로 선택하는가에 따라 달라지는 값들이다.

이제는 실례로 $p_1=5,\ p_2=13,\ k_1=2,\ k_2=1$인 경우에 정리 1을 리용하여 일반화된 원분수들을 결정해보자.

우선 $5\cdot 13=1^2+4\cdot 4^2=7^2+4\cdot 2^2$이므로 $p_1p_2=a^2+4b^2,\ a\equiv 1\ (\text{mod}\ 4)$인 쌍 $(a,\ |b|)$를 결정하면 $(1,\ 4),\ (-7,\ 2)$이다.

다음으로 $M=(33-1)/4=8$이므로 $a=1$인 경우에는 $A=15$이고 $a=-7$인 경우에는 $A=0$이다. 그런데 공통원시뿌리로 $g=2$를 취했다고 하면 직접적인 계산에 의하여 $A>0$이라는것을 확인할수 있다. 따라서 $A=15$이고 $a=1$이다. 그러므로 $|b|=4$이다. 따라서 $b=4$인 경우에는 $B=20$이고 $b=-4$인 경우에는 $B=0$이다. 그런데 직접적인 계산에 의하여 $B=0$이라는것을 확인할수 있다. 따라서 $b=-4$이다. 결국 일반화된 원분수들은 다음과 같다.

$$A=15,\ B=0,\ C=10,\ D=20,\ E=10$$

참 고 문 헌

[1] **김일성**종합대학학보 수학, 64, 4, 6, 주체107(2018).

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

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

[4] C. Choe, Int.; J. Number Theory, 14, 7, 2083, 2018.

[5] L. Hu et al.; Des. Codes Cryptogr., 69, 233, 2013.

주체108(2019)년 3월 15일 원고접수

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

Choe Chung Hyok

In this paper, we calculate the generalized cyclotomic numbers with respect to two prime powers, where both the primes are congruent to 5 modulo 8.

Key words: cyclotomic number, generalized cyclotomic number