스트림암호에서 원시다항식에 대한 고찰★

양 정 모*

요 약

스트림 암호는 1회용 패드(one time pad)형 암호 알고리즘으로 랜덤한 비트(또는 문자)들의 열을 열쇠로 사용하여 평문과 XOR과 같은 간단한 연산을 통해 암호화하므로 알고리즘의 안전성은 사용되는 열쇠의 난수성에 의존한다. 그러므로 사용되는 열쇠에 대해 주기, 선형복잡도, 비선형도, 상관면역도 등의 수학적 분석을 통해 보다 안전한 암호시스템을 설계할 수 있는 장점이 있다. 스트림 암호에서의 암호화 열쇠는 고유다항식을 가지고 LFSR(linear feedback shift register)에서 열쇠이진 수열을 생성하여 사용한다. 이 고유다항식 중 비도가 가장 우수한 다항식이 바로 원시다항식이다. 원시다항식은 스트림 암호뿐만 아니라 8차 원시 다항식을 사용한 블록암호인 SEED암호, 그리고 24차 원시 다항식을 사용하여 설계한 공개열쇠암호인 CR(Chor-Rivest) 암호 등에서도 널리 이용되고 있다. 본 논문의 주요내용은 이러한 암호알고리즘을 연구하는데 사용되는 갈루아(Galois)체에서의 원시다항식에 대한 개념과 다양한 성질들을 고찰해 보고 소수 p의 값이 2이상인 경우 F_p에서의 기약다항식과 원시다항식의 개수를 구하는 정리를 증명해 보았다. 이러한 연구는 보다 비도가 높은 원시다항식을 찾아 새로운 암호알고리즘을 개발하는 기반 연구가 될 수 있다.

A Study on primitive polynomial in stream cipher

Jeong-mo Yang*

ABSTRACT

Stream cipher is an one-time-pad type encryption algorithm that encrypt plaintext using simple operation such as XOR with random stream of bits (or characters) as symmetric key and its security depends on the randomness of used stream. Therefore we can design more secure stream cipher algorithm by using mathematical analysis of the stream such as period, linear complexity, non-linearity, correlation-immunity, etc. The key stream in stream cipher is generated in linear feedback shift register(LFSR) having characteristic polynomial. The primitive polynomial is the characteristic polynomial which has the best security property. It is used widely not only in stream cipher but also in SEED, a block cipher using 8-degree primitive polynomial, and in Chor-Rivest(CR) cipher, a public-key cryptosystem using 24-degree primitive polynomial. In this paper we present the concept and various properties of primitive polynomials in Galois field and prove the theorem finding the number of irreducible polynomials and primitive polynomials over F_p when p is larger than 2. This kind of research can be the foundation of finding primitive polynomials of higher security and developing new cipher algorithms using them.

Key words : irreducible polynomial, Galois field, splitting field, primitive element, primitive polynomial

접수일(2018년 9월 30일), 수정일(1차: 2018년 10월 25일), 게재확정일(2018년 10월 30일)

★ 이 논문은 2018년도 중부대학교 학술연구비 지원에 의하여 이루어진 것임.

* 중부대학교 정보보호학과

1. 서 론

스트림 암호에서 사용되는 암호열쇠는 초기상태 벡터와 열쇠이진 수열을 생성해 내는 고유(특성)다항식에 의해 결정된다. 열쇠이진 수열을 생성하는 고유다항식 중 주기나 선형복잡도 등 수학적으로 비도가 높은 다항식이 바로 원시다항식이다. 따라서 고유다항식은 열쇠의 비도를 결정하는 데 상당한 역할을 한다고 할 수 있다.

1-1 다항식환

체 F의 원소 $a_0, a_1, a_2, \cdots, a_n$과 부정원 x로 이루어진 식 $f(x)=a_0+a_1x+a_2x^2+\cdots+a_nx^n$ $(n=0, 1, 2, \cdots)$, $a_n \neq 0$을 F위의 x에 대한 n차 다항식이라 하고 $a_0, a_1, a_2, \cdots, a_n$을 이 다항식의 계수, n을 차수라고 한다. 또, $\deg f(x)=n$으로 나타내고 a_n을 이 다항식 $f(x)$의 최고차항의 계수라고 한다. 또, 체 F위의 다항식 전체의 집합을 $F[x]$로 나타낸다.

[정의 1.1] 가환환 $(F[x], +, \cdot)$을 체 F위의 다항식환(polynomial ring)이라고 한다.

[정의 1.2] 체 F위의 다항식 $f(x), g(x) \in F[x]$에 대하여 $g(x)=f(x)h(x)$인 다항식 $h(x) \in F[x]$가 존재할 때 $f(x)$을 $g(x)$의 약수 또는 인수라 하고 $g(x)$을 $f(x)$의 배수라고 한다. 이를 $f(x) \mid g(x)$로 나타내고 $f(x)$의 배수 전체의 집합을 $(f(x))$로 나타내기로 한다. 즉,

$$(f(x)) = \{f(x)h(x) \mid h(x) \in F[x]\}$$

이다. 또, $\gcd\{f(x), g(x)\}=1$일 때 이 두 다항식은 서로소(relative prime)라 한다.

[정의 1.3] 체 F위의 다항식 $p(x) \in F[x]$ $(\deg p(x) \geq 1)$에 대하여 $f(x) \mid p(x)$이면 어떤 $a \in F^*$에 대하여 $f(x)=a$ 또는 $f(x)=ap(x)$가 성립할 때 $p(x)$을 $F[x]$의 기약다항식(irreducible polynomial) 또는 체 F위에서 기약인 다항식이라 한다. 한편, 다항식 $p(x)$가 기약다항식이 아닐 때 즉,$p(x)=f(x)g(x)$, $(\deg f(x), \deg g(x) \geq 1)$인 다항식 $f(x), g(x) \in F[x]$가 존재할 때 $p(x)$을 $F[x]$의 가약다항식(reducible polynomial) 또는 체 F위에서 가약인 다항식이라 한다.

[정의 1.4] 체 F가 체 K의 부분체일 때 다항식 $f(x)=a_0+a_1x+\cdots+a_nx^n \in f[x]$와 $\alpha \in K$에 대하여 $f(\alpha)$을 $f(\alpha)=a_0+a_1\alpha+\cdots+a_n\alpha^n \in K$로 나타낸다. 특히, $f(\alpha)=0$일 때 α을 K에서의 다항식 $f(x)$의 근(root) 또는 영점(zero)이라고 한다.

[정리 1.5] 체 F위의 n차 다항식 $f(x)=c_0+c_1x+\cdots+c_{n-1}x^{n-1}+x^n \in F[x]$, $n \geq 1$에 대하여 $f(x)$가 기약다항식이면 가환환 $F[x]/(f(x))$는 체이다.

1-2 예제

[예 1.1] 체 $Z_2=\{0, 1\}$ 위에서 2차 기약다항식과 체 $Z_3=\{0, 1, 2\}$ 위에서 최고차항의 계수가 1인 2차 기약다항식을 구하여라.

[해] (1) 체 $Z_2=\{0, 1\}$ 위에서 2차 다항식은 $x^2, x^2+1, x^2+x, x^2+x+1$ 이다. 이 중에 x^2, x^2+1, x^2+x는 가약다항식이다. 한편, $p(x)=x^2+x+1$에 대하여 $p(0)=0^2+0+1 \neq 0$ $p(1)=1^2+1+1 \neq 0$ 이므로 $p(x)=x^2+x+1$은 Z_2 위에서 기약이다. 한편, 체 $Z_3=\{0, 1, 2\}$ 위에서 최고차항의 계수가 1인 2차 다항식은 $x^2, x^2+1, x^2+2, x^2+x, x^2+2x, x^2+x+1, x^2+x+2, x^2+2x+1, x^2+2x+2$이다. 이중에 3개인 $p_1(x)=x^2+1$, $p_2(x)=x^2+x+2$, $p_3(x)=x^2+2x+2$에 대하여 $x=0, 1, 2$을 각 다항식에 각각 대입하면 $p_1(x) \neq 0$, $p_2(x) \neq 0$, $p_3(x) \neq 0$이므로 $p_1(x), p_2(x), p_3(x)$는 Z_3에서 기약이다.

[예 1.2] 체 Z_2위에서 다항식 $p(x)=x^2+x+1$로 주어졌을 때 $K=Z_2[x]/(p(x))$을 구하고 체 임을 보여라.

[해] 예 1.1에 의하여 $p(x)=x^2+x+1$은 기약다항식이다. 또 체 Z_2위의 다항식 전체의 집합

$Z_2[x]$ 은 단위원 1을 가진 가환환이다. 따라서 정리 1.6에 의하여 $K = Z_2[x]/(p(x))$ 는 체이고 $K=\{a_0+a_1\alpha \mid a_0, a_1\in Z_2\} = \{0, 1, \alpha, 1+\alpha\}$, $\alpha^2+\alpha+1=0$이므로 $\alpha^2 = -1-\alpha = 1+\alpha$ 이다. 이 사실을 이용하면 K에서의 덧셈과 곱셈을 다음과 같이 할 수 있다.

$\alpha+\alpha=0$, $(1+\alpha)+\alpha=1$, $(1+\alpha)+(1+\alpha)=0$,
$\alpha\times\alpha=\alpha^2$, $\alpha^3=\alpha^2\times\alpha=(1+\alpha)\alpha=\alpha+\alpha^2=1$,
$\alpha(1+\alpha)=\alpha+\alpha^2=1$, $(1+\alpha)(1+\alpha)=\alpha$
특히 $K^*=K-\{0\}=\{1, \alpha, \alpha^2\}$, $\alpha^3=1$이다.

2. 원시다항식과 그 성질

2-1. $f(x)$의 분해 체와 원시다항식

임의의 소수 p와 $n\in Z^+$에 대하여 p^n 개의 원소를 가진 유한 체를 위수 p^n 인 **갈루아 체(Galois Field)**라 하고 F_{p^n}으로 나타낸다. 특히, $F_p = Z_p = \{0, 1, \cdots, p-1\}$이다. F_{p^n}은 체 F_p위에서의 다항식 $f(x)=x^{p^n}-x$의 분해체이다. 따라서 모든 $\alpha\in F_{p^n}$에 대하여 $\alpha^{p^n} = \alpha$ 이다. 이후 Z_p 대신 F_p로 나타내기로 하겠다.

[정의 2.1] 체 K을 체 F의 확대체라 하고 $\alpha\in K$라 하자. 영 다항식이 아닌 적당한 다항식 $f(x)\in F[x]$에 대하여 $f(x) = a_0 + a_1x + \cdots + a_nx^n$ 라 하면 $f(\alpha) = a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$ 일 때 α 을 체 F위에서 대수적 원소(Algebraic element)라고 한다. 또 체 K의 원소가 모두 F 위에서 대수적일 때 K을 F의 대수적 확대체(Algebraic extension)라고 한다.

[정리 2.2] 체 K가 체 F의 확대체일 때 $\alpha\in K$가 체 F위에서 대수적이면 다음 세 조건을 만족하는 다항식 $p(x)=b_0+b_1x+\cdots+b_mx^m\in F[x]$가 단 하나 존재한다.

(ⅰ) $\deg p(x) = m \geq 1$이고 $b_m = 1$ 이다.

(ⅱ) $p(\alpha) = b_0 + b_1\alpha + \cdots + b_m\alpha^m = 0$이다.

(ⅲ) 다항식 $f(x)\in F[x]$에 대하여 $f(\alpha) = 0$ 일 필요충분조건은 $F[x]$에서 $p(x) \mid f(x)$이다.

위 정리 2.2을 만족하는 다항식 $p(x)$을 체 F위에서의 α의 최소다항식(Minimum polynomial) 또는 **체 F위에서의 α의 기약다항식**이라 하고 이것을 $p(x)=\min.poly._F\alpha$ 또는 $p(x)=irr(\alpha, F)$로 나타낸다.

[정의 2.3] 체 F의 다항식 $f(x)\in F[x]$, $(\deg f(x)=n\geq 1)$에 대하여 다음 두 조건을 만족하는 F의 확대체 K을 다항식 $f(x)$의 **분해체(splitting field)**라 한다.

(1) $f(x)$는 K안에서 중복을 허락하여 n 개의 근 $\alpha_1, \cdots, \alpha_n$을 가지며 $f(x)$는 K에서 다음과 같이 일차식의 곱으로 인수분해 된다.

$$f(x) = a(x-\alpha_1)\cdots(x-\alpha_n),\ a\in F$$

(2)K는 이와 같은 F의 확대체 중에서 가장 작다.

[정의 2.4] 갈루아 체 F_{p^n}에서 $F_{p^n}^* = F_{p^n}-\{0\} = <\alpha> = \{1, \alpha, \alpha^2, \cdots, \alpha^{p^n-2}\}$, $\alpha^{p^n-1}=1$인 원소 $\alpha\in F_{p^n}$을 체 F_{p^n}의 **원시원소(primitive element)**라 한다. 그리고 F_{p^n}의 원시원소 α의 체 F_p에서의 최소다항식 $\min.poly._{F_p}\alpha$을 체 F_p 위에서의 n 차 **원시다항식(primitive polynomial)**이라고 한다.

[정리 2.5] 갈루아 체 F_{p^n}에서 α가 체 F_{p^n}의 한 원시원소일 때 $p(x) = \min.poly._{F_p}\alpha = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + x^n$ 이라고 하면 원시다항식 $p(x)$는 체 F_p위의 n 차의 기약다항식이고 또 $p(0)\neq 0$이며 $c_0+c_1\alpha+\cdots+c_{n-1}\alpha^{n-1}+\alpha^n=0$,

$$F_{p^n} = F_p(\alpha) = \{a_0+a_1\alpha+\cdots+a_{n-1}\alpha^{n-1} \mid a_0, a_1, \cdots, a_{n-1}\in F_p\}$$

$F_{p^n}^* = F_{p^n}-\{0\} = <\alpha> = \{1, \alpha, \alpha^2, \cdots, \alpha^{p^n-2}\}$, $\alpha^{p^n-1}=1$ 이다.

[정리 2.6] 임의의 소수 p와 양의 정수 n에 대하여 갈루아 체 F_{p^n}에는 $\varphi(p^n-1)$ 개의 원시원소가 존재하고 또한 체 F_p 위의 n 차의 원시다항식은 $\frac{\varphi(p^n-1)}{n}$ 개 존재한다.

2-2. 예제

[예 2.1] 체 F_2 위에서 $f(x) = x^{16} - x$ 의 분해체 F_{2^4} 을 구하고 그의 원시원소와 4차 원시 다항식을 구하여라.

[해] $f(x) = x^{16} - x = (x^4 - x)(x^{12} + x^9 + x^6 + x^3 + 1)$

$= x(x-1)(x^2 + x + 1)(x^{12} + x^9 + x^6 + x^3 + 1)$

한편, 다항식 $p(x) = x^4 + x + 1$ 은 체 F_2 위의 기약다항식이고 $p(x)$ 의 체 F_{2^4} 안에서의 한 근을 α라고 하면 $\alpha^4 + \alpha + 1 = 0$이므로 $\alpha = \alpha$,

$\alpha^2 = \alpha^2, \alpha^3 = \alpha^3,\ \alpha^4 = 1 + \alpha,\ \alpha^5 = \alpha + \alpha^2,$

$\alpha^6 = \alpha^2 + \alpha^3,\ \alpha^7 = \alpha^3 + \alpha^4 = 1 + \alpha + \alpha^3,$

$\alpha^8 = \alpha + \alpha^2 + \alpha^4 = 1 + \alpha^2,\ \alpha^9 = \alpha + \alpha^3,$

$\alpha^{10} = 1 + \alpha + \alpha^2,\ \alpha^{11} = \alpha + \alpha^2 + \alpha^3,$

$\alpha^{12} = 1 + \alpha + \alpha^2 + \alpha^3,\ \alpha^{13} = 1 + \alpha^2 + \alpha^3,$

$\alpha^{14} = 1 + \alpha^3,\ \alpha^{15} = \alpha + \alpha^4 = 1$

$F_{2^4} = \{a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 \mid a_0, a_1, a_2, a_3 \in F_2\}$

$F_{2^4}^* = <\alpha> = \{1, \alpha, \alpha^2, \cdots, \alpha^{14}\},\ \alpha^{15} = 1.$

따라서 α 는 체 F_{2^4} 의 원시원소이고 또 F_{2^4} 에는 $\varphi(15) = 8$ 개의 원시원소 $\alpha,\ \alpha^2,\ \alpha^4, \alpha^7, \alpha^4, \alpha^7, \alpha^8, \alpha^{11}, \alpha^{13}, \alpha^{14}$가 존재한다. 먼저 원시원소 $\alpha, \alpha^2, \alpha^4, \alpha^8$은 기약다항식$p(x) = x^4 + x + 1$의 근 이므로 다음이 성립한다.

$p(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4)(x - \alpha^8),$

$\min.poly._{F_2} \alpha^{2^i} = p(x),\quad (i = 0, 1, 2, 3)$

그리고 나머지 4개의 원소 $\alpha^7, (\alpha^7)^2 = \alpha^{14}, \alpha^7, (\alpha^7)^2 = \alpha^{14}, (\alpha^7)^4 = \alpha^{13}, (\alpha^7)^8 = \alpha^{11}$ 에 대하여 다음이 성립한다.

(ⅰ) $\alpha^7 + \alpha^{14} + \alpha^{13} + \alpha^{11} = 1$

(ⅱ) $\alpha^7\alpha^{14} + \alpha^7\alpha^{13} + \alpha^7\alpha^{11} + \alpha^{14}\alpha^{13} + \alpha^{14}\alpha^{11} + \alpha^{13}\alpha^{11}$

$= \alpha^6 + \alpha^5 + \alpha^3 + \alpha^{12} + \alpha^{10} + \alpha^9 = 0$

(ⅲ) $\alpha^7\alpha^{14}\alpha^{13} + \alpha^7\alpha^{14}\alpha^{11} + \alpha^7\alpha^{13}\alpha^{11} + \alpha^{14}\alpha^{13}\alpha^{11}$

$= \alpha^4 + \alpha^2 + \alpha + \alpha^8 = 0$

(ⅳ) $\alpha^7\alpha^{14}\alpha^{13}\alpha^{11} = \alpha^{15} = 1$

따라서 $q(x) = (x - \alpha^7)(x - \alpha^{14})(x - \alpha^{13})(x - \alpha^{11})$ 이라 하면 다음이 성립한다.

$q(x) = x^4 + x^3 + 1,\ \min.poly._{F_2} (\alpha^7)^{2^i} = q(x),$

$(i = 0, 1, 2, 3)$

그러므로 $p(x)$, $q(x)$ 는 체 F_2 위에서 4차의 원시다항식이다. 한편 $\alpha^3, (\alpha^3)^2 = \alpha^6, (\alpha^3)^4 = \alpha^{12}, (\alpha^3)^8 = \alpha^9$에 대하여 다음이 성립한다.

(ⅰ) $\alpha^3 + \alpha^6 + \alpha^{12} + \alpha^9 = 1$

(ⅱ) $\alpha^3\alpha^6 + \alpha^3\alpha^{12} + \alpha^3\alpha^9 + \alpha^6\alpha^{12} + \alpha^6\alpha^9 + \alpha^{12}\alpha^9$

$= \alpha^9 + \alpha^{15} + \alpha^{12} + \alpha^3 + \alpha^{15} + \alpha^6 = 1$

(ⅲ) $\alpha^3\alpha^6\alpha^{12} + \alpha^3\alpha^6\alpha^9 + \alpha^3\alpha^{12}\alpha^9 + \alpha^6\alpha^{12}\alpha^9$

$= \alpha^6 + \alpha^3 + \alpha^9 + \alpha^{12} = 1$

(ⅳ) $\alpha^3\alpha^6\alpha^{12}\alpha^9 = \alpha^{30} = 1$

따라서 $r(x) = (x - \alpha^3)(x - \alpha^6)(x - \alpha^{12})(x - \alpha^9)$ 이라고 하면 $r(x) = x^4 + x^3 + x^2 + x + 1$,

$\min.poly._{F_2} (\alpha^3)^{2^i} = r(x)\quad (i = 0, 1, 2, 3)$

이지만 $r(x)$ 는 F_2 위에서 원시다항식이 아니다. (α^3 은 원시원소가 아니기 때문이다.) 그리고 원시원소가 아닌 α^5 에 대하여 $(\alpha^5)^2 = \alpha^{10}$, $(\alpha^5)^2 = \alpha^{10}, (\alpha^5)^4 = \alpha^5, (\alpha^5)^8 = \alpha^{10}$ 이 므 로 $<\alpha^5> = <\alpha^{10}> = \{1, \alpha^5, \alpha^{10}\} \neq <\alpha>$, $\{0, 1, \alpha^5, \alpha^{10}\} = F_{2^2}$ 이고 또 $\alpha^5 + \alpha^{10} = 1$, $\alpha^5\alpha^{10} = \alpha^{15} = 1$ 이므로 다음 등식이 성립한다.

$$(x - \alpha^5)(x - \alpha^{10}) = x^2 + x + 1$$

결론적으로 체 F_2 위에서 4차의 기약다항식은

$p(x) = x^4 + x + 1, q(x) = x^4 + x^3 + 1,$

$r(x) = x^4 + x^3 + x^2 + x + 1$

뿐이고 체 F_2 위에서 4차의 원시다항식은 $p(x)$, $q(x)$뿐이다. 체 F_2 에서 2차의 기약다항식은 $x^2 + x + 1$ 뿐이고 일차다항식은 $x,\ x - 1$ 뿐이다. 이들 다항식은 모두 $f(x) = x^{16} - x$ 의 기약약수이며 $f(x)$ 는 체 F_2 위에서 다음과 같이 기약다항식의 곱으로 인수분해 된다.

$f(x) = x^{16} - x$

$= x(x-1)(x^2 + x + 1)(x^{12} + x^9 + x^6 + x^3 + 1)$

$= x(x-1)(x^2 + x + 1)p(x)q(x)r(x)$

3. 주요 정리 및 예제

3-1. 주요 정리

다음 정리는 F_2 에서 정의된 원시다항식을 F_p $(p \geq 2)$ 로 확장하여 생각해 보았다. 이는 스트림 암호에서 원시다항식에 의해 생성되는 열쇠이진

수열을 선택할 수 있는 개수와 주기, 선형복잡도가 소수 p 값이 증가함에 따라 늘어난다는 사실에 주목할 필요가 있다.

[정리 3.1] 체 F_p 위의 다항식환 $F_p[x]$ 에 대하여
(1) 최고차항의 계수가 1인 일차다항식은 꼭 p 개 있다.
(2) 최고차항의 계수가 1인 이차다항식은 꼭 p^2개 있으며, 이 중에서 기약인 다항식은 꼭 $\frac{p(p-1)}{2}$ 개 있다.

[증명] (1) 체 F_p 위의 다항식환 $F_p[x]$ 는
$F_p[x] = \{f(x) | f(x) = a_0 + a_1 x + a_2 x^2 + \cdots\}$
$(a_0, a_1, a_2, \cdots \in F_p)$ 에서 최고차항의 계수가 1인 일차다항식 $p(x) = x + a_0,\ a_0 \in Z_p$ 이므로 꼭 p 개가 있다.
(2) $Z_p[x]$ 에서 최고차항의 계수가 1인 이차다항식 $p(x) = x^2 + a_1 x + a_0,\ a_0, a_1 \in F_p$ 이므로 a_0, a_1 의 개수가 각각 p 개 이므로 이차다항식 $p(x)$ 의 총 개수는 p^2 개 이다. 이 중에 기약다항식의 경우는 a_1 의 경우의 수가 p 가지이고 a_1 값의 각각의 경우마다 a_0 는 $a_0 = 0$ 을 제외한 $p-1$ 가지에서 a_1 값의 합이 p 인 경우에 a_0 값이 같으므로 a_0 의 경우의 수는 $\frac{p-1}{2}$ 가지가 나온다. 따라서 총 경우의 수는 $\frac{p(p-1)}{2}$ 가지이다.

[다른 증명] 기약이 아닌 가약 다항식의 개수는 정의 1.3, 정리 2.2, 정의 1.4와 예 1.1의 방법을 이용하면 $\frac{p(p-1)}{2} + p$ 개가 나온다. 따라서 기약다항식의 총 개수는

$$p^2 - \left\{\frac{p(p-1)}{2} + p\right\} = p^2 - \left(\frac{p^2+p}{2}\right)$$
$$= \frac{p^2-p}{2} = \frac{p(p-1)}{2}$$

이다.

[정리 3.2] 다항식 $f(x) = x^4 + x^3 + 1$의 갈루아체 F_{2^4} 내의 한 근을 β라고 할 때, $\beta^i\ (0 \le i \le 15)$을 $a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3$ $(a_0, a_1, a_2, a_3 \in F_2)$ 의 꼴로 나타낼 수 있고 $F_{2^4}^* = F_{2^4} - \{0\} = <\beta>$이다.

[증명]예 2.1에 의하여 주어진 다항식 $f(x) = x^4 + x^3 + 1$는 원시 기약다항식이다. 그러므로 정리 1.6과 예 1.2에 의하여 $F_{2^4} = F_2[x]/(f(x))$
$= \{a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3 | a_0, a_1, a_2, a_3 \in F_2\}$꼴 로 나타낼 수 있다. 이는 원시원소 β에 의해 생성되므로 $f(\beta) = \beta^4 + \beta^3 + 1 = 0$ 을 이용하면
$F_{2^4}^* = F_{2^4} - \{0\} = <\beta>$이다.

3-2. 주요 예제

다음 예제는 위 정리를 이해하는 데 도움이 될 것이다.

[예제 3.1] p 값이 다음과 같이 주어졌을 때 최고차항의 계수가 1인 2차 기약 다항식의 개수와 원시다항식의 개수를 구하여라.
(1) $p = 5$ (2) $p = 7$

[풀이] (1) 체 F_5 위의 다항식환 $F_5[x]$ 는
$F_5[x] = \{f(x) | f(x) = a_0 + a_1 x + a_2 x^2 + \cdots\}$
$(a_0, a_1, a_2, \cdots \in F_5)$ 에서 최고차항의 계수가 1인 이차다항식 $p(x)$ 는

$$p(x) = x^2 + a_1 x + a_0,\ \ a_0, a_1 \in F_5$$

이므로 $a_1 = 0, 1, 2, 3, 4$ 인 각각의 경우에 a_0 값이 정의 1.3, 정리 2.2, 정의 1.4와 예 1.1의 방법을 이용하면 각각 $\frac{(5-1)}{2} = 2$ 개씩 나오게 된다. 따라서 (a_1, a_0) 의 경우의 수는 $5 \times \frac{(5-1)}{2} = 10$ 개 다. 즉, 2차 기약다항식의 개수가 10개이다. 이 표에 의하면 a_1 값이 1과 4인 경우와 a_1 값이 2와 3인 경우에 a_0 의 값이 같음을 알 수 있다. 한편 $p = 5$ 인 경우 원시다항식의 개수는 정리 2.6에 의하여 $n = 2$ 이므로

$$\frac{\varphi(5^2-1)}{2} = \frac{\varphi(24)}{2} = \frac{\varphi(2^3 \times 3)}{2} = \frac{\varphi(2^3)\varphi(3)}{2}$$

$= \frac{(2^3-2^2)\times 2}{2} = 4$ 이다. 즉, 총 기약다항식 10개 중에 원시다항식이 4개 존재한다는 의미이다.

참고적으로 $p=2$ 인 경우 2차 원시다항식의 개수는 1개밖에 없다.

(2) (1)과 같은 방법으로 하면 $a_1 = 0, 1, \cdots, 6$ 인 각각의 경우에 a_0 값이 각각 $\frac{(7-1)}{2} = 3$ 개씩 나오게 된다. 따라서 (a_1, a_0) 의 경우의 수는 $7 \times \frac{(7-1)}{2} = 21$ 개다. 즉, 2차 기약다항식의 개수가 21개이다. 이 표에 의하면 a_1 값이 1과 6인 경우, 2, 5인 경우 그리고 3, 4인 경우에 a_0 의 값이 같음을 알 수 있다. 한편 $p=7$ 인 경우 원시다항식의 개수는 정리 2.8에 의하여 $n=2$ 이므로

$$\frac{\varphi(7^2-1)}{2} = \frac{\varphi(48)}{2} = \frac{\varphi(2^4\times 3)}{2} = \frac{\varphi(2^4)\varphi(3)}{2}$$

$$= \frac{(2^4-2^3)\times 2}{2} = 8$$ 이 되어 $p=5$ 인 경우의 2배로 증가하게 된다. 즉, 총 기약다항식 21개 중에 원시다항식이 8개 존재한다는 의미이다.

[예 3.2] 체 $F_3 = \{0, 1, 2\}$ 위에서 체 F_{3^3} 의 원시원소와 3차 원시다항식을 구하여라.

[해] 다항식 $p(x) = x^3 - x + 1$ 은 체 F_3 위에서 기약다항식이다. 이제 $\alpha \in F_{3^3}$ 을 $p(x)$ 의 한 근이라고 하면

$p(\alpha) = \alpha^3 - \alpha + 1 = 0$, $\alpha^3 = \alpha - 1 = \alpha + 2$

이고 다음이 성립한다.

$F_{3^3} = \{a_0 + a_1\alpha + a_{2\alpha}^2 \mid a_0, a_1, a_2 \in Z_3\}$, $F_{3^3}^* = <\alpha>$

$\alpha^1 = \alpha$, $\alpha^2 = \alpha^2$, $\alpha^3 = 2 + \alpha$, $\alpha^4 = 2\alpha + \alpha^2$,

$\alpha^5 = 2 + \alpha + 2\alpha^2$, $\alpha^6 = 1 + \alpha + \alpha^2$,

$\alpha^7 = 2 + 2\alpha + \alpha^2$, $\alpha^8 = 2 + 2\alpha^2$, $\alpha^9 = 1 + \alpha$,

$\alpha^{10} = \alpha + \alpha^2$, $\alpha^{11} = 2 + \alpha + \alpha^2$, $\alpha^{12} = 2 + \alpha^2$,

$\alpha^{13} = 2$, $\alpha^{14} = 2\alpha$, $\alpha^{15} = 2\alpha^2$, $\alpha^{16} = 1 + 2\alpha$,

$\alpha^{17} = \alpha + 2\alpha^2$, $\alpha^{18} = 1 + 2\alpha + \alpha^2$,

$\alpha^{19} = 2 + 2\alpha + 2\alpha^2$, $\alpha^{20} = 1 + \alpha + 2\alpha^2$,

$\alpha^{21} = 1 + \alpha^2$, $\alpha^{22} = 2 + 2\alpha$, $\alpha^{23} = 2\alpha + 2\alpha^2$,

$\alpha^{24} = 1 + 2\alpha + 2\alpha^2$, $\alpha^{25} = 1 + 2\alpha^2$, $\alpha^{26} = 1$

따라서 α 는 체 F_{3^3} 의 원시원소이고 또 F_{3^3} 에는 $\varphi(26) = 12$ 개의 원시원소 α, $\alpha^3, \alpha^5, \alpha^7, \alpha^9, \alpha^{11}, \alpha^{15}, \alpha^{17}, \alpha^{19}, \alpha^{21}, \alpha^{23}, \alpha^{25}$ 가 존재하며 예 2.1과 마찬가지 방법으로 하면 다음이 성립함을 알 수 있다.

$p_1(x) = (x-\alpha)(x-\alpha^3)(x-\alpha^9) = x^3 - x + 1 = p(x)$,

$p_2(x) = (x-\alpha^5)(x-\alpha^{15})(x-\alpha^{19}) = x^3 + 2x^2 + x + 1$,

$p_3(x) = (x-\alpha^7)(x-\alpha^{21})(x-\alpha^{11}) = x^3 + x^2 + 2x + 1$,

$p_4(x) = (x-\alpha^{17})(x-\alpha^{25})(x-\alpha^{23}) = x^3 + 2x^2 + 1$,

$q_1(x) = (x-\alpha^2)(x-\alpha^6)(x-\alpha^{18}) = x^3 + 2x^2 + x + 2$,

$q_2(x) = (x-\alpha^4)(x-\alpha^{12})(x-\alpha^{10}) = x^3 + x^2 + 2$,

$q_3(x) = (x-\alpha^8)(x-\alpha^{24})(x-\alpha^{20}) = x^3 + 2x^2 + 2x + 2$,

$q_4(x) = (x-\alpha^{16})(x-\alpha^{22})(x-\alpha^{14}) = x^3 + 2x + 2$

따라서 체 F_3 위의 3차 원시다항식은 $p_1(x)$, $p_2(x)$, $p_3(x)$, $p_4(x)$ 뿐이고 또 다항식 $x^{27} - x$ 는 체 F_3 위에서 다음과 같이 인수분해 된다.(참고문헌 [1])

$$x^{27} - x = x(x-1)(x-2)p_1(x)p_2(x)p_3(x)p_4(x)$$
$$q_1(x)q_2(x)q_3(x)q_4(x)$$

참고문헌

[1] 김응태, 박승안. “현대 암호학”. 경문사, 30(1), pp. 475-483, 2003.

[2] 양정모, “SEED암호에서 S-함수에 대한 고찰”, 한국정보보호학회 논문지, Vol.27, No.6, pp. 1295-1305, 2017.

[3] 양정모, “스트림암호에서 높은 비선형도의 상관면역함수의 설계와 그의 안전성 분석”, 한국정보보호학회 논문지, 제 17권 제 4호, pp. 89-95, 2007.

[4] 이민섭. “현대 암호학”. 경문사, 30(1), pp. 168-258, 2007.

[5] 이민섭, 신현용, 이준열 “이진수열의 비선형성과 Correlation Attack에 관한 연구”, 한국전자통신연구소, 1992.

[5] R.J. Anderson, “Solving a class of stream ciphers”, Criptologia, 14(3), 1990.

〔저자소개〕

양 정 모(Jeong-mo Yang)

1984년 동국대학교 사범대학 수학과 학사
1989년 동국대학교 대학원 수학과 이학석사
1997년 단국대학교 대학원 수학과 이학박사
1995년 3월~ 중부대학교 정보보호학과 교수
email : jmyang@joongbu.ac.kr