通信情報保護學會誌
第3卷 第3號, 1993.9

# 확산 대역 통신에 응용되는 Legendre수열

오정환*, 윤석임**

## 1. 서 론

정보 보호 기능이 뛰어난 확산대역 통신은 신호를 전송하기 위해 필요한 최소의 대역 폭보다 넓은 대역폭을 이용하여 신호를 전송하는 통신방식이다. 여러가지 방식중 직접 시퀀스(direct sequence) 방식에서는 신호의 대역폭을 확산시키고 축소시키는 작용은 송수신기 사이에 공유하고 있는 확산(spreading) 수열에 의해 수행되는데 이 수열을 모르는 사용자들에게 확산된 신호는 잡음처럼 간주되는 특징을 갖는다. 이러한 성질을 이용하여 다수의 사용자가 같은 주파수 대역을 공동사용할 수 있는 다원접속방식을 구성할 수 있다. 코드 분할 다중 접속(code division multiple access, CDMA)방식의 통신에서는 서명(signature) 수열을 각 사용자에게 부과하여 통신하는데 이때의 수열은 동기화(synchronization)가 쉽고, 또 그러한 수열간에는 간섭(multi-user interference) 현상이 극소화 되어야 한다. 본 논문에서는 이러한 수열을 위한 이차 잉여(quadratic residue)에 의한 Legendre수열의 응용을 살펴본다.

## 2. 이차잉여 수열

이차 잉여를 정의하고, 그로부터 Legendre의 기호를 정의하는 것과 관련된 Euler의 판정식, 이차잉여의 상호 법칙등은 [오]의 제3절에 정리되어 있다. 이 절에서는 2차 잉여류와 Legendre기호, 그리고 이차 잉여의 상호법칙에 대하여 언급한다. 일반적인 2차 합동식 $ax^2 + bx + c \equiv 0 (\mathrm{mod}\ n)$은 n의 소인수 p를 법으로 하는 합동식으로, 즉, $ax^2 + bx + c \equiv 0 (\mathrm{mod}\ p)$로 변환하고, 이 합동식은 다시 일반 2차 방정식의 근의 공식을 유도할 때와 비슷한 방법에 의하여 결과적으로는 $x^2 \equiv a (\mathrm{mod}\ p)$를 푸는 문제로 귀착한다.

정의 2.1 $x^2 \equiv a (\mathrm{mod}\ p)$가 해를 가질때, a를 법 p의 2차 잉여류(quadratic residue, mod p)라 하고, 해를 가지지 않을 때, a를 법 p의 2차 비 잉여류(quadratic non-residue, mod p)라 한다.

p가 소수이고 a가 법 p의 2차 잉여류이면, $p \nmid a$이고, 어떤 x가 존재하여 $a \equiv x^2 (\mathrm{mod}\ p)$가 성립한다. 그런데 이 임의의 정수 x는 $0, 1, 2, \cdots\cdots, p-1 (\mathrm{mod}\ p)$ 중의 어느 하나와 합동이므로, a는

$$1^2, 2^2, \cdots\cdots, (p-1)^2 (\mathrm{mod}\ p)$$

의 어느 하나와 합동이다. 실제로는 $p-x \equiv -x (\mathrm{mod}\ p)$이므로, $(p-x)^2 \equiv (-x)^2 (\mathrm{mod}\ p)$, 즉, $(p-$

* 연세대학교 수학과
** 덕성여자대학교 수학과

$x)^2 = (x)^2 (\text{mod } p)$가 성립한다. 따라서, a가 법 p의 2차 잉여류가 되기 위해서는 a는

$$1^2, 2^2, \cdots\cdots, (\frac{p-1}{2})^2 \ (\text{mod } p)$$

중의 어느 하나와 합동이다. 그리고 이들은 어느 두 정수도 법 p에 관하여 합동이 되지 않는다. 따라서 정수 1,2,……, p-1중에는 꼭 $(\frac{p-1}{2})$개의 2차 잉여류와, 꼭 $(\frac{p-1}{2})$개의 2차 비 잉여류가 있다.

정의 2.2 소수 p가 홀수이고, $p \nmid a$일때, Legendre의 기호$(\frac{a}{p})$는 다음과 같이 정의한다.

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & a\text{가 법 p의 2차 잉여류인 경우} \\ -1, & a\text{가 법 p의 2차 비잉여류인 경우} \end{cases}$$

보기 p=13 일 때의 2차 잉여류와 2차 비 잉여류를 구하고, 해당되는 Legendre의 기호를 계산해 보자. $(\frac{p-1}{2}) = 6$이므로, 법 13의 2차 잉여류는 $1^2, 2^2, 3^2, 4^2, 5^2, 6^2$ 즉, 1,4,9,3,12,10이고, 2차 비 잉여류는 2,5,6,7,8,11이다. 따라서 다음과 같은 Legendre의 기호의 값을 얻는다. $(\frac{2}{13}) = -1$, $(\frac{3}{13}) = 1$, $(\frac{4}{13}) = 1$, $(\frac{5}{13}) = -1$. 또한, $18 \equiv 5 (\text{mod } 13)$이고, 5가 2차 비 잉여류이므로, 18 도 비 잉여류가 된다. 즉, $(\frac{5}{13}) = -1$.

Legendre의 기호는 18세기, 2차 잉여류를 계산하기 위해서 불란서의 수학자 Legendre가 처음 소개한 것이다. 이 Legendre기호를 법이 합성수가 되는 경우에 확장할 수 있도록 한 것이 Jacobi의 기호이다. 그 정의는 $n > 1$이고, $n = p_1 p_2 \cdots p_r$로 소인수분해 될 때, n과 서로소인 정수 a에 대해, $(\frac{a}{n})$은 Legendre의 기호를 사용하여 $(\frac{a}{p_1})(\frac{a}{p_2}) \cdots (\frac{a}{p_r})$이 된다.

Legendre의 기호의 정의로부터 쉽게 얻어지는 몇 가지 성질은 다음과 같다.

(i) $(\frac{a^2}{p}) = 1$,
(ii) $(\frac{1}{p}) = 1$,
(iii) $a \equiv b (\text{mod } p)$이면, $(\frac{a}{p}) = (\frac{b}{p})$.

가 성립하고, 보다 일반적으로는, 다음의 Euler의 판정식이 있다.

정리 2.3 (Euler의 판정식) 소수 p가 홀수이고, $p \nmid a$이면, 다음 식이 성립한다.

$$(\frac{a}{p}) = a^{\frac{(p-1)}{2}} (\text{mod } p).$$

증명 [Bu]의 216쪽 참고.

또 이 판정식으로부터 다음의 따름 정리를 얻는다. 즉,

따름정리 소수 p가 홀수이고, $p \nmid a$, $p \nmid b$이면,

$$(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p}).$$

Euler의 판정식으로부터 $(\frac{-1}{p}) = (-1)^{\frac{(p-1)}{2}} (\text{mod } p)$인데, 이것은 다음과 같이 풀어서 알아두는 것이 더 유용하다. 즉,

$$\left(\frac{-1}{p}\right) = \begin{cases} +1, & p \equiv 1 (\text{mod } 4) \\ -1, & p \equiv 3 (\text{mod } 4) \end{cases}$$

보기 합동식 $x^2 \equiv 19 (\text{mod } 23)$이 해를 가지는지의 여부를 살펴보자. $19 \equiv -4 (\text{mod } 23)$이므로,

$$\left(\frac{19}{23}\right) = \left(\frac{-4}{23}\right) = \left(\frac{-1}{23}\right)\left(\frac{2}{23}\right)^2 = -1.$$

따라서 위의 합동식은 해를 갖지 않는다.

정리 2.4 (Gauss의 보조정리) 소수 p가 홀수이고, $p \nmid a$라 하고, n개의 정수 $a, 2a, 3a, \cdots\cdots, \frac{(p-1)}{2}a$를 법 p에 대하여 $-\frac{(p-1)}{2}$와 $\frac{(p-1)}{2}$에 들어있는 잉여로 대치시켰을 때, 그 중에 포함된 음수 잉여의 개수를 n이라 하면, Legendre의 기호 $(\frac{a}{p})$는 $(-1)^n$과 같다.
증명 [Bu]의 226쪽 참고.

정리 2.5 (2차 잉여류의 상호법칙, Quadratic Reciprocity Law) 소수 p와 q가 서로 다른 홀수이면 다음 등식이 성립한다.

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}$$

증명 [Bu]의 235쪽 참고.

보기 $(\frac{7}{61})$을 구하여 보자.

$$\left(\frac{7}{61}\right) = (-1)^{\frac{60}{2}\frac{6}{2}}\left(\frac{61}{7}\right) = \left(\frac{5}{7}\right)$$
$$= (-1)^{\frac{6}{2}\frac{4}{2}}\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

이제 Legendre 수열을 정의하고 관계된 성질들을

살펴보자.

**정의 2.6** Legendre 기호 $(\frac{a}{p})$가 법 $p$에 대한 이차 잉여인 경우, 이차 비잉여인 경우, 그리고 $a \equiv 0 \pmod{p}$인 경우 각각 +1, −1, 0으로 정의할 때, $s_n = (\frac{n}{p})$를 Legendre수열이라 한다.

보기 $p$=7일때 $s_n$ = 0, 1, 1, −1, 1, −1, −1, 0, …이며 이는 주기 7을 가지고 반복된다.

이 $s_n$은 Euler의 판정식에 의해 편리하게 생성된다. 즉, $s_n = (\frac{n}{p}) \equiv n^{\frac{(p-1)}{2}} \pmod{p}$이다.

**정의 2.7** a가 p에 대한 이차잉여일 때, $s_{na} = s_n$이다. 또 a가 p에 대한 이차 비잉여일 때, $s_{na} = -s_n$이다.
증명 : $s_{na} = (\frac{na}{p}) = (\frac{n}{p}) \cdot (\frac{a}{p}) = \pm (\frac{n}{p})$ 이어서 $(\frac{a}{p})$의 부호(sign)에 따라 $s_n$과 $-s_n$이 결정된다.

특별히 p−1이 p의 이차 비잉여인 경우 $s_n$은 antisymmetric이 된다. 이러한 $s_{-n} = -s_n$인 성질에 의하여 특이한 이산 Fourier변환(Discrete Fourier Transform, DFT)을 한다.

**정의 2.8** Legendre 수열의 DFT는 다음과 같이 주어진다.

$$S_m = \sum_{n=0}^{p-1} s_n e^{-2\pi inm/p}$$

여기서 $m \equiv 0 \pmod{p}$이라면 $S_0 = 0$이다.

**정리 2.9** $S_m$은 $s_m$의 상수배이다.
증명 : 임의의 m에 대하여 $s_n$은 $s_{nm}(\frac{m}{p}) = s_{nm}\, s_m$으로 대치될 수 있다. 따라서

$$S_m = s_m \sum_{n=0}^{p-1} s_{nm} e^{-2\pi inm/p}$$

이다. $nm = k$, $m \not\equiv 0 \pmod{p}$라면,

$$S_m = s_m \sum_{n=0}^{p-1} s_k e^{-2\pi ik/p} = s_m S_1$$

이다. 또한 $s_0 = 0$이므로 $m \equiv 0 \pmod{p}$인 경우도 성립한다. 따라서 Legendre수열의 DFT인 $S_m$은 $s_m$의 상수배이다.

## 3. Gauss의 합과 Legendre수열의 확산 대역 통신을 위한 자기상관 특성

이제 상수 $S_1$을 결정해 보도록 하자. 이를 위하여 다음 $s(p)$을 생각해 보자.

**정의 3.1** 아래와 같이 정의된 $s(p)$를 Gauss의 합이라 한다.

$$s(p) = \sum_{k=0}^{p-1} (s_k + 1)\, e^{2\pi ik/p}$$

여기서 0이 아닌 k가 p에 대한 이차 잉여이면 $s_k + 1 = 2$이고, 이차 비잉여이면 $s_k + 1 = 0$이다. 따라서 $s(p)$에 영향을 미치는 $k$는 어떤수의 제곱일 경우 뿐이다. 다음 두정리의 증명은 간단하다.

**정리 3.2** $p \equiv 1 \pmod{4}$일 때 $s^2(p) = |s(p)|^2 = p$이고, $p \equiv 3 \pmod{4}$일 때 $s^2(p) = -|s(p)|^2 = -p$이다.

**정리 3.3** 두소수의 곱 pq에 대한 Gauss의 합은 그 각각의 Gauss의 합에 대하여 다음 관계식을 가지고 있다.

$$s(pq) = (-1)^{\frac{(p-1)(q-1)}{4}} s(p) s(q)$$

일반적으로 Gauss의 합 S(n)은 법 4에 대하여 n이 0, 1, 2, 3과 합동일 때 각각 $(1+i)\sqrt{n}$, $\sqrt{n}$, 0, $i\sqrt{n}$ 으로 알려져 있다. 이 Gauss의 합에 대한 결과를 Legendre수열 $s_m$의 DFT에 응용하면 다음과 같은 결과를 얻는다.

$p \equiv 1 \pmod{4}$라면 $S_m = \sqrt{p}\, b_m$이고, $p \equiv 3 \pmod{4}$라면 $S_m = -i\sqrt{p}\, b_m$이다. 여기서 $s_m = 0$을 $\tilde{s}_m = 1$로 바꾸면(이진 수열화 하기 위해) $p \equiv 3 \pmod{4}$인 경우의 새로운 DFT는 $\tilde{S}_m = 1 - i\sqrt{p}\, s_m$이다. 따라서 power spectrum이 $|\tilde{S}_m|^2 = 1 + p$인 이진수열 $\tilde{s}_m = \pm 1$을 얻는다. 물론 $m \equiv 0 \pmod{p}$일 경우는 1이 된다.

Legendre 수열로부터 얻은 이와같은 이진수열은 정의 3.1의 Gauss의 합에 대한 정의와 같이 다음 수열로 변형될 수 있다.

$$r_n^{(m)} = e^{2\pi imn^2/p},\ m = 1, 2, \cdots\cdots,\ p-1$$

에 의하여 $p-1$개의 수열을 얻을 수 있는데 이 수열은 확산 대역 통신에 적합한 낮은 상호 상관관계(*crosscorrelation*)과 뛰어난 자기 상관관계(*autocorrelation*)를 갖고 있다.

다음 하나의 수열 $r_n = e^{2\pi in^2/p}$를 살펴보자. 이 수열은 주기가 p이고 각항의 크기는 1과 같다. 이 수열의 주기적 상관수열 $c_k$는 다음과 같다.

$$c_k = \sum_{n=0}^{p-1} r_n r_{n+k} = e^{-2\pi ik^2/p} \sum_{n=0}^{p-1} e^{-4\pi ink/p}$$

$k \not\equiv 0 \pmod p$인 k에 대하여 1의 pth root of unity에 대한 합이 되므로 $c_k=0$이 된다. 또한 $k \equiv 0 \pmod p$인 $k$에 대하여는 $c_0=p$가 된다. 따라서 자기 상관 관계가 적합함을 알 수 있다. 또한 다른 수열들과의 상호상관 관계 역시 낮아서 확산대역통신에 적합한 수열이 된다.

## 참 고 문 헌

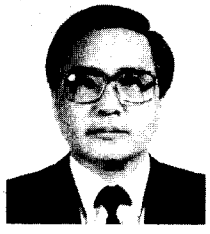
[오] 오정환, 김 철, "Legendre 기호와 암호학", 정보통신보호학회지 2권 2호, p.25-30, 1992.6

[Bu] D.M. Button, Elementary Number Theory Wm.C. Brown, Dubuque, Iowa, 1989

[Ma] J.E. Mazo, "Some theoretical observations on spread-spectrum communications". Bell Syst. Tech. J. 58, 2013-2023 (1979)

[Sc] R.A. Scholtz, "The origins of spread-spectrum communication". IEEE Trans. Communication, 30, 822-852 (1982).

## □ 著者紹介



**오 정 환**

연세대학교 수학과(이학석사 · 박사)
1972년~1974년 미국 Pennsylvania State University
1986년~1987년 미국 University of Illinois at Urabana 방문교수
1964년~현 재 연세대학교 수학과 교수
연구관심분야 : 대수적 수론

**윤 석 임**

성균관대학교 수학과(학사)
연세대학교 수학과(석사)
불란서 Montpellier II 대학교(박사)
현재 : 덕성여자대학교 자연대학 수학과 부교수