김일성종합대학학보 주체110(2021)년
수 학 제67권 제1호

위수가 4인 일반화된 원분클라스들로부터 얻어지는 몇가지 가우스주기의 계산

박충일, 최충혁

CDMA통신체계에서 서로 다른 사용자들의 신호들을 구별하는데서 널리 리용되는 WBE부호책이나 MWBE부호책들을 구성하거나 주파수비약렬을 얻는데 일반화된 원분수와 일반화된 원분클라스들이 리용된다.[2, 3]

선행연구[2]에서는 계차모임 및 거의계차모임을 리용하여 부호책을 구성하였으며 선행연구[3]에서는 두 씨수에 관한 위수가 4인 일반화된 원분클라스들로부터 얻어지는 가우스주기를 계산하였으며 그것을 부호책구성에 적용하였다.

한편 선행연구[1]에서는 두 씨수의 제곱들에 관한 위수가 4인 일반화된 원분클라스들을 구성하고 일반화된 원분수를 계산하는 공식을 얻었다.

이로부터 우리는 두 씨수의 제곱들에 관한 위수가 4인 일반화된 원분클라스들로부터 얻어지는 몇가지 가우스주기를 계산하였다.

$p_1,\ p_2$를 $8k+5$모양의 씨수, $k_1,\ k_2$를 $\gcd(\varphi(p_1^{k_1}),\ \varphi(p_2^{k_2}))=4$를 만족시키는 정의옹근수라고 하자.

$n=p_1^{k_1}p_2^{k_2}$이고 g를 $p_1^{k_1},\ p_2^{k_2}$의 공통원시뿌리라고 하면 군 $\mathbf{Z}_n^*$에서 g의 위수는

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

으로 된다.

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

이제 $y\in\mathbf{Z}_n$을 환동형넘기기

$$\begin{aligned}\varphi:\ \mathbf{Z}_n\ &\cong\ \mathbf{Z}_{p_1^{k_1}}\times\mathbf{Z}_{p_2^{k_2}}\\ a\ &\mapsto\ (a,\ a)\end{aligned}$$

에 의한 $(g,\ 1)$의 원상 즉 $\varphi(y)=(g,\ 1)$이라고 하자.

이때 $D_i:=y^iW,\ i\in\mathbf{Z}_4$들은 가역원소군 $\mathbf{Z}_n^*$의 서로 다른 합동류들 즉 위수 4인 일반화된 원분클라스들이고 따라서 $\mathbf{Z}_n^*=\bigcup_{i=0}^{3}D_i$이다.

그리고 $R:=p_1p_2\mathbf{Z}_n,\ P:=p_1\mathbf{Z}_n-R,\ Q:=p_2\mathbf{Z}_n-R$라고 하면 $\mathbf{Z}_n=\mathbf{Z}_n^*\cup P\cup Q\cup R$이다.

명제 1 [1] $p_1\equiv p_2\equiv 5\ (\mathrm{mod}\ 8)$일 때 일반화된 원분수행렬은 $\begin{pmatrix}A & B & C & D\\ B & D & E & E\\ C & E & C & E\\ D & E & E & B\end{pmatrix}$로 된다.

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

명제 2[1] $p_1 \equiv p_2 \equiv 5 \pmod 8$, $M = \dfrac{(p_1-2)(p_2-2)-1}{4}$ 이라고 하자.

이때 $p_1p_2 = a^2+4b^2$, $a \equiv 1 \pmod 4$ 을 만족시키는 옹근수 a, b 가 있어서

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

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

이 성립된다. 여기서 A, B, C, D, E 는 명제 1에서 정의된 값들이다.

정리 1 매 $w \in P \cup Q \cup R$ 에 대하여 다음의 식이 성립된다.

$$|D_i \cap (D_j+w)| = \begin{cases} d/4, & i \neq j,\ w \in P \cup Q \\ 0, & i \neq j,\ w \in R \\ d(p_2-5)/[4(p_2-1)], & i = j,\ w \in P \\ d(p_1-5)/[4(p_1-1)], & i = j,\ w \in Q \\ d, & i = j,\ w \in R \end{cases}$$

증명 x 를 모임 $D_i \cap (D_j+w)$ 의 원소라고 하면 $x = y^i g^a = y^j g^b + w$ 인 $a, b \in \mathbf{Z}_d$ 가 존재하므로 다음의 식을 만족시키는 $a, b \in \mathbf{Z}_d$ 의 개수를 구하면 된다.

$$y^i g^a = y^j g^b + w \tag{1}$$

그런데 식 (1)은 다음의 식과 동등하다.

$$\begin{cases} g^{b+j}(g^{a-b+i-j}-1) \equiv w \pmod{p_1^{k_1}} \\ g^b(g^{a-b}-1) \equiv w \pmod{p_2^{k_2}} \end{cases} \tag{2}$$

$w \in P$ 인 경우를 증명하자.

이 경우 $w = p_1^s u$, $u \notin p_1\mathbf{Z}_n \cup p_2\mathbf{Z}_n$ 을 만족시키는 $u (\in \mathbf{Z}_n)$ 가 존재한다.

$s < k_1$ 이라고 가정하고 $a, b \in \mathbf{Z}_d$ 가 식 (2)를 만족시킨다고 하면 식 (2)의 첫번째 식으로부터 $p_1^s \| g^{b+j}(g^{a-b+i-j}-1)$ 이며 g 가 $p_1^{k_1}$ 의 원시뿌리이므로 $\gcd(g,\ p_1)=1$ 이라는것을 고려하면 $p_1^s \| (g^{a-b+i-j}-1)$ 이다. 그런데 g 가 p_1^s 의 원시뿌리이기도 하므로 결국 $\varphi(p_1^s) | (a-b+i-j)$, $\varphi(p_1^{s+1}) \nmid (a-b+i-j)$ 가 성립된다. 따라서

$$a-b+i-j = \varphi(p_1^s)k,\ p_1 \nmid k,\ 0 \le k < d/\varphi(p_1^s) = p_1^{k_1-s}\varphi(p_2^{k_2})/4 \tag{3}$$

를 만족시키는 k 가 존재한다. 이때 식 (2)의 첫번째 식은 $s = k_1$ 이면 식 (3)을 만족시키는 임의의 a, b 에 대하여 성립되고 $s < k_1$ 이면 $g^{b+j} \cdot (g^{\varphi(p_1^s)k}-1)/p_1^s \equiv u \pmod{p_1^{k_1-s}}$ 으로 쓸 수 있는데 $p_1 \nmid (g^{\varphi(p_1^s)k}-1)/p_1^s$, u 이고 g 가 $p_1^{k_1-s}$ 의 원시뿌리이므로 식 (3)을 만족시키는 k 가 하나 주어질 때 b 는 모듈 $\varphi(p_1^{k_1-s})$ 에 관하여 유일하게 결정된다.

한편 식 (2)의 두번째 식으로부터 $g^{a-b}-1 \in \mathbf{Z}^*_{p_2^{k_2}}$ 이므로 $p_2 \nmid (g^{a-b}-1)$ 이며 g 가 p_2 의 원시뿌리이므로 다음과 같다.

$$(p_2-1) \nmid (\varphi(p_1^s)k-i+j) \tag{4}$$

만일 $i \neq j$ 이면 $4 \nmid (i-j)$, $\gcd(\varphi(p_1^s),\ p_2-1) = 4$ 이므로 모든 k 에 대하여 식 (4)가 성

립된다. 그러므로 식 (3)을 만족시키는 k가 하나 주어질 때 식 (2)의 두번째 식을 만족시키는 b는 모듈 $\varphi(p_2^{k_2})$에 관하여 유일하게 결정되게 된다. 따라서 $s=k_1$일 때 식 (2)를 만족시키는 $(a,\ b)\in\mathbf{Z}_d^2$의 개수는 $\varphi(p_2^{k_2})/4\cdot d/\varphi(p_2^{k_2})=4\cdot d$이다.

그리고 $s<k_1$이면 $\gcd(\varphi(p_1^{k_1-s}),\ \varphi(p_2^{k_2}))=4$이므로 $b \bmod \varphi(p_1^{k_1-s})$과 $b \bmod \varphi(p_2^{k_2})$로부터 $b \bmod \varphi(p_1^{k_1-s})\varphi(p_2^{k_2})/4$의 값이 결정되자면 $b \bmod \varphi(p_1^{k_1-s})$과 $b \bmod \varphi(p_2^{k_2})$의 차가 4의 배수여야 한다.

이제 몇개의 $b \bmod \varphi(p_1^{k_1-s})$의 값이 이 조건을 만족시키는가를 따져보자.

$$(g^{\varphi(p_1^s)k}-1)/p_1^s\equiv(g^{\varphi(p_1^s)l}-1)/p_1^s \pmod{p_1^{k_1-s}}\Leftrightarrow g^{\varphi(p_1^s)k}\equiv g^{\varphi(p_1^s)l} \pmod{p_1^{k_1}}\Leftrightarrow$$
$$\Leftrightarrow\varphi(p_1^s)k\equiv\varphi(p_1^s)l \pmod{\varphi(p_1^{k_1})}\Leftrightarrow k\equiv l \pmod{p_1^{k_1-s}}$$

이므로 모듈 $p_1^{k_1-s}$에 관하여 합동이 아닌 매 k에 대하여 $b \bmod \varphi(p_1^{k_1-s})$의 값은 서로 다르다. 따라서 $b \bmod \varphi(p_1^{k_1-s})$ 가 취하는 서로 다른 $\varphi(p_1^{k_1-s})$ 개의 값가운데서 $b \bmod \varphi(p_2^{k_2})$의 값과의 차가 4의 배수로 되는것은 $\varphi(p_1^{k_1-s})/4$개이다.

결국 식 (3)을 만족시키는 k의 $p_1^{k_1-s}\varphi(p_2^{k_2})/4-p_1^{k_1-s-1}\varphi(p_2^{k_2})/4=\varphi(p_1^{k_1-s})\varphi(p_2^{k_2})/4$개 값들가운데서 $1/4$에 해당한 값들에 대해서만 $b \bmod \varphi(p_1^{k_1-s})$과 $b \bmod \varphi(p_2^{k_2})$으로부터 $b \bmod \varphi(p_1^{k_1-s})\varphi(p_2^{k_2})/4$의 값이 결정되며 이렇게 얻어지는 b와 k로부터 a는 유일하게 정해진다. 그러므로 식 (2)를 만족시키는 $(a,\ b)\in\mathbf{Z}_d^2$의 개수는 다음과 같다.

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

또한 만일 $i=j$이면 식 (4)는 $(p_2-1)\nmid\varphi(p_1^s)k$로 쓸수 있으므로 $(p_2-1)/4\nmid k$인 k에 대해서만 식 (4)가 성립된다. 따라서 식 (4)를 만족시키는 k의 값의 개수는 $s=k_1$이면 $\dfrac{\varphi(p_2^{k_2})}{4}-\dfrac{\varphi(p_2^{k_2})/4}{(p_2-1)/4}=\dfrac{p_2^{k_2-1}(p_2-5)}{4}$이고 $s<k_1$이면

$$\frac{p_1^{k_1-s}\varphi(p_2^{k_2})}{4}-\frac{p_1^{k_1-s}\varphi(p_2^{k_2})/4}{p_1}-\frac{p_1^{k_1-s}\varphi(p_2^{k_2})/4}{(p_2-1)/4}+\frac{p_1^{k_1-s}\varphi(p_2^{k_2})/4}{p_1(p_2-1)/4}=\frac{\varphi(p_1^{k_1-s})p_2^{k_2-1}(p_2-5)}{4}$$

이다. 그러므로 우에서 론의한 $i\neq j$ 인 경우와 마찬가지로 식 (2)를 만족시키는 $(a,\ b)\in\mathbf{Z}_d^2$의 개수를 구하면 $s=k_1$일 때에는 $\dfrac{p_2^{k_2-1}(p_2-5)}{4}\cdot\dfrac{d}{\varphi(p_2^{k_2})}=\dfrac{d}{4}\cdot\dfrac{p_2-5}{p_2-1}$이고 $s<k_1$일 때에는 $\dfrac{1}{4}\cdot\dfrac{\varphi(p_1^{k_1-s})p_2^{k_2-1}(p_2-5)}{4}\cdot\dfrac{d}{\varphi(p_1^{k_1-s})\varphi(p_2^{k_2})/4}=\dfrac{d}{4}\cdot\dfrac{p_2-5}{p_2-1}$이다.

$w\in Q$이거나 $w\in R$인 경우에도 우와 류사하게 증명할수 있으므로 략한다.(증명끝)

$\zeta:=e^{2\pi i/n}$이면 $\mathbf{Z}_n$의 더하기지표전부는 $\Psi_n^{(h)}(m)=\zeta^{mh},\ 0\le h\le n-1$로 주어진다.

$\mathbf{Z}_n$의 매 비지 않은 부분모임 M에 대하여 $\Psi_n^{(h)}(M):=\sum\limits_{m\in M}\Psi_n^{(h)}(m)$이라고 약속하자.

보조정리 $0\le h\le n-1$일 때 다음의 사실들이 성립된다.

$$\Psi_n^{(h)}(R)=\begin{cases}p_1^{k_1-1}p_2^{k_2-1}, & p_1^{k_1-1}p_2^{k_2-1}\mid h\\ 0, & p_1^{k_1-1}p_2^{k_2-1}\nmid h\end{cases}$$

$$\Psi_n^{(h)}(P)=\begin{cases}p_1^{k_1-1}\varphi(p_2^{k_2}), & p_1^{k_1-1}p_2^{k_2}\mid h\\ -p_1^{k_1-1}p_2^{k_2-1}, & p_1^{k_1-1}p_2^{k_2-1}\mid h,\ \ p_1^{k_1-1}p_2^{k_2}\nmid h\\ 0, & p_1^{k_1-1}p_2^{k_2-1}\nmid h\end{cases}$$

$$\Psi_n^{(h)}(Q)=\begin{cases}\varphi(p_1^{k_1})p_2^{k_2-1}, & p_1^{k_1}p_2^{k_2-1}\mid h\\ -p_1^{k_1-1}p_2^{k_2-1}, & p_1^{k_1-1}p_2^{k_2-1}\mid h,\ \ p_1^{k_1}p_2^{k_2-1}\nmid h\\ 0, & p_1^{k_1-1}p_2^{k_2-1}\nmid h\end{cases}$$

증명 $R=\{p_1p_2j\mid 0\le j\le p_1^{k_1-1}p_2^{k_2-1}-1\}$ 이므로 $\Psi_n^{(h)}(R)=\sum_{j=0}^{p_1^{k_1-1}p_2^{k_2-1}-1}e^{2hp_1p_2j\pi i/n}$ 이다. 따라서 $e^{2hp_1p_2\pi i/n}\ne 1$ 즉 $hp_1p_2/n\notin\mathbf{Z}$ 이면 $\Psi_n^{(h)}(R)=\dfrac{1-(e^{2hp_1p_2\pi i/n})^{p_1^{k_1-1}p_2^{k_2-1}}}{1-e^{2hp_1p_2\pi i/n}}=0$ 이고 $hp_1p_2/n\in\mathbf{Z}$ 이면 $\Psi_n^{(h)}(R)=p_1^{k_1-1}p_2^{k_2-1}$ 이다. 또한 $P\cup R=\{p_1j\mid 0\le j\le p_1^{k_1-1}p_2^{k_2}-1\}$ 이므로 $hp_1/n\notin\mathbf{Z}$ 이면 $\Psi_n^{(h)}(P\cup R)=\dfrac{1-(e^{2hp_1\pi i/n})^{p_1^{k_1-1}p_2^{k_2}}}{1-e^{2hp_1\pi i/n}}=0$ 이고 $hp_1/n\in\mathbf{Z}$ 이면 $\Psi_n^{(h)}(P\cup R)=p_1^{k_1-1}p_2^{k_2}$ 이다.

이때 $\Psi_n^{(h)}(P)=\Psi_n^{(h)}(P\cup R)-\Psi_n^{(h)}(R)$ 임을 고려하면 결과가 나온다.

$\Psi_n^{(h)}(Q)$ 에 대해서도 같은 방법으로 증명할수 있다.(증명끝)

정리 2 $\gcd(h,\ n)=1$ 일 때 $\Psi_n^{(h)}(D_0)=\Psi_n^{(h)}(D_2)=0$ 이거나

$$\Psi_n^{(h)}(D_0)=(p_1^{k_1-1}p_2^{k_2-1}\pm p_1^{k_1-1}p_2^{k_2-1}\sqrt{a})/2,\ \Psi_n^{(h)}(D_2)=(p_1^{k_1-1}p_2^{k_2-1}\mp p_1^{k_1-1}p_2^{k_2-1}\sqrt{a})/2$$

이다.

참 고 문 헌

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

[2] C. Ding et al.; Des. Codes Cryptogr., 46, 113, 2008.

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

주체109(2020)년 9월 5일 원고접수

Calculation of Some Gauss Periods from Generalized Cyclotomic Classes of Order 4

Pak Chung Il, Choe Chung Hyok

We calculate some Gauss periods obtained from generalized cyclotomic classes of order 4 in respect to two prime powers.

Keywords: generalized cyclotomic classes, Gauss period