



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2022-0087601
(43) 공개일자 2022년06월27일

(51) 국제특허분류(Int. Cl.)
G06F 7/58 (2006.01)

(52) CPC특허분류
G06F 7/582 (2013.01)

(21) 출원번호 10-2020-0176946

(22) 출원일자 2020년12월17일

심사청구일자 2020년12월17일

(71) 출원인
인하대학교 산학협력단

인천광역시 미추홀구 인화로 100(용현동, 인하대학교)

(72) 발명자

정상태

인천광역시 연수구 송도문화로28번길 28 송도글로벌캠퍼스푸르지오, 104동 1704호

(74) 대리인

이은철, 이수찬

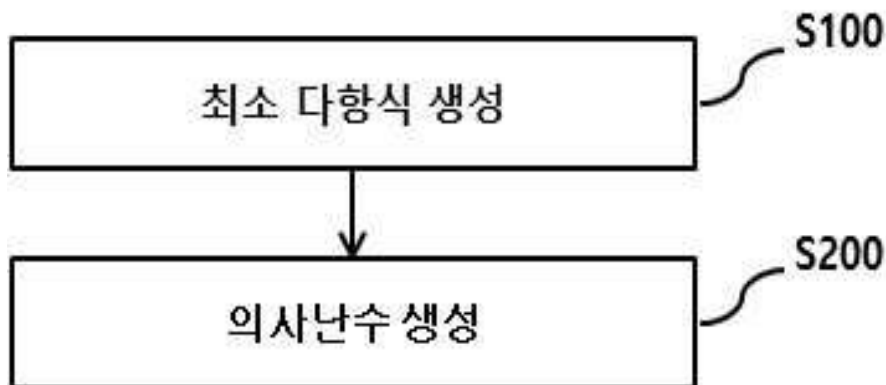
전체 청구항 수 : 총 4 항

(54) 발명의 명칭 p -진 정수환 위의 최소 다항식을 이용한 의사난수 생성 방법

(57) 요약

본 발명은 p -진 정수환 위의 최소 다항식을 이용한 의사난수 생성 방법에 관한 것이다. 본 발명의 실시예에 따르면, 임의의 소수 p 에 대한 p -진 정수환 위의 최소 다항식을 분류 및 생성함으로써 효율적으로 의사난수 생성 함수를 획득하고, 난수 분포가 균일한 의사 난수를 생성할 수 있는 이점이 있다.

대표도 - 도1



명세서

청구범위

청구항 1

의사난수를 생성하는 방법에 있어서,

다항식 $f(x) = a_0 + a_1x + \dots + a_dx^d \in \mathbb{Z}/p\mathbb{Z}[x]$ 에 대해 임의의 소수 p (2, 3 또는 5 이상의 소수)에 대한 최소 다항식을 생성하는 단계; 및

생성된 상기 최소 다항식에 기반하여 의사난수를 생성하는 단계를 포함하는 것을 특징으로 하는 p -진 정수환 위의 최소 다항식을 이용한 의사난수 생성 방법.

청구항 2

제1항에 있어서,

상기 최소 다항식 생성 단계는,

상기 소수 p 가 3이고 최소 다항식의 차수 d 가 1 이상인 경우에 상수 항에 대한 제한 없이 $[a_0, A_1, A_0, D_0, D_1, D_2] \bmod 3 = [\cdot, \cdot, \cdot, \cdot, \cdot, \cdot]$ 에 대해 다음의 조건 (i) ~ (viii) 중 어느 하나의 충족 여부에 따라 최소다항식을 생성하는 것을 특징으로 하는 p -진 정수환 위의 최소 다항식을 이용한 의사난수 생성 방법.

- (i) $[1, 1, 0, 1, 1, 1], A_0 + 6 \not\equiv 0 \pmod{9}, A_0 + 6 \not\equiv 6a_2 + 3 \sum_{j \geq 0} a_{6j+2} \pmod{9}$;
- (ii) $[1, 1, 0, 1, 2, 2], A_1 + a_0 + 4 \not\equiv 0 \pmod{9}, A_1 + a_0 + 4 \not\equiv 3a_2 + 3 \sum_{j \geq 0} a_{6j+5} \pmod{9}$;
- (iii) $[1, 1, 0, 2, 1, 2], A_1 + 2a_0 + 3 \not\equiv 0 \pmod{9}, A_1 + 2a_0 + 3 \not\equiv 6a_2 + 3 \sum_{j \geq 0} a_{6j+5} \pmod{9}$;
- (iv) $[1, 1, 0, 2, 2, 1], A_0 + 2a_0 + 4 \equiv 0 \pmod{9}, A_0 + 2a_0 + 4 \not\equiv 3a_2 + 3 \sum_{j \geq 0} a_{6j+2} \pmod{9}$;
- (v) $[2, 1, 0, 1, 1, 1], A_0 + 3 \not\equiv 0 \pmod{9}, A_0 + 3 \not\equiv 6a_2 + 3 \sum_{j \geq 0} a_{6j+2} \pmod{9}$;
- (vi) $[2, 1, 0, 1, 2, 2], A_1 + 2a_0 + 7 \not\equiv 0 \pmod{9}, A_1 + 2a_0 + 7 \not\equiv 6a_2 + 3 \sum_{j \geq 0} a_{6j+5} \pmod{9}$;
- (vii) $[2, 1, 0, 2, 1, 2], A_0 + 2a_0 + 5 \not\equiv 0 \pmod{9}, A_0 + 2a_0 + 5 \not\equiv 3a_2 + 3 \sum_{j \geq 0} a_{6j+2} \pmod{9}$; and
- (viii) $[2, 1, 0, 2, 2, 1], A_1 + a_0 + 6 \not\equiv 0 \pmod{9}, A_1 + a_0 + 6 \not\equiv 3a_2 + 3 \sum_{j \geq 0} a_{6j+5} \pmod{9}$.

청구항 3

제1항에 있어서,

상기 최소 다항식 생성 단계는,

상기 소수 p 가 5이상의 소수이고 최소 다항식의 차수 d 가 $2p-1$ 이하인 경우에 다음의 조건 (i), (ii) 및 (iii) 충족 여부에 따라 최소 다항식을 생성하는 것을 특징으로 하는 p -진 정수환 위의 최소 다항식을 이용한 의사난수 생성 방법.

- (i) f 는 전이 모듈로 p 이다.
- (ii) $(f^p)'(0) \equiv 1 \pmod{p}$; and

$$(iii) \quad f^p(0) \in pZ_p \setminus p^2Z_p.$$

청구항 4

제3항에 있어서,

상기 최소 다항식 생성 단계는,

상기 소수 p 가 5이상의 소수이고 최소 다항식의 차수 d 가 $2p$ 이상인 경우에 다음의 수식식과 조건 (i) 및 (i)를 이용하여 최소 다항식을 생성하는 것을 특징으로 하는 p -진 정수환 위의 최소 다항식을 이용한 의사난수 생성 방법.

$$f(x) = f_0(x) + pf_1(x),$$

이 때, (i) $f_0(x) = \sum_{i=0}^{2p-1} e_i x^i \in Z/pZ[x]$ 는 상기 $(f^p)'(0) \equiv 1 \pmod{p}$ 에 따라 결정,

$$(ii) \quad f_1(x) = \sum_{j=0}^{2p-1} z_j x^j + \frac{1}{p} \sum_{j=2p}^d a_j h_j(x),$$

의 다항식 $f_1(x)$ 는

$$l(z_0, \dots, z_d) = \frac{1}{p} f_0^p(0) + \frac{1}{f_0'(0)} z_0 + \sum_{i=1}^{p-1} w_i f_1(f_0^i(0)) \pmod{p},$$

$l(z_0, \dots, z_d)$ 선형 다항식의 0이 아닌 모듈로 p 를 충족.

발명의 설명

기술 분야

[0001] 본 발명은 p -진 정수환 위의 최소 다항식을 이용한 의사난수 생성 방법에 관한 것으로 더욱 구체적으로는 난수 분포가 균일한 의사 난수를 생성하는 p -진 정수환 위의 최소 다항식을 이용한 의사난수 생성 방법에 관한 것이다.

배경 기술

[0003] 난수는 특정한 배열 순서나 각 항간의 의존성이 없는 임의적인 수열을 말하는데, 이 난수를 컴퓨터에 발생시키면 어떤 알고리즘에 의해 생성되기 때문에 긴 주기를 갖게 된다. 이와 같이 진정한 의미로는 난수가 아니지만 사용상 난수로 간주해도 지장이 없는 난수를 의사 난수라고 한다.

[0004] 생성된 의사난수의 품질을 확보하기 위하여는 난수 분포가 치우치지 않는 균일성이 최대한 확보되어야 하고, 난수가 반복되는 주기가 최대한 긴 의사난수 생성 함수를 구하여야 하고, 난수 분포가 균일한 의사난수 생성 함수를 효율적으로 구할 수 있어야 한다.

[0005] p -진 정수환 $\mathbb{Z}_p$ 위의 동역학 시스템 또는 양의 표수의 대응체계는 컴퓨터 공학과 양자 역학, 암호학에서 상당한 이론적 가치를 가진다. 실용적인 응용의 한 예는 정수 계수를 가지는 다항식에 대해 주어진 양의 정수의 큰 사이클 모듈로로부터 의사 난수를 생성하는 것이다.

[0006] 중국인의 나머지 정리를 이용하여 이러한 작업은 $\mathbb{Z}_p$ 에서 임의의 소수 p 의 어떤 멍수에 대한 전체 길이 사이클 모듈로를 유도하는 최소 다항식을 찾아내는 것으로 축소할 수 있다.

[0007] 익히 알려진 바와 같이 $\mathbb{Z}_p$ 에서 다항식의 계수에 관한 의 최소 다항식의 완전한 설명은 더 어려운 작업이다. 왜냐하면 연관된 순열 다항식 모듈로 p 가 그 계수의 관점에서 특성화하기 어렵다고 알려져 있기 때문이다.

[0008] 종래에 $\mathbb{Z}_p$ 에서 $p = 2$ 에 대한 최소성 기준과 $p = 3$ 에 대한 최소성 기준이 제시되고 있으나 $p = 3$ 에 대한 최소성 기준을 새롭게 제시하고, $p \geq 5$ 에 대한 최소성 기준을 제시함으로써 최소 다항식을 임의의 소수 p 에 대한 그들의 계수 관점에서 특성화하여 정수 계수를 가지는 다항식에 대해 주어진 양의 정수의 큰 사이클 모듈로로부터 의사 난수를 생성하여야 할 필요가 있다.

선행기술문헌

특허문헌

[0010] (특허문헌 0001) 1. 한국 등록특허공보 제10-2185385호

발명의 내용

해결하려는 과제

[0011] 본 발명은 상기와 같은 문제를 해결하기 위한 것으로서 난수 분포가 균일한 의사난수 생성 함수로부터 의사난수를 생성할 수 있는 임의의 소수 p 에 대한 p -진 정수환 위의 최소 다항식을 이용한 의사난수 생성 방법을 제고하는데 그 목적이 있다.

과제의 해결 수단

[0013] 진술한 목적을 달성하기 위한 본 발명은 의사난수를 생성하는 방법에 있어서, 다항식 $f(x) = a_0 + a_1x + \dots + a_dx^d \in \mathbb{Z}/p\mathbb{Z}[x]$ 에 대해 임의의 소수 p (2, 3 또는 5 이상의 소수)에 대한 최소 다항식을 생성하는 단계; 및 생성된 상기 최소 다항식에 기반하여 의사난수를 생성하는 단계를 포함하는 것이다.

[0014] 바람직하게는, 상기 최소 다항식 생성 단계는, 상기 소수 p 가 3이고 최소 다항식의 차수 d 가 1 이상인 경우에 상수 항에 대한 제한 없이 $[a_0, A_1, A_0, D_0, D_1, D_2] \bmod 3 = [\cdot, \cdot, \cdot, \cdot, \cdot, \cdot]$ 에 대해 다음의 조건 (i) ~ (viii) 중 어느 하나의 충족 여부에 따라 최소다항식을 생성하는 것이다.

- (i) $[1, 1, 0, 1, 1, 1], A_0 + 6 \neq 0 \pmod{9}, A_0 + 6 \neq 6a_2 + 3 \sum_{j \geq 0} a_{6j+2} \pmod{9}$;
- (ii) $[1, 1, 0, 1, 2, 2], A_1 + a_0 + 4 \neq 0 \pmod{9}, A_1 + a_0 + 4 \neq 3a_2 + 3 \sum_{j \geq 0} a_{6j+5} \pmod{9}$;
- (iii) $[1, 1, 0, 2, 1, 2], A_1 + 2a_0 + 3 \neq 0 \pmod{9}, A_1 + 2a_0 + 3 \neq 6a_2 + 3 \sum_{j \geq 0} a_{6j+5} \pmod{9}$;
- (iv) $[1, 1, 0, 2, 2, 1], A_0 + 2a_0 + 4 \equiv 0 \pmod{9}, A_0 + 2a_0 + 4 \neq 3a_2 + 3 \sum_{j \geq 0} a_{6j+2} \pmod{9}$;
- (v) $[2, 1, 0, 1, 1, 1], A_0 + 3 \neq 0 \pmod{9}, A_0 + 3 \neq 6a_2 + 3 \sum_{j \geq 0} a_{6j+2} \pmod{9}$;
- (vi) $[2, 1, 0, 1, 2, 2], A_1 + 2a_0 + 7 \neq 0 \pmod{9}, A_1 + 2a_0 + 7 \neq 6a_2 + 3 \sum_{j \geq 0} a_{6j+5} \pmod{9}$;
- (vii) $[2, 1, 0, 2, 1, 2], A_0 + 2a_0 + 5 \neq 0 \pmod{9}, A_0 + 2a_0 + 5 \neq 3a_2 + 3 \sum_{j \geq 0} a_{6j+2} \pmod{9}$; and
- (viii) $[2, 1, 0, 2, 2, 1], A_1 + a_0 + 6 \neq 0 \pmod{9}, A_1 + a_0 + 6 \neq 3a_2 + 3 \sum_{j \geq 0} a_{6j+5} \pmod{9}$.

[0015]

[0016] 바람직하게는, 상기 최소 다항식 생성 단계는, 상기 소수 p 가 5이상의 소수이고 최소 다항식의 차수 d 가 $2p-1$ 이하인 경우에 다음의 조건 (i), (ii) 및 (iii) 충족 여부에 따라 최소 다항식을 생성하는 것이다.

[0017] (i) f 는 전이 모듈로 p 이다.

[0018] (ii) $(f^p)'(0) \equiv 1 \pmod{p}$; and

[0019] (iii) $f^p(0) \in pZ_p \setminus p^2Z_p$.

[0020] 바람직하게는, 상기 최소 다항식 생성 단계는, 상기 소수 p 가 5이상의 소수이고 최소 다항식의 차수 d 가 $2p$ 이 상인 경우에 다음의 수학적식과 조건 (i) 및 (ii)를 이용하여 최소 다항식을 생성하는 이다.

[0021]
$$f(x) = f_0(x) + pf_1(x),$$

[0022] 이 때, (i) $f_0(x) = \sum_{i=0}^{2p-1} e_i x^i \in Z/pZ[x]$ 는 상기 $(f^p)'(0) \equiv 1 \pmod{p}$ 에 따라 결정,

[0023] (ii) $f_1(x) = \sum_{j=0}^{2p-1} z_j x^j + \frac{1}{p} \sum_{j=2p}^d a_j h_j(x),$ 의 다항식 $f_1(x)$ 는

[0024]
$$l(z_0, \dots, z_d) = \frac{1}{p} f_0^p(0) + \frac{1}{f_0'(0)} z_0 + \sum_{i=1}^{p-1} w_i f_1(f_0^i(0)) \pmod{p},$$
 선형 다항식의 0이 아닌 모듈로 p 를 충족.

발명의 효과

[0025] 전술한 바와 같은 본 발명에 따르면, 임의의 소수 p 에 대한 p -진 정수환 위의 최소 다항식을 분류 및 생성함으로써 효율적으로 의사난수 생성 함수를 획득하고, 난수 분포가 균일한 의사 난수를 생성할 수 있는 이점이 있다.

도면의 간단한 설명

[0027] 도 1은 본 발명의 일 실시예에 따른 p -진 정수환 위의 최소 다항식을 이용한 의사난수 생성 방법의 흐름도이다.

발명을 실시하기 위한 구체적인 내용

[0028] 이상의 본 발명의 목적들, 다른 목적들, 특징들 및 이점들은 첨부된 도면과 관련된 이하의 바람직한 실시예들을 통해서 쉽게 이해될 것이다. 그러나 본 발명은 여기서 설명되는 실시예들에 한정되지 않고 다른 형태로 구체화될 수도 있다. 오히려, 여기서 소개되는 실시예들은 개시된 내용이 철저하고 완전해질 수 있도록 그리고 당업자에게 본 발명의 사상이 충분히 전달될 수 있도록 하기 위해 제공되는 것이다. 본 명세서에서, 어떤 구성요소가 다른 구성요소 상에 있다고 언급되는 경우에 그것은 다른 구성요소 상에 직접 형성될 수 있거나 또는 그들 사이에 제 3의 구성요소가 개재될 수도 있다는 것을 의미한다.

[0029] 어떤 엘리먼트, 구성요소, 장치, 또는 시스템이 프로그램 또는 소프트웨어로 이루어진 구성요소를 포함한다고 언급되는 경우, 명시적인 언급이 없더라도, 그 엘리먼트, 구성요소, 장치, 또는 시스템은 그 프로그램 또는 소프트웨어가 실행 또는 동작하는데 필요한 하드웨어(예를 들면, 메모리, CPU 등)나 다른 프로그램 또는 소프트웨어(예를 들면 운영체제나 하드웨어를 구동하는데 필요한 드라이버 등)를 포함하는 것으로 이해되어야 할 것이다.

[0030] 또한 어떤 엘리먼트(또는 구성요소)가 구현됨에 있어서 특별한 언급이 없다면, 그 엘리먼트(또는 구성요소)는 소프트웨어, 하드웨어, 또는 소프트웨어 및 하드웨어 어떤 형태로도 구현될 수 있는 것으로 이해되어야 할 것이다.

[0031] 본 명세서에서 사용된 용어는 실시예들을 설명하기 위한 것이며 본 발명을 제한하고자 하는 것은 아니다. 본 명

세서에서, 단수형은 문구에서 특별히 언급하지 않는 한 복수형도 포함한다. 명세서에서 사용되는 '포함한다 (comprises)' 및/또는 '포함하는(comprising)'은 언급된 구성요소는 하나 이상의 다른 구성요소의 존재 또는 추가를 배제하지 않는다.

[0032] 이하, 도면을 참조하여 본 발명을 상세히 설명하도록 한다. 아래의 특정 실시예들을 기술하는데 있어서, 여러 가지의 특징적인 내용들은 발명을 더 구체적으로 설명하고 이해를 돕기 위해 작성되었다. 하지만 본 발명을 이해할 수 있을 정도로 이 분야의 지식을 갖고 있는 독자는 이러한 여러 가지의 특징적인 내용들이 없어도 사용될 수 있다는 것을 인지할 수 있다. 어떤 경우에는, 발명을 기술하는 데 있어서 흔히 알려졌으면서 발명과 크게 관련 없는 부분들은 본 발명을 설명하는 데 있어 별 이유 없이 혼돈이 오는 것을 막기 위해 기술하지 않음을 미리 언급해 둔다.

[0033] 도 1을 참조하면, 본 발명에 따른 p -진 정수환 위의 최소 다항식을 이용한 의사난수 생성 방법은 의사난수를 생성하는 방법에 있어서, 최소 다항식 생성 단계(S100)과 의사난수 생성 단계(S200)을 포함한다.

[0034] S100 단계는 다항식 $f(x) = a_0 + a_1x + \dots + a_dx^d \in \mathbb{Z}/p\mathbb{Z}[x]$ 에 대해 임의의 소수 p (2, 3 또는 5 이상의 소수)에 대한 최소 다항식을 생성한다. S200 단계는 S100 단계에서 생성된 최소 다항식에 기반하여 의사난수를 생성한다.

[0035] 본 발명은 $\mathbb{Z}_p$ 에서 3보다 큰 어떤 소수 p 에 대하여 최소 다항식을 그들의 계수 관점에서 특성화하는 것을 보여준다. 이를 위해 최소 다항식은 두가지 사전 요구 사항을 만족한다는 것을 확인한다. 전체 길이 사이클을 유도하는 축소된(reduced) 다항식 모듈로 p 는 전이적이다. 그리고, 그것의 $0, \dots, p-1$ 에서 도함수의 곱은 1 모듈로 p 이다. 규정된 조건에 따라 이러한 두 가정을 만족하는 계수의 선택은 정확히 $(p-1)!(p-1)^{p-1}$ 가지 선택이 존재한다.

[0036] 본 발명의 실시예에 따라 제안된 방법은 모든 규정된 조건들이 완전히 발견되면 $\mathbb{Z}_p$ 에서의 모든 가능한 최소 다항식을 그들의 계수 관점에서 분류하는 것을 가능하게 한다. 그러므로 $\mathbb{Z}_p$ 에서 최소 다항식을 찾는 것이나 주어진 다항식 맵이 최소인지 결정하는 것은 완전히 답변될 수 있다.

[0037] $\mathbb{Z}_p$ 를 소수 p 에 대한 p -진 정수 환이라고 한다. $\mathbb{Q}_p$ 를 p -진수 환이라고 한다. $|\cdot|$ 를 $\mathbb{Q}_p$ 에서 (정규화된) 절대 값이라고 하고 $|x| = p^{-\text{ord}_p(x)}$ 와 같은 $\mathbb{Q}_p$ 에서 ord 덧셈 부치와 관련된다. $\mathbb{Z}_p$ 에서 1-립시츠 함수는 다음과 같이 정의된다.

[0038] 함수 $f: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ 는 모든 $x, y \in \mathbb{Z}_p$ 에 대해 $|f(x) - f(y)| \leq |x - y|$ 이면 1-립시츠 함수라고 한다. 전형적인 $\mathbb{Z}_p$ 에서 1-립시츠 함수의 예는 $\mathbb{Z}_p$ 에서 계수를 가지는 다항식과 β -함수의 클래스를 포함한다. 1-립시츠 함수는 다음과 같은 몇가지 동등한 진술문을 가진다.

[0040] (L1) $f(x) \equiv f(y) \pmod{p^n}$ 일 때는 어떤 정수 $n \geq 1$ 에 대해 언제나 $x \equiv y \pmod{p^n}$ 이다.

[0041] (L2) 모든 $x \in \mathbb{Z}_p$ 그리고 어떤 정수 $n \geq 1$ 에 대해

[0042] $f(x + p^n \mathbb{Z}_p) \subset f(x) + p^n \mathbb{Z}_p$ 이다.

[0044] (L3) 모든 $x, y \in \mathbb{Z}_p$ 에 대해 $|f(x + y) - f(x)| \leq |y|$ 이다.

[0046] 여기에서 (L1)은 1-립시츠 함수 $f: Z_p \rightarrow Z_p$ 가 아래와 같은 몫의 환에 의해 정의 되는 축소된 함수의 시퀀스 $f/n (n \geq 1)$ 를 유도한다는 것을 나타낸다.

$$[0048] \quad f/n : Z_p/p^n Z_p \rightarrow Z_p/p^n Z_p, x + p^n Z_p \mapsto f(x) + p^n Z_p$$

[0050] Z_p 에서 p진 동역학 시스템은 트리플 (Z_p, μ_p, f) 로서 이해된다. $f: Z_p \rightarrow Z_p$ 가 축소가능 함수이고, μ_p 는 Z_p 에서 자연 확률 측도이고, $\mu_p(Z_p) = 1$ 로 정규화된다.

[0051] 단원소의 μ_p -축소가능 집합들은 p^{-k} 반지름의 p진 구들이다. 이들은 $a \in Z_p$ 이고 정수 $k \geq 0$ 에 대해 $a + p^k Z_p$, 형태의 집합이다. 이러한 구의 측도는 그것의 반지름으로서 정의된다(i.e., $\mu_p(a + p^k Z_p) = 1/p^k$).

[0053] 정의 2.2.

[0054] (Z_p, μ_p, f) 를 Z_p 에 p진 동역학 시스템이라고 하자. 함수 $f: Z_p \rightarrow Z_p$ 는 만약 각 가측 부분집합 $M \subset Z_p$ 에 대해 $\mu_p(f^{-1}(M)) = \mu_p(M)$ 이면 측도보존 된다고 한다.

[0056] 측도 보존 함수 $f: Z_p \rightarrow Z_p$ 는 그것이 적절한 불변 부분집합(i.e., $\mu_p(M) = 1$ 또는 $\mu_p(M) = 0$ 둘 다 $f^{-1}(M) = M$ 과 같은 어떠한 가측 부분집합 $M \subset Z_p$ 을 보류한다)을 가지지 않는 경우 에르고딕하다고 한다.

[0058] 정의 2.3

[0059] 연속함수 $f: Z_p \rightarrow Z_p$ 는 모든 $x \in Z_p$ 에 대해 x 에서 f의 전방궤도가 Z_p 에서 밀집하는 경우에 최소라고 한다.

[0061] S 를 $N \geq 1$ 원소의 유한 집합이라고 하고 f를 S 에서의 셀프-사상이라고 하고, f^n 을 f^0 가 S 에서 항등 사상이 라고 할 때 f의 n -th 반복 이라고 정의한다.

[0063] 정의 2.4.

[0064] 함수 $f: S \rightarrow S$ 는 S가 f의 단일 사이클을 형성한다면 S 에서 전이적이거나 최소이다. 즉, 어떤 고정된 초점, $x_0 \in S$ 에 대해 $\{x_0, f(x_0), \dots, f^{N-1}(x_0)\} = S$ 이다.

[0066] Z_p 에서 1-립시츠 함수는 측도 보존에 대해 몇 가지 동등한 진술문을 가진다.

[0068] 명제 2.5

[0069] $f: Z_p \rightarrow Z_p$ 를 1-립시츠 함수라고 할 때, 다음 진술문은 동등하다.

[0071] (1) f 는 전사함수이다.

[0072] (2) f 는 등거리 사상이다.

[0073] (3) f/n 은 모든 정수 $n \geq 1$ 에 대해 전단사 함수이다.

[0074] (4) f 는 측도 보존이다.

[0076] $Z_p[x]$ 의 다항식에 대한 더 단순한 측도 보존 특징이 알려져 있다.

[0078] 명제 2.6

[0079] (1) f/n 은 모든 정수 $n \geq 1$ 에 대해 전단사 함수이다.

[0080] (2) $f/2$ 는 전단사 함수이다.

[0081] (3) $f/1$ 은 전단사 함수이고, $f'(x) \equiv 0 \pmod{p}$ 는 Z_p 에서 해를 가지지 않는다.

[0083] 에르고딕성 또는 최소성에 관해서 우리는 다음 동등한 진술문을 얻을 수 있다.

[0085] 명제 2.7

[0086] $f: Z_p \rightarrow Z_p$ 를 측도 보존 1-립시츠 함수라고 할 때, 다음 진술문은 동등하다.

[0088] (1) f 는 최소이다.

[0089] (2) f 는 에르고딕이다.

[0090] (3) f/n 은 모든 $n \geq 1$ 정수에 대해 $Z_p/p^n Z_p$ 에서 전이함수이다.

[0091] (4) f 는 Z_p 에서 $t(x) = x + 1$ 함수와 켄레이다.

[0092] (5) f 는 특이하게 에르고딕이다. (i.e., 오직 하나의 에르고딕 측도가 있다)

[0094] 명제 2.8.

[0095] $f: Z_p \rightarrow Z_p$ 를 $Z_p[x]$ 에서 $(Z_p/p^n Z_p, f/n)$ 가 $n \geq 1$ 에 대해 최소임을 만족하는 다항식이라고 한다. 그러면 다음이 동등하다.

[0097] (1) $(Z_p/p^{n+1} Z_p, f/n+1)$ 는 최소이다.

[0098] (2) 모든 $x \in Z_p$ 에 대해 $f^{p^n}(x) - x \notin p^{n+1} Z_p$ 와 $(f^{p^n})'(x) \in 1 + p Z_p$ 를 가진다. 그리고,

[0099] (3) $f^{p^n}(x) - x \notin p^{n+1}Z_p$ 와 $(f^{p^n})'(x) \in 1 + pZ_p$ 과 같은 $x \in Z_p$ 가 존재한다.

[0101] **명제 2.9.**

[0102] 한 다항식, $f \in Z_p[x]$ 는 오직 p 가 2 또는 3이면 $\mu = 3$ 이고, $p \geq 5$ 이면 $\mu = 2$ 에서 $(Z_p/p^\mu Z_p, f/n)$ 가 최소일 때 최소이다.

[0104] 소수 p 에 대해 다음과 같이 설정한다.

[0106]
$$\mu := \mu(p) = \begin{cases} 3 & \text{if } p \in 2, 3; \\ 2 & \text{if } p \geq 5, \end{cases}$$

[0108] 그리고 다음과 같이 설정한다.

[0109]
$$\delta(x) := \delta_p(x) = \begin{cases} \begin{pmatrix} x \\ 2 \end{pmatrix} & \text{if } p \in 2, 3; \\ \begin{pmatrix} x \\ 2p \end{pmatrix} & \text{if } p \geq 5. \end{cases} \quad (1)$$

[0111] Z_p 위 다항식에 대한 다른 최소성 기준의 주요 결과를 진술하기 위하여, $Z/p^\mu Z$ 에서의 계수와 함께 차수가 $\deg(\delta)$ 보다 작은 모든 비동등 최소 다항식의 집합 $R(p^\mu)$ 를 정의한다. 평소처럼, $R(p^\mu)$ 의 모든 원소는 $Z/p^\mu Z := \{0, \dots, p^\mu - 1\}$ 에서의 정수 계수를 가지는 다항식이 될 수 있는 것으로 이해된다.

[0113] **정리 3.1.**

[0114] $f \in Z_p[x]$ 를 양의 차수의 다항식이라고 하면,

[0115] (1) f 는 오직 $f(x)$ 모듈로 $\delta(x)$ 의 축소가 $R(p^\mu)$ 에서 최소일 때 최소이다.

[0116] (2) $R(p^\mu)$ 의 원소 수는 다음에 따라 정해진다.

[0118]
$$\#R(p^\mu) = \begin{cases} 16 & \text{if } p = 2 \\ 2^5 3^{10} & \text{if } p = 3 \\ (p-1)!(p-1)^p p^{p-1} & \text{if } p \geq 5 \end{cases}$$

[0120] 이에 대한 증명은 다음과 같다.

[0121] (1) $r(x)$ 가 f 를 δ 로 나눈 나머지라고 한다. 그러면,

[0122] $f(x) = q(x) \delta(x) + r(x)$ 이고, 이 때, $q, r \in \mathbb{Z}_p[x]$ 이고, $r(x)$ 의 차수가 $\deg(\delta)$ 보다 작다.

[0124] 명제 2.9.에 의해 합동이 성립한다는 전제에서 그 결과는 다음과 같다.

[0125]
$$f(x) \equiv r(x) \pmod{p^\mu}$$

[0126] $q(x)$ 의 모든 계수는 p^μ 에 의해 나누어지는 것을 보이고 이로 인해 주장된 결과를 보이게 된다. 뉴턴 보간법 공식에 의하거나 말러의 p진 변수의 연속 함수에 대한 보간 순열에 의하면, 어떤 다항식, $f \in \mathbb{Z}_p[x]$ 는 이항 계수 다항식 측면에서 형태의 유한 함으로 고유하게 표현된다.

[0128]
$$f(x) = \sum_{n=0}^d a_n \binom{x}{n}$$

[0129]
$$= \sum_{n=0}^{\deg(\delta)-1} a_n \binom{x}{n} + \sum_{n=\deg(\delta)}^d a_n \binom{x}{n}, \quad (2)$$

[0131] 이 때, 모든 $a_n \in \mathbb{Z}_p$ 이고, d 는 $\deg(\delta)$ 에 관해 더 크거나 같은 것으로 가정된다. 왜냐하면 $\mathbb{Z}_p[x]$ 에서의 모든 다항식은 명제 3.58로부터 해석적 함수이고, 모든 $a_n/n!$ 는 p진 정수에 포함되고 있다. 이리하여, $g(x) \in \mathbb{Z}_p[x]$ 인 모든 $n \geq \deg(\delta)$, $a_n \binom{x}{n} = g(x) \delta(x)$ 에 대해 모든 계수가 p^μ 로 나누어지는지 확인된다. 실제로, 모든 소수 p에 대해 다음과 같이 통합된 방식으로 이를 수행한다.

[0133] $n \geq \deg(\delta)$ 에 대해

[0134]
$$a_n \binom{x}{n} \Big|_{n=\deg(\delta)} = \frac{a_n}{n!} (x - \deg(\delta)) \cdots (x - n + 1) \delta(x)$$
 를 얻는다.

[0135] $\deg(\delta)!$ 이 p^μ 에 의해 나누어지기 때문에, (2)의 우변의 두 번째 합에 있는 모든 항에서 공통 인자 δ 를 인수 분해하면 (2)의 두 번째 합이

[0136] $q(x) \delta(x)$ 형식의 곱으로 축소되고, $q(x) \in \mathbb{Z}_p[x]$ 의 모든 계수는 p^μ 로 나눌 수 있고, (2)의 첫 번째 합은 δ 로 나눈 f 의 나머지 $r(x)$ 이다. 이로서 증명이 완성된다.

[0138] 정리 3.1.의 (2)부분은 이미 알려져 있다.

[0140] 우리는 $f \in \mathbb{Z}_p[x]$ 의 다항식은 어떤 $\alpha \in \mathbb{Z}_p$ 에 대해 $f(\alpha) \equiv 0 \pmod{m}$ 이면 양의 정수 m에 대해 항등 모듈로 m이라고 한다. 정리 3.1의 증명으로부터 다항식 q는 항등 모듈로 p^μ 인 것을 관찰 할 수 있다.

[0142] **따름 정리 3.3.**

[0143] 다항식, $f \in \mathbb{Z}_p[x]$ 는 오직 $f(x)$ 가 다음의 형식으로 표현가능할 때에만 최소이다.

$$[0145] \quad f(x) = r(x) + t(x)$$

[0146] 이 때, $r(x) \in R(p^u)$ 이고, $t(x)$ 는 항등 모듈로 p^u 이다.

[0148] $p=2$ 에 대해 $\mathbb{Z}_p[x]$ 에서의 다항식의 최소성 기준은 그것의 계수 측면에서 잘 알려져 있다. 종래 각각 $\mathbb{Z}_2[x]$ 에서 보편 다항식의 최소 기준이 제시된 바 있다. 본 발명의 실시예는 종래 최소 기준 결과의 대안적인 증명을 제시한다. 이를 위해 먼저 최대 3차의 다항식에 대한 최소 조건을 되새긴다.

[0150] **따름정리 4.1.**

[0151] 다항식 $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 \in \mathbb{Z}_2[x]$ 는 오직 다음 관계식이 만족되는 시스템일 때에만 최소이다.

$$[0152] \quad a_0 \equiv 1 \pmod{2} ;$$

$$[0153] \quad a_2 \equiv 0 \pmod{2} ;$$

$$[0154] \quad a_3 \equiv 0 \pmod{4} ; \text{ and}$$

$$[0155] \quad a_1 + a_2 \equiv 1 \pmod{4}$$

[0157] 이에 관한 원 증명은 M. V. Larin, Transitive polynomial transformations of residue class rings, Discrete Math. and Applications(2002)에서 주어지고 있다. 완전성을 위해 우리는 대안적인 증명을 제시하기 위한 다음의 몇가지 인자를 따른다 F. Durand and F. Paccaut, Minimal polynomial dynamics on the set of 3-adic intergers, Bull.Lond. Math.Soc. 41 (2), (2009)에 따르면 f 는 오직 다음 조건을 만족시킬 때 최소이다.

$$[0159] \quad (M1) \quad f(0) \equiv 1 \pmod{2} \text{ and } f(1) \equiv 0 \pmod{2} ;$$

$$[0160] \quad (M2) \quad (f^2)'(0) \equiv 1 \pmod{2} ;$$

$$[0161] \quad (M3) \quad (f^2)(0) \in 2\mathbb{Z}_2 \setminus 4\mathbb{Z}_2 ; \text{ and}$$

$$[0162] \quad (M4) \quad (f^4)(0) \in 4\mathbb{Z}_2 \setminus 8\mathbb{Z}_2 .$$

[0164] 간단한 계산을 통해, (M1)과 (M2)가 다음 관계식과 동등하다는 것을 쉽게 보일 수 있다.

$$[0166] \quad a_0 \equiv 1 \pmod{2}; a_1 \equiv 1 \pmod{2}; a_2 \equiv 0 \pmod{2}; a_3 \equiv 0 \pmod{2}$$

[0168] 둘째로 $f^2(0) \equiv 1 + a_1 + a_2 + a_3 \pmod{4}$ 이기 때문에 (M3)는 $a_1 + a_2 + a_3 \equiv 1 \pmod{4}$ 와 동등하다. 최종적으로 F. Durand and F. Paccaut, Minimal polynomial dynamics on the set of 3-adic intergers, Bull.Lond. Math.Soc. 41 (2), (2009)의 증명으로부터 (M4)는 $(f^2)'(0) + (f^2)''(0) \equiv 1 \pmod{4}$ 와 동등하고, 또한 $2a_2 + a_1(a_1 + a_3) \equiv 1 \pmod{4}$ 와도 동등하다. 모든 관계를 종합하면 원하는 최종결과를 얻을 수 있다. 이제 다음과 같이 $\#R(p^u) = 16$ 임을 보여줌으로써 $p=2$ 일 때 케이스에 대한 정리 3.1. (2)부분의 증명을 마친다.

[0170] **따름정리 4.2.**

[0171] 다항식 $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 \in \mathbb{Z}_2[x]$ 는 오직 링 $\mathbb{Z}/8\mathbb{Z}$ 에서 다음 16개의 다항식 중 하나에 의해 유도된 맵, $x \mapsto f(x) \pmod{8}$, $x \in \{0, 1, \dots, 7\}$ 과 일치할 때 최소이다.

[0174]

$x + 1$	$5x + 1$	$2x^2 + 3x + 1$	$2x^2 + 7x + 1$
$x + 3$	$5x + 3$	$2x^2 + 3x + 3$	$2x^2 + 7x + 3$
$x + 5$	$5x + 5$	$2x^2 + 3x + 5$	$2x^2 + 7x + 5$
$x + 7$	$5x + 7$	$2x^2 + 3x + 7$	$2x^2 + 7x + 7$

[0176] 증명. $R(p^u)$ 에서 모든 구별되는 최소 다항식을 나열하기 위하여 따름정리 4.1을 이용한다. 따름정리 4.1에 따라 먼저 2 미만 차수의 $a_i \in \mathbb{Z}/8\mathbb{Z}$ 인 최소 다항식 $f(x) = a_0 + a_1x + a_2x^2$ 을 다룬다. $z_i \in \mathbb{Z}/4\mathbb{Z}$ 이고 $a_0 = 1 + 2z_0$, $a_1 = 1 + 2z_1$, $a_2 = 2z_2$ 라고 한다. 이리하여 $z_1 + z_2 \equiv 0 \pmod{2}$ 조건에서 최소 다항식 $f(x) = 1 + x + 2(z_0 + z_1x + z_2x^2)$ 을 얻을 수 있다.

[0178] 만약 집합 $S = \{(z_0, z_1, z_2) \in (\mathbb{Z}/4\mathbb{Z})^3 \mid z_1 + z_2 \equiv 0 \pmod{2}\}$ 을 넣는다면 S는 32개 원소를 가지고, S의 각 원소는 최소 다항식을 유도한다. 그들 중 일부는 모듈로 8과 동등할 수 있다. 따라서, 이러한 다항식을 유도하는 S의 원소를 세어 동등하지 않은 최소 다항식을 찾아볼 수 있다. 모듈로 8 최소 다항식과 동등한 것을 유도하는 S에서 두 원소, (z_0, z_1, z_2) 와 (z'_0, z'_1, z'_2) 를 가정한다. f 의 표현으로부터 우리는 다음과 같은 관계식을 파생할 수 있다.

[0180]
$$z_0 + z_1x + z_2x^2 \equiv z'_0 + z'_1x + z'_2x^2 \pmod{4}$$

[0181] 이는 다음 관계식과 동등하다.

[0182]
$$z_0 = z'_0; z_1 \equiv z'_1 \pmod{2}; \text{ and } z_2 \equiv z'_2 \pmod{2}$$

[0184] 따라서, S에서 오직 8개 원소가 이러한 관계식들을 위반한다. 따라서, 진술문에서 행렬 배열의 첫 번째 및 세 번째 열을 구성하는 정확히 8개의 동등하지 않은 최소 다항식이 존재한다. 두 번째, 우리는 3차의 최소 다항식 $f(x) = a_0 + a_1x + a_2x^2 + 4x^3$ 으로 전환할 수 있고, 이는 $f(x) \equiv a_0 + (a_1 + 4)x + a_2x^2 \pmod{8}$ 과 동등

하다.

[0185] 왜냐하면 $4x^3 \equiv 4x \pmod{8}$ 이기 때문이다.

[0186] 따라서, f 는 a_1 이 a_1+4 에 의해 대체된 첫 번째 경우로 축소된다. 동등하게 z_1 은 z_1+2 에 의해 대체된다. 이러한 변화에서 f 에 대한 최소 조건과 S의 증가 관계는 첫 번째 경우와 마찬가지로 불변이다. 따라서 진술문에서 행렬 배열의 두 번째 및 네 번째 열을 구성하는 정확히 8개의 동등하지 않은 최소 다항식이 있다. 두 케이스를 결합하면 16개의 결과가 나온다.

[0187] 다항식에 상수 항이 1이라는 가정을 제거하기 위해 종래의 최소 기준을 다시 검토한다. 이를 마치기 위해 $\mathbb{Z}_2[x]$ 에서 $d \geq 1$ 차수의 다항식 $f(x) = a_0 + a_1x + \dots + a_dx^d$ 에 대해 다음과 같이 정한다.

$$A_0 = \sum_{0 < i \equiv 0 \pmod{2}} a_i; A_1 = \sum_{i \equiv 1 \pmod{2}} a_i$$

[0191] 정리 4.3.

[0192] 한 다항식, $f(x) = a_0 + a_1x + \dots + a_dx^d \in \mathbb{Z}_2[x]$ 는 오직 다음 관계식을 만족하는 시스템일 때 최소이다.

$$[0194] a_0 \equiv 1 \pmod{2};$$

$$[0195] a_1 \equiv 1 \pmod{2};$$

$$[0196] A_1 \equiv 1 \pmod{2};$$

$$[0197] A_0 \equiv 1 \pmod{4}; \text{ and}$$

$$[0198] 2^{a_2 + a_1} A_1 \equiv 1 \pmod{4}$$

[0200] 증명. $a_0 = f(0) = 1$ 이라는 가정을 제외하고 F. Durand and F. Paccout, Minimal polynomial dynamics on the set of 3-adic intergers, Bull.Lond. Math.Soc. 41 (2), (2009)의 증명과 동일하다.

[0201] 위와 같이 증명이 동일하기 때문에 $f^2(0)$ 모듈로 4를 계산하여 a_0 를 포함하는 네 번째 조건도 a_0 에 대한 제한 없이 변경되지 않는 점을 지적한다. 테일러 정리를 이용하여 $f'(1) \equiv A_1 \equiv 1 \pmod{2}$ 이기 때문에 다음을 얻을 수 있다.

$$[0203] f^2(0) = f(a_0) = f(1+2z_0) \equiv f(1) + 2^{z_0} f'(1) \equiv 2^{a_0-1} A_0 + A_1 \pmod{4}$$

[0205] 따라서, (M3)에 의해서, $f^2(0) \equiv 2 \pmod{4}$ 는 $A_0 + A_1 \equiv 1 \pmod{4}$ 와 같은 $a_0 \equiv 1 \pmod{2}$ 와 동등하다는 것을 쉽게 알 수 있다. 완전성을 위해 따름정리 4.1에서 따르는 결과를 간단한 축소 절차를 통해 설명한다.

[0207] 따름정리 4.4.

[0208] 한 다항식 $f(x) = a_0 + a_1x + \dots + a_dx^d \in \mathbb{Z}_2[x]$ 는 오직 다음 관계식을 만족하는 시스템일 때에만 최소이다.

[0210] $a_0 \equiv 1 \pmod{2};$

[0211] $a_1 \equiv 1 \pmod{2};$

[0212] $A_1 - a_1 \equiv 2^{a_2} \pmod{4};$ and

[0213] $A_0 \equiv a_1 + 2^{a_2} - 1 \pmod{4}.$

[0215] 증명. 정리 4.3의 관계식은 위 진술문의 관계식과 동등하다. M. V. Larin, Transitive polynomial transformations of residue class rings, Discrete Math. and Applications(2002)의 명제 21에서 원 증명을 확인할 수 있다.

[0216] $p=3$ 케이스에 대해 F. Durand and F. Paccaut, Minimal polynomial dynamics on the set of 3-adic intergers, Bull.Lond. Math.Soc. 41 (2), (2009)는 다항식 $f \in \mathbb{Z}_3[x]$ 에 대한 완전한 최소성 기준을 그 계수의 측면에서 $f(0) \equiv 1$ 이라는 가정 아래 제시하고 있다. 그들의 주요 특성은 다음에 기초한다.

[0218] 명제 5.1.

[0219] $f \in \mathbb{Z}_3[x]$ 을 양의 차수의 다항식이라고 한다. 그러면 f 는 오직 다음 조건을 만족할 때 최소이다.

[0221] (M1) $f/1$ 은 이행적이다. 즉, f 는 이행적인 모듈로 3이다.

[0222] (M2) $(f^3)'(0) \equiv 1 \pmod{3}$ 즉, $(f)'(f^2(0))f'(f(0))f'(0) \equiv 1 \pmod{3};$

[0223] (M3) $f^3(0) \in 3\mathbb{Z}_3 \setminus 9\mathbb{Z}_3$; and

[0224] (M4) $3(f^3)''(0) - 2f^3(0) \not\equiv 0 \pmod{9}$

[0226] 일반 다항식은 상수 항의 더 높은 거듭 제곱을 포함하는 다항식의 최소 기준을 제공하기 위해 켈레 동형을 이용한다. 본 발명은 다른 관점에서 F. Durand and F. Paccaut, Minimal polynomial dynamics on the set of 3-adic intergers, Bull.Lond. Math.Soc. 41 (2), (2009)의 기준을 다시 검토하고, 상수 항에 대한 제한없이 계수 측면에서 다항식 $f \in \mathbb{Z}_3[x]$ 의 완전한 최소 기준을 제공한다.

[0227] 이를 적절하게 설명하기 위해, 차수 $d \geq 1$ 인 다항식 $f(x) = a_0 + a_1x + \dots + a_dx^d \in \mathbb{Z}_3[x]$ 의 계수와 관련된 다음 상수를 설정한다.

[0229] $a_0 = a_0 ; \sum_{i \in 1+2\mathbb{Z}} a_i = A_1 ; \sum_{0 < i \in 2\mathbb{Z}} a_i = A_0 ;$

$$[0230] \quad a_1 = D_0 ; \quad \sum_{i=1}^d i a_i = D_1 \quad ; \text{ and } \quad \sum_{i=1}^d i a_i 2^{i-1} = D_2 . \quad (3)$$

[0233] 정리 5.2.

[0234] 차수 $d \geq 1$ 인 다항식, $f(x) = a_0 + a_1 x + \dots + a_d x^d \in \mathbb{Z}_3[x]$ 은 오직 f 가 (i)-(viii) 조건 중의 하나를 만족할 때 최소이다.

[0235] 다음 세팅에서 $[a_0, A_1, A_0, D_0, D_1, D_2] \bmod 3 = [\cdot, \cdot, \cdot, \cdot, \cdot, \cdot]$,

- (i) $[1, 1, 0, 1, 1, 1], A_0 + 6 \not\equiv 0 \pmod{9}, A_0 + 6 \not\equiv 6a_2 + 3 \sum_{j \geq 0} a_{6j+2} \pmod{9}$;
- (ii) $[1, 1, 0, 1, 2, 2], A_1 + a_0 + 4 \not\equiv 0 \pmod{9}, A_1 + a_0 + 4 \not\equiv 3a_2 + 3 \sum_{j \geq 0} a_{6j+5} \pmod{9}$;
- (iii) $[1, 1, 0, 2, 1, 2], A_1 + 2a_0 + 3 \not\equiv 0 \pmod{9}, A_1 + 2a_0 + 3 \not\equiv 6a_2 + 3 \sum_{j \geq 0} a_{6j+5} \pmod{9}$;
- (iv) $[1, 1, 0, 2, 2, 1], A_0 + 2a_0 + 4 \equiv 0 \pmod{9}, A_0 + 2a_0 + 4 \not\equiv 3a_2 + 3 \sum_{j \geq 0} a_{6j+2} \pmod{9}$;
- (v) $[2, 1, 0, 1, 1, 1], A_0 + 3 \not\equiv 0 \pmod{9}, A_0 + 3 \not\equiv 6a_2 + 3 \sum_{j \geq 0} a_{6j+2} \pmod{9}$;
- (vi) $[2, 1, 0, 1, 2, 2], A_1 + 2a_0 + 7 \not\equiv 0 \pmod{9}, A_1 + 2a_0 + 7 \not\equiv 6a_2 + 3 \sum_{j \geq 0} a_{6j+5} \pmod{9}$;
- (vii) $[2, 1, 0, 2, 1, 2], A_0 + 2a_0 + 5 \not\equiv 0 \pmod{9}, A_0 + 2a_0 + 5 \not\equiv 3a_2 + 3 \sum_{j \geq 0} a_{6j+2} \pmod{9}$; and
- (viii) $[2, 1, 0, 2, 2, 1], A_1 + a_0 + 6 \not\equiv 0 \pmod{9}, A_1 + a_0 + 6 \not\equiv 3a_2 + 3 \sum_{j \geq 0} a_{6j+5} \pmod{9}$.

[0237]

[0238] 정리 5.2를 증명하기 위해 명제 5.1.을 이용한다.

[0239] 증명. 이 증명에 대한 핵심 아이디어는 주어진 상수 열 벡터 $[a_0, A_1, A_0, D_0, D_1, D_2]^t \bmod 3$ 에 대해 변수 $a_0 \dots a_d$ 의 선형 시스템 모듈로 3의 방정식을 보는 것이 필요하다. 여기서 t는 행렬의 전치를 나타낸다.

[0240] 그 다음 규정된 벡터 $[a_0, A_1, A_0, D_0, D_1, D_2] \bmod 3$ 을 갖는 다항식 f 의 최소성에 대해 필요 충분 조건을 찾는다.

[0241] (M1)과 (M2)가 모두 충족되는지 확인하기 위해 다음 Type I, Type II를 구성하는 가능한 8개의 행 벡터 $[a_0, A_1, A_0, D_0, D_1, D_2] \bmod 3$ 의 집합을 모두 나열한다.

Type I : $[1, 1, 0, 1, 1, 1], [1, 1, 0, 1, 2, 2], [1, 1, 0, 2, 1, 2], [1, 1, 0, 2, 2, 1]$;
Type II : $[2, 1, 0, 1, 1, 1], [2, 1, 0, 1, 2, 2], [2, 1, 0, 2, 1, 2], [2, 1, 0, 2, 2, 1]$.

[0243]

[0245] f 모듈로 3의 전이성은 Type I, Type II를 유도하고, 전자는 $f(0) \equiv 1 \pmod{3}$ 이고, 후자는 $f(0) \equiv 2 \pmod{3}$ 이다. 각 유형에 대해 (M2)의 $D_0 D_1 D_2 \equiv 1 \pmod{3}$ 을 충족하는 $[D_0, D_1, D_2] \bmod 3$ 에 대해 정확히 4개의 경우가 있다. 전체적으로 상수 벡터 $[a_0, A_1, A_0, D_0, D_1, D_2] \bmod 3$ 에 대한 8가지 선택사항이 있다. 따라서 Type 1, 2 순서로 나타나는 8개의 모든 상수 벡터 $[a_0, A_1, A_0, D_0, D_1, D_2] \bmod 3$ 에 대해 선형 시스템에 대한 모든 솔루션 $[a_0, \dots, a_d] \bmod 3$ 를 동시에 결정할 수 있다. 단순화를 위해, 선형 시스템 모듈로 3의 계

수 행렬에는 6-11번째 열 벡터가 주기적으로 나타나는 주기적 부분 행렬이 있기 때문에 f 의 차수가 6^k 라고 가정할 수 있다.

$$\left(\begin{array}{cccccccccccccccc|cccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdot & \cdots & \cdot & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & \cdot & \cdots & \cdot & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & \cdot & \cdots & \cdot & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdot & \cdots & \cdot & 1 & 1 & 2 & 2 & 1 & 1 & 2 & 2 \\ 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & \cdot & \cdots & \cdot & 1 & 2 & 1 & 2 & 1 & 2 & 1 & 2 \\ 0 & 1 & 1 & 0 & 2 & 2 & 0 & 1 & 1 & 0 & 2 & 2 & 0 & \cdot & \cdots & \cdot & 1 & 2 & 2 & 1 & 1 & 2 & 2 & 1 \end{array} \right)$$

[0247]

[0249]

위 선형 시스템의 증강 계수 행렬의 감소된 행 사다리꼴 형태는 동시에 다음과 같이 주어진다.

$$\left(\begin{array}{cccccccccccccccc|cccccccc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdot & \cdots & \cdot & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \cdot & \cdots & \cdot & 1 & 1 & 2 & 2 & 1 & 1 & 2 & 2 \\ 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & 0 & \cdot & \cdots & \cdot & 0 & 0 & 1 & 2 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 2 & 0 & 1 & 0 & 0 & 0 & \cdot & \cdots & \cdot & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & \cdot & \cdots & \cdot & 0 & 0 & 2 & 1 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 2 & 0 & 0 & 0 & 1 & 0 & \cdot & \cdots & \cdot & 0 & 2 & 2 & 2 & 0 & 2 & 2 & 2 \end{array} \right)$$

[0250]

(4)

[0252]

축소된 형태 (4)는 점선 부분 행렬에 이 순서로 나타나는 $C_7, \dots, C_{12}$ 로 표시되는 7번째에서 12번째 열의 열 벡터와 관련하여 특정 패턴을 갖는 것을 관찰할 수 있다. f 가 6^k 차수이기 때문에 C_7 벡터는 k 번 나타나고, 나머지 5열 벡터는 $k-1$ 번 나타난다. 축약형은 C_7 로 끝이 난다. 선택한 선형 시스템의 파라메트릭 표현은 다음 관계식으로 제공된다 :

$$\begin{aligned} a_0 &= r_0 + 3z_0; \\ a_1 &= r_1 + 3z_1; \\ a_2 &= r_2 + 3z_2 + (a_6 + a_{12} + \cdots + a_{6k}) + 2(a_8 + a_{14} + \cdots + a_{6k-4}); \\ a_3 &= r_3 + 3z_3 + (a_7 + a_{13} + \cdots + a_{6k-5}) + 2(a_9 + a_{15} + \cdots + a_{6k-3}); \\ a_4 &= r_4 + 3z_4 + (a_6 + a_{12} + \cdots + a_{6k}) + 2(a_{10} + a_{16} + \cdots + a_{6k-2}); \\ a_5 &= r_5 + 3z_5 + (a_7 + a_{13} + \cdots + a_{6k-5}) + 2(a_{11} + a_{17} + \cdots + a_{6k-1}), \end{aligned}$$

[0254]

(5)

[0256]

여기서 $[r_0, \dots, r_5]$ 는 (4)에서 축소된 형태의 8개 상수 열 벡터 중 하나이다. 각 열의 항목에서 다항식

$$r(x) = \sum_{i=0}^5 r_i x^i$$

를 형성하고, 이러한 모든 다항식은 다음 순서로 나열된다.

$$P_8 := \{1+x, 1+x+x^3+2x^5, 1+2x+x^2+2x^4+2x^5, 1+2x+2x^2+x^4+2x^5, 2+x, 2+x+x^3+2x^5, 2+2x+x^2+2x^4+2x^5, 2+2x+2x^2+x^4+2x^5\}.$$

[0257]

[0259]

이러한 관계식 (5)를 $f(x)$ 로 대체하면 다음과 같이 산출된다.

[0261]

$$f(x) = r(x) + H(x), \quad r \in P_8, \quad (6)$$

[0263]
$$H(x) = 3 \sum_{i=0}^5 z_i x^i + \sum_{i=6}^{6k} a_i h_i(x), \quad 1 \leq i \leq k, \quad (7)$$

[0265]
$$\begin{aligned} h_{6i}(x) &= x^2 + x^4 + x^{6i}, h_{6i+1}(x) = x^3 + x^5 + x^{6i+1}, h_{6i+2}(x) = 2x^2 + x^{6i+2} \\ h_{6i+3}(x) &= 2x^3 + x^{6i+3}, h_{6i+4}(x) = 2x^4 + x^{6i+4}, h_{6i+5}(x) = 2x^5 + x^{6i+5}. \end{aligned}$$

[0267] 다항식 h_i 는 모듈로 3의 항등이며 모듈로 9인 $h_i(2) \equiv 2^6 \equiv 1 \pmod{9}$ 로 계산하기 쉽다. 따라서 (7)에서 H 의 다음과 같은 중요한 속성을 쉽게 확인할 수 있으며 이후 계산에서 암시적으로 많이 사용된다.

[0269] $H(x)$ 와 $H'(x)$ 는 모듈로 3의 항등이다.

[0270] $t(x)$ 가 모듈로 3의 항등인 경우 $H(x+t(x)) \equiv H(x) \pmod{9}$ 이다.

[0272] $H(i)$ 모듈로 9의 값은 각 $i=0,1,2$ 에 대해 다음과 같이 얻어진다.

[0273]
$$\begin{aligned} H(0) &= 3z_0; \\ H(1) &\equiv 3(z_0 + z_1 + z_2 + z_3 + z_4 + z_5) + 3E_0 + 3E_1 + 3E_2 + 3E_3 + 3E_4 + 3E_5 \pmod{9}; \quad (8) \\ H(2) &\equiv 3(z_0 + 2z_1 + z_2 + 2z_3 + z_4 + 2z_5) + 3E_0 + 6E_1 + 3E_2 + 6E_3 + 3E_4 + 6E_5 \pmod{9}, \end{aligned}$$

[0274] , 이 때 $0 \leq k \leq 5, E_k = \sum_{i \geq 6, i \equiv k \pmod{6}} a_i$ 이다.

[0276] 다음을 계산하는 것은 유용하다.

[0277]
$$H(0) + H(1) + H(2) \equiv 6(z_2 + z_4) + 6E_0 + 6E_2 + 6E_4 \pmod{9}$$

[0279] (M3)의 경우 이제 계수 a_i 의 관점에서 $f^3(0)$ 모듈로 9를 계산한다. 테일러 정리는 (6)의 다항식에 대해 다음을 산출한다.

[0281]
$$\begin{aligned} f^2(x) &\equiv f(r(x) + H(x)) \equiv f(r(x)) + H(x)r'(r(x)) \pmod{9} \\ &\equiv r^2(x) + H(r(x)) + H(x)r'(r(x)) \pmod{9}. \end{aligned} \quad (9)$$

[0283] 유사하게, $f^3(x)$ 를 한번 더 계산하면 다음을 산출한다.

[0284]
$$f^3(x) \equiv r^3(x) + H(r^2(x)) + H(r(x))r'(r^2(x)) + H(x)r'(r(x))r'(r^2(x)) \pmod{9}$$

[0286] 따라서, $f^3(0) \equiv r^3(0) + r'(r^2(0))r'(r(0))H(0) + r'(r^2(0))H(r(0)) + H(r^2(0)) \pmod{9}$ 이다.

[0288] 각 $r \in P_8$ 에 대해서 $r(0)$ 모듈로 9를 계산하면 다음과 같다.

$$f^3(0) \equiv \begin{cases} 3 + H(0) + H(1) + H(2) \pmod{9} & \text{if Case 1;} \\ H(0) + 2H(1) + H(2) \pmod{9} & \text{if Case 2;} \\ 2H(0) + 2H(1) + H(2) \pmod{9} & \text{if Case 3;} \\ 2H(0) + H(1) + H(2) \pmod{9} & \text{if Case 4;} \\ 6 + H(0) + H(1) + H(2) \pmod{9} & \text{if Case 5;} \\ 3 + H(0) + H(1) + 2H(2) \pmod{9} & \text{if Case 6;} \\ 6 + 2H(0) + H(1) + H(2) \pmod{9} & \text{if Case 7; and} \\ 6 + 2H(0) + H(1) + 2H(2) \pmod{9} & \text{if Case 8.} \end{cases}$$

[0290] (11)

[0292] (8)의 값을 사용하여 (11)의 표현식을 a_i 로 다시 쓸 수 있다.

$$f^3(0) \equiv \begin{cases} 2(A_0 + 6) \pmod{9} & \text{if Case 1;} \\ A_1 + a_0 + 4 \pmod{9} & \text{if Case 2;} \\ A_1 + 2a_0 + 3 \pmod{9} & \text{if Case 3;} \\ 2(A_0 + 5a_0 + 1) \pmod{9} & \text{if Case 4;} \\ 2(A_0 + 3) \pmod{9} & \text{if Case 5;} \\ 2(A_1 + 5a_0 + 1) \pmod{9} & \text{if Case 6;} \\ 2(A_0 + 5a_0 + 8) \pmod{9} & \text{if Case 7; and} \\ 2(A_1 + a_0 + 6) \pmod{9} & \text{if Case 8.} \end{cases} \quad (12)$$

[0294]

[0295] 이제 $(f^3)''(0) \pmod{3}$ 값을 다음과 같이 계산하여 (M4)로 바꾼다.

$$\begin{aligned} (f^3)''(0) &= f'(f^2(0))f'(f(0))f''(0) + f'(f^2(0))f'(0)^2f''(f(0)) + f'(f(0))^2f'(0)^2f''(f^2(0)) \\ &\equiv f'(f^2(0))f'(f(0))f''(0) + f'(f^2(0))f''(f(0)) + f''(f^2(0)) \pmod{3}, \end{aligned} \quad (13)$$

[0297]

[0299] 왜냐하면 임의의 $\lambda \not\equiv 0 \pmod{3}$ 에 대해 $\lambda^2 \equiv 1 \pmod{3}$ 이기 때문이다.

[0301] (13)으로부터 $f(x) \equiv r(x) \pmod{3}$ 과 $f'(x) \equiv r'(x) \pmod{3}$ 이기 때문에, 다음을 가진다.

$$(f^3)''(0) \equiv r'(r^2(0))r'(r(0))f''(0) + r'(r^2(0))f''(r(0)) + f''(r^2(0)) \pmod{3}. \quad (14)$$

[0303]

[0305] 위 (10)과 (14)의 r' 관련 계수 사이에는 완벽한 일치이 있다. (14)의 공식을 이용하여 다음을 얻는다.

$$(f^3)''(0) \equiv \begin{cases} f''(0) + f''(1) + f''(2) \pmod{3} & \text{if Case 1;} \\ f''(0) + 2f''(1) + f''(2) \pmod{3} & \text{if Case 2;} \\ 2f''(0) + 2f''(1) + f''(2) \pmod{3} & \text{if Case 3;} \\ 2f''(0) + f''(1) + f''(2) \pmod{3} & \text{if Case 4;} \\ f''(0) + f''(1) + f''(2) \pmod{3} & \text{if Case 5;} \\ f''(0) + f''(1) + 2f''(2) \pmod{3} & \text{if Case 6;} \\ 2f''(0) + f''(1) + f''(2) \pmod{3} & \text{if Case 7; and} \\ 2f''(0) + f''(1) + 2f''(2) \pmod{3} & \text{if Case 8.} \end{cases} \quad (15)$$

[0306]

[0308] 이에 대한 직접적인 계산은 다음을 산출한다.

[0310]
$$f'''(0) = 2a_2; f'''(1) \equiv -\sum_{j \geq 0} a_{3j+2} \pmod{3}; f'''(2) \equiv -\sum_{j \geq 0} (-1)^j a_{3j+2} \pmod{3}.$$

[0312] 이들의 항등을 (15)에 적용하면 다음을 산출한다.

[0314]
$$(f^3)''(0) \equiv \begin{cases} 2a_2 + \sum_{j \geq 0} a_{6j+2} \pmod{3} & \text{if Case 1;} \\ 2a_2 + 2\sum_{j \geq 0} a_{6j+5} \pmod{3} & \text{if Case 2;} \\ a_2 + 2\sum_{j \geq 0} a_{6j+5} \pmod{3} & \text{if Case 3;} \\ a_2 + \sum_{j \geq 0} a_{6j+2} \pmod{3} & \text{if Case 4;} \\ 2a_2 + \sum_{j \geq 0} a_{6j+2} \pmod{3} & \text{if Case 5;} \\ 2a_2 + \sum_{j \geq 0} a_{6j+5} \pmod{3} & \text{if Case 6;} \\ a_2 + \sum_{j \geq 0} a_{6j+2} \pmod{3} & \text{if Case 7; and} \\ a_2 + \sum_{j \geq 0} a_{6j+5} \pmod{3} & \text{if Case 8.} \end{cases} \quad (16)$$

[0316] 따라서, (M3)의 등가 조건은 정리 5.2.의 설명에 표시된 것처럼 각 경우에 대해 (12)에 의해 제공된다. (M4)와 관련하여, (12) 및 (16)에서 $2 f^3(0) \not\equiv 3(f^3)'(0) \pmod{9}$ 를 계산하면 정리 5.2.의 설명에 표시된 것처럼 각 경우에 대해 동등한 조건이 생성된다. 정리 5.2.에서 $a_0=1$ 에 주목하여 F. Durand and F. Paccaut, Minimal polynomial dynamics on the set of 3-adic intergers, Bull.Lond. Math.Soc. 41 (2), (2009)의 결과를 산출한다.

[0318] **따름정리 5.3.**

[0319] 차수 $d \geq 1$ 의 다항식 $f(x) = a_0 + a_1x + \dots + a_dx^d \in \mathbb{Z}_3[x]$ 은 오직 f 가 (i)-(iv) 조건 중 하나를 이행할 때에만 최소이다($[a_0, A_1, A_0, D_0, D_1, D_2] \pmod{3} = [\cdot, \cdot, \cdot, \cdot, \cdot, \cdot]$ 로 설정한다).

- [0321] (i) $[1, 1, 0, 1, 1, 1], A_0 + 6 \not\equiv 0 \pmod{9}, A_0 + 6 \not\equiv 6a_2 + 3\sum_{j \geq 0} a_{6j+2} \pmod{9};$
 (ii) $[1, 1, 0, 1, 2, 2], A_1 + 5 \not\equiv 0 \pmod{9}, A_1 + 5 \not\equiv 3a_2 + 3\sum_{j \geq 0} a_{6j+5} \pmod{9};$
 (iii) $[1, 1, 0, 2, 1, 2], A_1 + 5 \not\equiv 0 \pmod{9}, A_1 + 5 \not\equiv 6a_2 + 3\sum_{j \geq 0} a_{6j+5} \pmod{9};$ and
 (iv) $[1, 1, 0, 2, 2, 1], A_0 + 6 \equiv 0 \pmod{9}, A_0 + 6 \not\equiv 3a_2 + 3\sum_{j \geq 0} a_{6j+2} \pmod{9};$

[0323] 정리 3.1.에 비추어 볼 때, 정리 5.2.에서 최대 8차 다항식의 완전한 최소 기준을 추론하는 것이 중요하다.

[0325] **따름정리 5.4.**

[0326] 다항식 $f(x) = a_0 + a_1x + \dots + a_8x^8 \in \mathbb{Z}_3[x]$ 는 오직 다음 조건(i)-(viii) 중 하나를 이행할 때 최소이다($[a_0, A_1, A_0, D_0, D_1, D_2] \pmod{3} = [\cdot, \cdot, \cdot, \cdot, \cdot, \cdot]$ 로 설정한다). 다음은 정리 5.2.으로부터 자명하다.

(i) $[1, 1, 0, 1, 1, 1], a_2 + a_4 + a_6 + a_8 + 6 \not\equiv 0 [9], a_2 + a_4 + a_6 + 7a_8 + 6 \not\equiv 0 [9];$
(ii) $[1, 1, 0, 1, 2, 2], a_0 + a_1 + a_3 + a_5 + a_7 + 4 \not\equiv 0 [9], a_0 + a_1 + 6a_2 + a_3 + 7a_5 + a_7 + 4 \not\equiv 0 [9];$
(iii) $[1, 1, 0, 2, 1, 2], 2a_0 + a_1 + a_3 + a_5 + a_7 + 3 \not\equiv 0 [9], 2a_0 + a_1 + 3a_2 + a_3 + 7a_5 + a_7 + 3 \not\equiv 0 [9];$
(iv) $[1, 1, 0, 2, 2, 1], 2a_0 + a_2 + a_4 + a_6 + a_8 + 4 \not\equiv 0 [9], 2a_0 + 4a_2 + a_4 + a_6 + 7a_8 + 4 \not\equiv 0 [9];$
(v) $[2, 1, 0, 1, 1, 1], a_2 + a_4 + a_6 + a_8 + 3 \not\equiv 0 [9], a_2 + a_4 + a_6 + 7a_8 + 3 \not\equiv 0 [9];$
(vi) $[2, 1, 0, 1, 1, 2], 2a_0 + a_1 + a_3 + a_5 + a_7 + 7 \not\equiv 0 [9], 2a_0 + a_1 + 3a_2 + a_3 + 7a_5 + a_7 + 7 \not\equiv 0 [9];$
(vii) $[2, 1, 0, 2, 1, 2], 2a_0 + a_2 + a_4 + a_6 + a_8 + 5 \not\equiv 0 [9], 2a_0 + 4a_2 + a_4 + a_6 + 7a_8 + 5 \not\equiv 0 [9];$ and
(viii) $[2, 1, 0, 2, 2, 1], a_0 + a_1 + a_3 + a_5 + a_7 + 6 \not\equiv 0 [9], a_0 + a_1 + 6a_2 + a_3 + 7a_5 + a_7 + 6 \not\equiv 0 [9].$

[0327]

[0328] 다음 부명제는 $p=3$ 케이스에 대한 정리 3.1.의 part(2)의 증명을 완료하는 것으로 입증된다.

[0330] **부명제 5.5.**

[0331]
$$\#R(3^3) = 2^5 \cdot 3^{10}.$$

[0333] 증명. 우리는 따름정리 5.4.를 사용하여 모든 가능한 비동등 최소 다항식 모듈로 3^3 의 수는 8가지 경우 각각에 대해 $4 \cdot 3^{10}$ 이라고 단언한다. 우리는 나머지는 비슷한 방식으로 수행할 수 있기 때문에 케이스 1에 대해서만 이 작업을 수행한다. $f(x) = a_0 + a_1x + \dots + a_8x^8 \in \mathbb{Z}/27\mathbb{Z}[x]$ 가 최대 8차의 최소 다항식이라고 하면 (5)로부터 따름정리 5.5.의 Case (i)에서 f 의 파라메트릭 표현은 다음 관계식으로 주어진다.

[0334]
$$\begin{aligned} a_0 &= 1 + 3z_0, a_1 = 1 + 3z_1, a_2 = a_6 + 2a_8 + 3z_2, a_3 = a_7 + 3z_3; \\ a_4 &= a_6 + 3z_4, a_5 = a_7 + 3z_5, a_6 = e_6 + 3z_6, a_7 = e_7 + 3z_7, a_8 = e_8 + 3z_8, \end{aligned} \quad (17)$$

[0337] 이 때, $z_i \in \mathbb{Z}/9\mathbb{Z} (0 \leq i \leq 8)$ 그리고 $e^i \in \mathbb{Z}/3\mathbb{Z} (6 \leq i \leq 8)$ 이다. 이러한 관계식은 다음 형식의 f 에 대한 분해를 산출한다.

[0339]
$$f(x) = 1 + x + H(x), \quad (18)$$

[0341] 이 때,

[0342]
$$\begin{aligned} H(x) &= 3(z_0 + z_1x + (z_2 + z_6 + 2z_8)x^2 + (z_3 + z_7)x^3 + (z_4 + z_6)x^4 + (z_5 + z_7)x^7) \\ &\quad + 3(z_6x^6 + z_7x^7 + z_8x^8) + e_6(x^2 + x^4 + x^6) + e_7(x^3 + x^5 + x^7) + e_8(2x^2 + x^8). \end{aligned}$$

[0344] Case 1에 대한 따름정리 5.4.로부터 f 의 최소 조건들은 다음과 같이 주어진다.

[0346]
$$a_2 + a_4 + a_6 + a_8 + 6 \not\equiv 0 [9], a_2 + a_4 + a_6 + 7a_8 + 6 \not\equiv 0 [9].$$

[0348] (17)을 통해 그들은 각각 다음과 같다.

[0350]
$$z_2 + z_4 + e_6 + e_8 + 2 \not\equiv 0 \pmod{3}, \quad z_2 + z_4 + e_6 + 2 \not\equiv 0 \pmod{3}. \quad (19)$$

[0352] S를 (19)의 두 상태를 만족하는 다음과 같은 모든 계수 벡터의 집합이라고 한다.

[0353]
$$\mathbf{z} := [z_0, \dots, z_5, e_6, e_7, e_8, z_6, z_7, z_8] \in (Z/9Z)^6 \times (Z/3Z)^3 \times (Z/9Z)^3$$

[0355] S의 집합크기가 $4 \cdot 3^{19}$ 임을 보여주는 것은 간단하다. 실제로 보수집합으로 인해 S의 모든 벡터의 수는 다음과 같으며,

[0356]
$$\begin{aligned} & 3^{21} - \#\{[z_0, \dots, z_5, e_6, e_7, e_8, z_6, z_7, z_8] \mid z_2 + z_4 + e_6 + e_8 + 2 \equiv 0 \pmod{3}\} \\ & \quad - \#\{[z_0, \dots, z_5, e_6, e_7, e_8, z_6, z_7, z_8] \mid z_2 + z_4 + e_6 + 2 \equiv 0 \pmod{3}\} \\ & \quad + \#\{[z_0, \dots, z_5, e_6, e_7, e_8, z_6, z_7, z_8] \mid z_2 + z_4 + e_6 + e_8 + 2 \equiv 0 \pmod{3}; z_2 + z_4 + e_6 + 2 \equiv 0 \pmod{3}\}, \end{aligned}$$

[0357] 이는 다음과 같다.

[0358]
$$3^{21} - 3^{20} - 3^{20} + 3^{19} = 4 \cdot 3^{19}$$

[0360] S에 동일한 다항식 모듈로 27을 유도하는 최소 다항식이 있을 수 있기 때문에 이제 S에 대한 등가 관계를 고려하여 S에서 동일하지 않은 최소 다항식의 하위 집합을 계산한다. S의 두 벡터 $\mathbf{z}$ 와 $\mathbf{z}'$ 에 대해, 두 다항식 $f_{\mathbf{z}}$ 와 $f_{\mathbf{z}'}$ 가 연관된 두 개의 다항식이 동일한 최소 다항식을 유도하면 $\mathbf{z} \sim \mathbf{z}'$ 이라고 한다. 여기서 $f_{\mathbf{z}}(x) = 1 + x + H_{\mathbf{z}}(x)$ 와 $f_{\mathbf{z}'}(x) = 1 + x + H_{\mathbf{z}'}(x)$ 는 (19)와 같다. 그러면 $\sim$ 가 S에 대한 등가 관계인지 확인하여야 함이 명백하다. 벡터 $\mathbf{z}$ 의 등가 클래스를 계산하기 위해 다음과 같은 합동에서 시작한다.

[0362]
$$1 + x + H_{\mathbf{z}}(x) \equiv 1 + x + H_{\mathbf{z}'}(x) \pmod{27}$$

[0364] 이로부터 즉시 다음을 얻는다.

[0366]
$$\frac{1}{3}H_{\mathbf{z}}(x) \equiv \frac{1}{3}H_{\mathbf{z}'}(x) \pmod{9}. \quad (20)$$

[0368] $Z = (Z_0, \dots, Z_5, E_6, E_7, E_8, Z_6, Z_7, Z_8) := \mathbf{z} - \mathbf{z}'$ 를 설정하면, $x=0, \dots, 8$ 을 (20)의 합동 방정식으로 대체하여 Z'_i s와 E'_i s 관점에서 모듈로 9의 선형 방정식 시스템을 얻는다. 링 $Z/9Z$ 에 대해 작업하기 때문에 곱고 계수 행렬의 행 사다리꼴 형식은 다음 행렬로 제공된다.

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 6 & 0 & 3 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 7 & 3 & 0 & 3 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 6 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 & 0 & 0 \end{pmatrix} \quad (21)$$

$Z_i \in \mathbb{Z}/9\mathbb{Z}$ 이고, $E_i \in \mathbb{Z}/3\mathbb{Z}$ 이기 때문에 (21)의 사다리꼴 형식에서 다음과 같은 자명한 관계를 산출한다.

$$Z_0 = 0; E_6 = 0; E_7 = 0; E_8 = 0$$

이러한 관계와 함께 다음과 같은 일부 비자명한 관계도 제공된다.

$$\begin{aligned} Z_1 + Z_3 + Z_5 + 3Z_7 &\equiv 0 \pmod{9}; \\ Z_2 + Z_4 + 3Z_6 + 3Z_8 &\equiv 0 \pmod{9}; \\ 3Z_3 &\equiv 0 \pmod{9}; \\ 3Z_4 &\equiv 0 \pmod{9}; \text{ and} \\ 3Z_5 &\equiv 0 \pmod{9}. \end{aligned}$$

이러한 관계에서 S의 f 에 대한 최소 조건이 불변하다는 것을 알 수 있다.

$1 \leq i \leq 5$ 에 대해 $w_i \in \mathbb{Z}/3\mathbb{Z}$ 인 $Z_i = 3w_i$ 이고, $i = 6, 7, 8$ 에 대해 $w_i, d_i \in \mathbb{Z}/3\mathbb{Z}$ 인 $Z_i = w_i + 3d_i$ 라고 쓰는 것은, 위와 같은 관계에서 다음을 얻을 수 있다.

$$\begin{aligned} w_1 + w_3 + w_5 + w_7 &\equiv 0 \pmod{3}; \\ w_2 + w_4 + w_6 + w_8 &\equiv 0 \pmod{3}. \end{aligned} \quad (22)$$

모든 w_i 가 $\mathbb{Z}/3\mathbb{Z}$ 에 걸쳐 있기 때문에 $[w_1, w_2, \dots, w_8]$ 벡터에 대해 정확히 3^6 개의 선택 항목이 있으며 (22)의 관계를 충족한다. 따라서 벡터 Z 의 수가 3^6 이므로, S의 계수 벡터 $\mathbf{z}$ 의 등가 클래스는 $4 \cdot 3^{19} / 3^9 = 4 \cdot 3^{10}$ 의 카디널리티를 갖는다. 따라서 S에서 동일하지 않은 최소 다항식의 수는 $4 \cdot 3^{10}$ 이다. 이로써 증명이 완성된다.

본 발명은 임의의 소수 $p \geq 5$ 를 포함하여 최소 다항식에 대한 완전한 설명을 제공한다. 중국인의 나머지 정리를 사용하여, 이 작업은 고정 소수 p 의 모든 거듭 제곱에 대한 모듈로 전이(최소) 다항식을 분류하는 것으로 축소된다. 이전 내용에서 $p = 2$ or 3 에 대하여 설명을 마쳤고, 이제 $\mathbb{Z}_p[x]$ 위에서 임의의 소수 $p \geq 5$ 에 대해 설명한다.

[0385] $Z_p[x]$ 에서 다항식의 최소 기준은 다음과 같은 명제에 의하여 찾을 수 있으며, 이는 명제 2.8. 및 2.9.의 형식을 따른다.

[0387] **명제 6.1.**

[0388] 다항식 $f \in Z_p[x]$ 는 오직 다음 조건을 충족할 때에만 최소이다.

[0389] (i) f 는 전이 모듈로 p 이다.

[0390] (ii) $(f^p)'(0) \equiv 1 \pmod{p}$; and

[0391] (iii) $f^p(0) \in pZ_p \setminus p^2Z_p$.

[0393] 정리 3.1.에서 δ 로 축소하여, Z/p^2Z 링에서 정수 계수를 가지는 $Z_p[x]$ 에서의 다항식에서 먼저 $2p-1$ 이하 차수의 다항식으로 제한하고, 이어서 최대 $2p-1$ 차수의 모든 최소 다항식에 대한 완전한 설명을 제시한다. 다음 주요 결과는 집합 $R(p^2)$ 의 최소 다항식의 구조를 보여준다.

[0396] **정리 6.2.**

[0397] 다항식 $f \in Z/p^2Z[x]$ 는 $R(p^2)$ 에서 오직 $f(x) = f_0(x) + pf_1(x)$ 일 때 최소이다.

[0398]

[0399] 이 때, (i) $f_0(x) = \sum_{i=0}^{2p-1} e_i x_i \in Z/pZ[x]$ 는 최대 $2p-1$ 차수의 전이 다항식 모듈로 p 이고, 그것의 계수 열 벡터 $[e_0, \dots, e_{2p-1}]^t$ 의 유일한 해는 다음과 같은 선형 시스템의 형태를 가진다.

[0400] $M \mathbf{x} \equiv \mathbf{b} \pmod{p}$,

[0401] 이 때, 계수 매트릭스 M 은 (28)에 의해 주어지고, (25)에서 $\mathbf{b} = [B_0, \dots, B_{p-1}, D_0, \dots, D_{p-1}]$ 는 명제 6.1.의 조건 (i)과 (ii)를 충족하는 $(p-1)!(p-1)^{p-1}$ 선택 중에 선택되어 주어진 상수 벡터이다.

[0403] (ii) 계수 행 벡터, $f_1(x) = \sum_{i=0}^{2p-1} z_i x_i \in Z/pZ[x]$ 의 $[z_0, \dots, z_{2p-1}]$ 는 다음과 같은 선형 다항식 l 의 0이 되지 않는 모듈로 p 를 충족한다.

[0405] $l(z_0, \dots, z_{2p-1}) \not\equiv 0 \pmod{p}$,

[0407] 이 때, $l(z_0, \dots, z_{2p-1})$ 은 다음 공식에 의해 명백히 주어진다.

[0408]
$$l(z_0, \dots, z_{2p-1}) = \frac{1}{p} f_0^p(0) + \frac{1}{f_0'(0)} z_0 + \sum_{i=1}^{p-1} w_i f_1(f_0^i(0)), \quad (23)$$

[0410] 이 때, $1 \leq i \leq p-2$ 에 대해 다음과 같다.

[0411]
$$w_i = \prod_{j=i+1}^{p-1} f_0'(f_0^j(0)) \text{ and } w_{p-1} = 1. \quad (24)$$

[0413] 2. $\#R(p^2) = (p-1)!(p-1)^p p^{p-1}$ 이다.

[0414] 증명. $f(x) = a_0 + a_1 x + \dots + a_{2p-1} x^{2p-1} \in Z/p^2 Z[x]$ 에 대해, 최대 $2p-1$ 차수의 다항식의 상수 $B_0, \dots, B_{p-1}, D_0, \dots, D_{p-1}$ 은 다음과 같다.

$$\begin{aligned} a_0 &= B_0; \\ a_1 + a_p + a_{2p-1} &= B_1; \\ a_2 + a_{p+1} &= B_2; \\ &\vdots \\ a_{p-1} + a_{2p-2} &= B_{p-1}; \\ a_1 &= D_0; \\ \sum_{i=1}^{2p-1} i a_i &= D_1; \\ &\vdots \\ \sum_{i=1}^{2p-1} i(p-1)^{i-1} a_i &= D_{p-1}, \end{aligned} \quad (25)$$

[0416]

[0418] $x^p \equiv x \pmod{p}$ 이기 때문에 다항식 f 는 다음과 같은 모듈로 p 로 축소된다.

[0419]
$$f(x) \equiv B_0 + B_1 x + \dots + B_{p-1} x^{p-1}. \quad (26)$$

[0421] 나아가, 각 $0 \leq i \leq p-1$ 에 대해 $f'(i) = D_i$ 이다.

[0422] 다음으로 (25)를 주어진 상수 열 벡터, $\mathbf{b} = [B_0, \dots, B_{p-1}, D_0, \dots, D_{p-1}]^t$ 모듈로 p 에 대해 명제 6.1.의 조건 (i)과 (ii)를 만족하는 변수 $\mathbf{x} = [a_0, \dots, a_{2p-1}]^t$ 인 선형 시스템으로 고려한다.

[0423]
$$M\mathbf{x} \equiv \mathbf{b} \pmod{p}, \quad (27)$$

[0424] 이 때, M 은 다음과 같은 형태로 명백하게 주어지는 $2p \times 2p$ 계수 행렬이다.

$$M = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 1 & \cdots & 1 \\ 0 & 0 & 1 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & \cdots & 0 \\ 0 & 1 & 2 & \cdots & p-1 & p & \cdots & 2p-1 \\ 0 & 1 & 2 \cdot 2 & \cdots & (p-1) \cdot 2^{p-2} & p \cdot 2^{p-1} & \cdots & (2p-1) \cdot 2^{2p-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 1 & 2 \cdot (p-1) & \cdots & (p-1) \cdot (p-1)^{p-2} & p \cdot (p-1)^{p-1} & \cdots & (2p-1) \cdot (p-1)^{2p-2} \end{pmatrix} \quad (28)$$

[0425]

[0426] 행렬 M 모듈로 p 가 가역적임을 확인하는 것은 흥미로운 연습이다. 실제로 행 연산과 페르마의 소 정리를 사용하여 M 의 축소된 행-사다리꼴이 Vandermonde 부분 행렬을 도출함으로써 단위 행렬임을 보여줄 수 있다. M 모듈로 p 의 가역성은 상수 열 벡터 $\mathbf{b} = [B_0, \dots, B_{p-1}, D_0, \dots, D_{p-1}]^t$ 모듈로 p 가 절절하게 선택될 때마다 (27)의 선형 시스템에 대한 해가 고유함을 의미한다. 주어진 다항식 $f \in R(p^2)$ 이 최소가 되도록 명제 6의 (i) 및 (ii) 조건을 만족하는 상수 열 벡터 $\mathbf{b}$ 를 선택해야 한다. 따라서 계수 벡터 $[B_0, B_1, \dots, B_{p-1}] \pmod{p}$ 를 선택하여 (26)에서 f 의 축소된 함수가 전이 다항식 모듈로 p 가 되도록 한다. 동시에 아래와 같이 조건 (ii)를 만족하는 벡터 $[D_0, D_1, \dots, D_{p-1}] \pmod{p}$ 를 선택해야 한다.

[0428]

$$(f^p)'(0) \equiv f'(0) \cdot f'(1) \cdots f'(p-1) \equiv D_0 \cdot D_1 \cdots D_{p-1} \equiv 1 \pmod{p}.$$

[0430]

위와 같은 합동으로부터, 상수 벡터 $[D_0, D_1, \dots, D_{p-1}] \pmod{p}$ 에 대한 정확히 $(p-1)^{p-1}$ 개 선택이 존재한다. 함께 취하면, 조건 (i) 및 (ii)가 동시에 충족되도록 상수 벡터 $\mathbf{b} = [B_0, \dots, B_{p-1}, D_0, \dots, D_{p-1}]^t$ 모듈로 p 에 대해 정확히 $(p-1)!(p-1)^{p-1}$ 개의 선택이 존재한다.

[0431]

$E = [e_0, \dots, e_{2p-1}] \pmod{p}$ 가 $(p-1)!(p-1)^{p-1}$ 가지 선택 중에서 선택된 상수 벡터 $\mathbf{b}$ 에 대한 (27) 선형 시스템에 대한 유일한 해라고 한다. 해 벡터 E 에 대해 아래와 같은 다항식을 연결한다.

[0433]

$$f_0(x) = \sum_{i=0}^{2p-1} e_i x^i \in \mathbb{Z}/p\mathbb{Z}[x].$$

[0435]

그러면, $f(x) \equiv f_0(x) \pmod{p}$ 그리고 $f'(x) \equiv f_0'(x) \pmod{p}$ 이다.

[0437]

다음으로 f_0 을 이용하여 명제 6.1.의 조건 (iii)에 해당하는 더 간단한 조건을 찾는 것이 남아있다. 이를 위해, 먼저 $a_0 = e_0 + pz_0$ 과 다음과 같은 합동을 유도한다.

$$\frac{1}{p}f^p(0) \equiv \frac{1}{p}f^{p-1}(e_0) + \frac{1}{f'_0(0)}z_0 \pmod{p}. \quad (29)$$

[0439]

[0441] 실제로, 테일러 정리는 다음을 산출한다.

[0442]

$$f^2(0) = f(e_0 + pz_0) \equiv f(e_0) + pz_0f'(e_0) \equiv f(e_0) + pz_0f'_0(e_0) \pmod{p^2}.$$

[0443]

유사하게,

[0444]

$$f^3(0) \equiv f(f(e_0) + pz_0f'_0(e_0)) \equiv f^2(e_0) + pz_0f'_0(e_0)f'_0(f_0(e_0)) \pmod{p^2}.$$

[0445]

이러한 식으로 계속하면 다음을 얻는다.

[0446]

$$f^p(0) \equiv f^{p-1}(e_0) + pz_0f'_0(e_0)f'_0(f_0(e_0)) \cdots f'_0(f_0^{p-2}(e_0)) \pmod{p^2}.$$

[0448]

$\prod_{i=0}^{p-1} f'(i) \equiv \prod_{i=0}^{p-1} f'_0(i) \equiv 1 \pmod{p}$ 이므로 $f \equiv f_0 \pmod{p}$ 는 전이 모듈로 p 이고, f 는 조건 (ii)를 만족하므로 다음과 같은 합동을 제공한다. 따라서, p 로 나누는 것은 (29)에서 원하는 합동을 생성한다.

[0449]

$$f^p(0) \equiv f^{p-1}(e_0) + \frac{1}{f'_0(0)}pz_0 \pmod{p^2}.$$

[0451]

$f^p(0)$ 에 대한 더 간단한 공식을 찾기 위해 한 단계 더 나아가 $f^{p-1}(e_0)$ 모듈로 p^2 에 해당하는 공식을 도출한다. 이를 마치기 위해, f 를 두 다항식의 합으로 분해하기 위해 $a_i = e_i + pz_i (0 \leq i \leq 2p-1)$ 이라고 쓴다.

[0452]

$$f(x) = f_0(x) + pf_1(x), \quad f_1(x) = \sum_{i=0}^{2p-1} z_i x^i \in \mathbb{Z}/p\mathbb{Z}[x].$$

[0454]

이 작업은 z_i 의 모듈로 p , 즉 a_i 모듈로 p^2 에서 조건을 찾는 것이므로 f 는 전이 다항식 모듈로 p^2 이다. 따라서, f 는 최소이다. 이는 다항식 f_0 을 처음부터 알고 있기 때문에 가능하다. 따라서 f 의 분해를 사용하여 $f^{p-1}(e_0)$ 모듈로 p^2 을 계산할 수 있다.

[0456]

먼저, 테일러 정리는 다음을 준다.

[0457]

$$\begin{aligned} f^2(e_0) &\equiv f(f_0(e_0) + pf_1(e_0)) \equiv f(f_0(e_0)) + pf_1(e_0)f'(f_0(e_0)) \pmod{p^2} \\ &\equiv f_0^2(e_0) + pf_1(f_0(e_0)) + pf_1(e_0)f'_0(f_0(e_0)) \pmod{p^2}. \end{aligned}$$

[0459]

한번더,

[0460]

$$\begin{aligned} f^3(e_0) &\equiv f(f_0^2(e_0) + pf_1(f_0(e_0)) + pf_1(e_0)f'_0(f_0(e_0))) \\ &\equiv f_0^3(e_0) + pf_1(f_0^2(e_0)) + (pf_1(f_0(e_0)) + pf_1(e_0)f'_0(f_0(e_0)))f'_0(f_0^2(e_0)) \\ &\equiv f_0^3(e_0) + pf_1(f_0^2(e_0)) + pf_1(f_0(e_0))f'_0(f_0^2(e_0)) + pf_1(e_0)f'_0(f_0(e_0))f'_0(f_0^2(e_0)) \pmod{p^2}. \end{aligned}$$

[0461] 이 절차를 반복하면 모듈로 p^2 을 얻는다.

$$\begin{aligned} f^{p-1}(e_0) &= f_0^{p-1}(e_0) + pf_1(f_0^{p-2}(e_0)) + pf_1(f_0^{p-3}(e_0))f_0'(f_0^{p-2}(e_0)) \\ &\quad + pf_1(f_0^{p-4}(e_0))f_0'(f_0^{p-2}(e_0))f_0'(f_0^{p-3}(e_0)) + \cdots \\ &\quad + pf_1(f_0(e_0))f_0'(f_0^2(e_0))f_0'(f_0^3(e_0)) \cdots f_0'(f_0^{p-2}(e_0)) + pf_1(e_0)f_0'(f_0(e_0))f_0'(f_0^2(e_0)) \cdots f_0'(f_0^{p-2}(e_0)). \end{aligned}$$

[0463]

[0465] $1 \leq i \leq p-2$ 와 $w_{p-1}=1$ 에 대해 $w_i = \prod_{j=i}^{p-2} f_0'(f_0^j(e_0)) = \prod_{j=i+1}^{p-1} f_0'(f_0^j(0))$ 라고 설정하는 것은 다음과 동등하다.

$$f^{p-1}(e_0) \equiv f_0^{p-2}(e_0) + p \sum_{i=1}^{p-1} w_i f_1(f_0^i(0)) \pmod{p^2}. \quad (30)$$

[0467]

[0469] (29)와 (30)으로부터 명제 6.1.의 조건 (iii)에서 $\frac{1}{p}f^p(0)$ 에 대한 공식은 f_0 와 f_1 의 측면에서 다음과 같이 명백하게 표현된다.

$$\frac{1}{p}f^p(0) \equiv \frac{1}{p}f_0^p(0) + \frac{1}{f_0'(0)}z_0 + \sum_{i=1}^{p-1} w_i f_1(f_0^i(0)) \pmod{p}. \quad (31)$$

[0471]

[0473] 이후 (31)의 오른쪽은 $l(z_0, \dots, z_{2p-1})$ 로 표시된다. 다항식 f_1 에서 $l(z_0, \dots, z_{2p-1})$ 은 변수 $z_0, \dots, z_{2p-1}$ 에서 다항식이며 최대 차수 1인 $\mathbb{Z}/p\mathbb{Z}$ 에서 계수를 가진다. 마지막으로, 아래 보조정리 6.3.에 의해 조건 (iii)은 다음과 같은 선형 다항식 l 의 0이 아닌 모듈로 p 에 의해 결정된다.

$$l(z_0, \dots, z_{2p-1}) \not\equiv 0 \pmod{p}.$$

[0475]

[0477] 이로써, 정리 6.2.의 첫 번째 부분의 증명이 완성된다.

[0479] **보조정리 6.3.**

[0480] $l(z_0, \dots, z_{2p-1})$ 은 선형 다항식이다.

[0481] 증명. 먼저, $l(z_0, \dots, z_{2p-1})$ 에서 z_0 의 계수를 수집한다. z_0 의 계수는 $\frac{1}{f_0'(0)} + \sum_{i=1}^{p-1} w_i$ 에 의해 주어진다. 이 값이 모듈로 p 로 사라지지 않으면 원하는 결과가 명확하게 나타난다. 그러면, $l(z_0, \dots, z_{2p-1})$ 은 변수 $z_1, \dots, z_{2p-1}$ 의 다항식이다. 우리는 여기서 $l(z_0, \dots, z_{2p-1})$ 이 나머지 변수에서 선형이라는 단언한다. $l(z_0, \dots, z_{2p-1})$ 에서 변수 $z_1, \dots, z_{2p-1}$ 의 모든 계수가 0 모듈로 p 라고 가정한다. 그런 다음 계수행렬이 $p-1$ 개

의 구별되는 값 $f_0(0), \dots, f_0^{p-1}(0)$ 모듈로 p 와 관련된 방테르몽드 행렬인 변수 $w_1, \dots, w_{p-1}$ 에서 동종 선형 시스템을 얻는다. 방테르몽드 행렬의 가역성은 해 벡터 $[w_1, \dots, w_{p-1}]$ 이 자명하다는 것을 의미한다. 이는 w_i 가 모두 0이 아닌 모듈로 p 라는 명제 2.6.과 모순된다.

[0482] 이제 보조정리 6.3.을 이용해 정리 6.2의 파트 (2)를 증명한다. $(p-1)!(p-1)^{p-1}$ 가지 선택을 벗어나는 고정 상수 열 벡터 b 에 대해 조건 $l(z_0, \dots, z_{2p-1})$ 을 만족하는 모든 계수 벡터 $[z_1, \dots, z_{2p-1}] \pmod{p}$ 에 해당하는 $R(p^2)$ 에서 동일하지 않은 최소 다항식 집합을 계산할 필요가 있다. 이를 위해 다음과 같은 집합을 고려한다.

[0484]
$$S := \{[z_0, \dots, z_{2p-1}] \in (\mathbb{Z}/p\mathbb{Z})^{2p} \mid l(z_0, \dots, z_{2p-1}) \not\equiv 0 \pmod{p}\}.$$

[0486] 그 다음, 보조정리 6.3.으로 인해 S 는 여집합을 계산하여 집합의 크기가 $(p-1)p^{2p-1}$ 이다. S 의 $\mathbf{z}=[z_0, \dots, z_{2p-1}]$ 과 $\mathbf{z}'=[z'_0, \dots, z'_{2p-1}]$ 에 대해 만약 이들이 다음과 같이 분해가능한 동일한 최소 다항식 $f \in R(p^2)$ 를 유도하면 집합 S 에 대해 관계 $\mathbf{z} \sim \mathbf{z}'$ 을 정의한다.

[0488]
$$f = f_0 + pf_{1,\mathbf{z}} \equiv f_0 + pf_{1,\mathbf{z}'} \pmod{p^2}, \quad (32)$$

[0490] 이 때, $f_{1,\mathbf{z}}(x) = \sum_{i=0}^{2p-1} z_i x^i$ 와 $f_{1,\mathbf{z}'}(x) = \sum_{i=0}^{2p-1} z'_i x^i$ 이다. $\sim$ 가 S 위에서의 동치 관계인지 확인하는 것은 쉽다. $x^p \equiv x \pmod{p}$ $f_{1,\mathbf{z}}(x)$ 와 $f_{1,\mathbf{z}'}(x)$ 들이 (26)의 형식 $\sum_{i=0}^{p-1} B_i x^i$ 로 축소되기 때문에 (32)의 합 등은 다음과 동일하다.

[0492]
$$\sum_{i=0}^{p-1} B_i(\mathbf{z})x^i \equiv \sum_{i=0}^{p-1} B_i(\mathbf{z}')x^i \pmod{p}, \quad (33)$$

[0494] 이 때, $B_i(v)$ 는 B_i 를 정의하는 원소를 벡터 $\mathbf{v}$ 의 항목으로 대체하여 얻은 계수를 나타낸다. 합동(33)은 $\mathbf{z} \sim \mathbf{z}'$ 이 행렬 T 의 널 공간에 있다고 하는 것과 동일하다는 것을 쉽게 알 수 있다. 이 때, T 는 (28)에서 M 의 상위 $p \times 2p$ 부분 행렬이다. T 는 랭크 p 를 갖고, T 의 퇴화차수는 p 이기 때문에 S 의 동치류 클래스 집합의 크기는 $(p-1)p^{2p-1}/p^p = (p-1)p^{p-1}$ 이다. 따라서 각 b 에 대해 정확히 $(p-1)p^{p-1}$ 개의 비동등 최소 다항식이 있다는 결론을 내릴 수 있다. 따라서 $R(p^2) = (p-1)!(p-1)p^{p-1}$ 이다. 정리 6.2.의 파트 (2)에 대한 증명이 완료되고 이에 의하여 정리 3.1.의 파트 (2)의 증명도 마친다.

[0495] 정리 6.2.에 기술된 방법은 V. Anashin, and A. Khrennikov, Applied algebraic dynamics, Walter de Gruyter & Co., Berlin, 2009.와 본 발명자의 S. Jeong, Ergodic functions over $\mathbb{Z}_p$; preprint.에서 제안된 방법과 비교할 수 있다. V. Anashin,의 작업에서는 보간 다항식 f_ϕ 와 $f_{\phi,\psi}$ 를 계산하고 이들이 전이 모듈로 p^2 인지 테스트를 해야했다. 또한 S. Jeong, Ergodic functions over $\mathbb{Z}_p$; preprint의 방법에서는 이항 계수 다항식으로 표현되는 다항식의 최소 조건을 사용했다. 본 발명에서 제안된 방법은 기존 방법에 비하여 더 자연스럽게 효율적

이며 모든 차수의 다항식에 적용이 가능하다.

[0496] 이제 MATLAB 계산으로 구성된 예제로 정리 6.2의 절차를 설명한다.

[0497] 예제 1. $\phi = (1324560)$ 이 단일 사이클 순열 $\mathbf{F}$ 이라고 한다. (41) 또는 R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, 1997.의 Equation 7.1의 라그랑주 보간공식에 의해 보간 다항식, $f_\phi(x) = 3x^5 + 6x^4 + 3x^3 + 5x^2 + 6x + 1$ 이 결정된다. 따라서 벡터 $[B_0, \dots, B_6] \bmod 7 = [1, 6, 5, 3, 6, 3, 0]$ 이 발견된다. 잘 선택된 벡터 $[B_0, \dots, B_6, D_0, \dots, D_6] \bmod 7 = [1, 6, 5, 3, 6, 3, 0, 1, 1, 1, 1, 6, 6]$ 에 대해 (27)의 선형 시스템에 대한 모듈로 7, $[1, 1, 6, 0, 6, 5, 1, 2, 6, 3, 0, 5, 6, 3]$ 의 유일한 해를 찾고, 이로써 다음을 얻을 수 있다.

[0499]
$$f_0(x) = 3x^{13} + 6x^{12} + 5x^{11} + 3x^9 + 6x^8 + 2x^7 + x^6 + 5x^5 + 6x^4 + 6x^2 + x + 1.$$

[0501] f_0 으로부터 $f_0'(0) \equiv 14 \pmod{7^2}$, $[f_0'(0), f_0'(1), \dots, f_0'(6)] \bmod 7 = [1, 1, 1, 1, 1, 6, 6]$ 과 $[w_1, w_2, \dots, w_6] \bmod 7 = [1, 1, 1, 1, 6, 1]$ 을 얻는다. 따라서, 그 계수가 다음과 같이 (23)의 최소 조건을 충족하는 $f_1 = \sum_{i=0}^{13} z_i x^i$ 을 얻는다.

[0503]
$$l(z_0, \dots, z_{13}) = 5z_0 + 4z_1 + 6z_2 + 2z_3 + 3z_4 + z_5 + 4z_6 + 4z_7 + 6z_8 + 2z_9 + 3z_{10} + z_{11} + 4z_{12} + 4z_{13} + 2 \not\equiv 0 \pmod{7}.$$

[0505] 따라서, 이 조건을 만족하는 벡터, $[z_0, \dots, z_{13}] \bmod 7 = [5, 0, 0, 2, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0]$ 를 취하여 다음과 같은 최소 다항식을 얻는다.

[0507]
$$\begin{aligned} f(x) &= f_0 + 7f_1 \\ &= 3x^{13} + 6x^{12} + 5x^{11} + 3x^9 + 6x^8 + 2x^7 + x^6 + 5x^5 + 20x^4 + 14x^3 + 6x^2 + x + 36, \end{aligned}$$

[0509] 위 최소 다항식의 단일 사이클 궤도 모듈로 7^2 은 다음과 같이 주어진다.

[0511]
$$(0, 36, 45, 9, 39, 33, 27, 14, 1, 10, 23, 4, 47, 13, 28, 15, 24, 37, 18, 12, 48, 42, 29, 38, 2, 32, 26, 34, 7, 43, 3, 16, 46, 40, 20, 21, 8, 17, 30, 11, 5, 6, 35, 22, 31, 44, 25, 19, 41).$$

[0513] 다른 최소 다항식에 대해, 벡터 $[z_0, \dots, z_{13}] \bmod 7 = [1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1]$ 를 취하면 같은 최소 조건을 충족하고 다음과 같은 최소 다항식을 얻을 수 있다.

[0515]
$$f(x) = 10x^{13} + 6x^{12} + 5x^{11} + 3x^9 + 6x^8 + 2x^7 + x^6 + 5x^5 + 13x^4 + 13x^2 + 8x + 8,$$

[0517] 위 최소 다항식의 단일 사이클 레도 모듈로 7^2 은 다음과 같이 주어진다.

[0519] $(0, 8, 38, 16, 46, 40, 41, 21, 29, 10, 37, 18, 12, 20, 42, 1, 31, 9, 39, 33, 48, 14, 22, 3, 30, 11, 5, 27, 35, 43, 24, 2, 32, 26, 6, 7, 15, 45, 23, 4, 47, 34, 28, 36, 17, 44, 25, 19, 13).$

[0521] 이제 $p=3$ 의 경우와 같이 계수 측면에서 모든 차수의 다항식 $f \in \mathbb{Z}_p[x]$ 의 최소 조건을 찾는 방법을 설명한다. 다른 최소 다항식에 대해, 벡터 $[z_0, \dots, z_{13}] \bmod 7 = [1, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1]$ 를 취하면 같은 최소 조건을 충족하고 다음과 같은 최소 다항식을 얻을 수 있다.

[0523] $f(x) = 10x^{13} + 6x^{12} + 5x^{11} + 3x^9 + 6x^8 + 2x^7 + x^6 + 5x^5 + 13x^4 + 13x^2 + 8x + 8,$

[0525] 위 최소 다항식의 단일 사이클 레도 모듈로 7^2 은 다음과 같이 주어진다.

[0527] $(0, 8, 38, 16, 46, 40, 41, 21, 29, 10, 37, 18, 12, 20, 42, 1, 31, 9, 39, 33, 48, 14, 22, 3, 30, 11, 5, 27, 35, 43, 24, 2, 32, 26, 6, 7, 15, 45, 23, 4, 47, 34, 28, 36, 17, 44, 25, 19, 13).$

[0529] 이제 $p=3$ 의 경우와 같이 계수 측면에서 모든 차수의 다항식 $f \in \mathbb{Z}_p[x]$ 의 최소 조건을 찾는 방법을 설명한다. 차수 $d \geq 2p$ 다항식 $f(x) = a_0 + a_1x + \dots + a_dx^d \in \mathbb{Z}_p[x]$ 에 대해 상수 $B_0, \dots, B_{p-1}, D_0, \dots, D_{p-1}$ 을 다음과 같이 설정한다.

$$\begin{aligned} a_0 &= B_0; \\ \sum_{i>0, i \equiv 1 \pmod{p-1}} a_i &= B_1; \\ \sum_{i>0, i \equiv 2 \pmod{p-1}} a_i &= B_2; \\ &\vdots \\ \sum_{i>0, i \equiv 0 \pmod{p-1}} a_i &= B_{p-1}; \\ a_1 &= D_0; \\ \sum_{i=1}^d i a_i &= D_1; \\ &\vdots \\ \sum_{i=1}^d i(p-1)^{i-1} a_i &= D_{p-1}, \end{aligned} \tag{34}$$

[0530]

[0531] 최대 $2p-1$ 차수의 다항식의 경우와 같이 (34)의 방정식은 주어진 상수 열 벡터 $\mathbf{b} = [B_0, \dots, B_{p-1}, D_0, \dots, D_{p-1}]^t$ 모듈로 p 에 대해 변수 $\mathbf{x} = [a_0, \dots, a_d]^t$ 의 아래와 같은 선형 시스템으로 간주된다.

$$\tilde{M}x \equiv b \pmod{p}, \quad (35)$$

이 때, $\tilde{M}$ 은 $\tilde{M} = [MM']$ 형태의 $2p \times (d+1)$ 계수 행렬이고, M 은 (28)의 $2p \times 2p$ 행렬 이고, M' 은 나머지 $2p \times (d-2p-1)$ 부분 행렬이다. 우리는 M 모듈로 p 가 특정 패턴을 가지고 있음을 관찰한다. 실제로 B_i 에 해당하는 부분 행렬의 첫 번째 열을 제외한 모든 열은 주기 길이가 $p(p-1)$ 인 D_i 에 해당하는 부분 행렬이 주기적 길이 $p-1$ 로 주기적으로 나타난다. 왜냐하면 $i \equiv j \pmod{p(p-1)}$ 이면 $\alpha \in 1, \dots, p-1$ 에 대해 $i\alpha^{i-1} \equiv j\alpha^{j-1} \pmod{p}$ 이기 때문이다. 이러한 이유로, 필요한 경우 계수가 0인 항을 더하여 f 의 차수가 $d = p(p-1)k + 2p-1$ 이라고 가정할 수 있다. 상술한 바와 같이 명제 6. 1.의 조건 (i) 및 (ii)를 충족하는 상수 열 벡터 b 에 대해 정확히 $(p-1)!(p-1)^{p-1}$ 개의 선택 항목이 있다. 잘 선택된 b 에 대해, 증가된 계수 행렬의 축소된 행 사다리꼴은 $[L_{2p}R|E]$ 형태의 행렬로 주어진다. 이 때, L_p 는 $2p \times 2p$ 항등 행렬이고, R 과 E 는 각각 M' 과 b 의 축소된 부분이다. $\tilde{M}$, $R = (R_{ij})$ 의 패턴으로 인해 첫 번째 $p(p-1)$ 열 벡터가 열 순서에서 정확히 k 번 나타나는 특정 패턴이 있다. 따라서 관련 선형 시스템에 대한 매개변수 표현은 다음 형식의 방정식으로 제공된다.

$$\begin{aligned} a_0 &= e_0 + pz_0; \\ a_1 &= e_1 + pz_1; \\ a_2 &= e_2 + pz_2 - \sum_{j \in J_2} a_j R_{2j}; \\ &\vdots \\ a_{2p-1} &= e_{2p-1} + pz_{2p-1} - \sum_{j \in J_{2p-1}} a_j R_{(2p-1)j}, \end{aligned} \quad (36)$$

이 때, $[e_0, \dots, e_{2p-1}]^t = E$ 와 각 $0 \leq i \leq 2p-1$ 에 대해 인덱스 집합 J_i 는 $J_i = \{j | 2p+1 \leq j \leq d+1 \text{ and } R_{ij} \not\equiv 0 \pmod{p}\}$ 로 정의된다. J_i 는 $i=0,1$ 에 대한 공집합이다.

(36)에서 이러한 관계를 $f(x)$ 로 대체하면 다음과 같다.

$$f(x) = f_0(x) + pf_1(x), \quad (37)$$

$$\text{이 때, } f_0(x) = \sum_{j=0}^{2p-1} e_j x^j,$$

$$f_1(x) = \sum_{j=0}^{2p-1} z_j x^j + \frac{1}{p} \sum_{j=2p}^d a_j h_j(x), \quad (38)$$

이다.

이 때, h_j 는 계수가 a_j 인 0이 아닌 항을 수집하여 얻은 다항식이다. 다항식 f_0 은 전이 모듈로 p 이므로 f_0 은 다 음 속성을 만족한다.

$$f(x) \equiv f_0(x) \pmod{p}; \quad f'(x) \equiv f'_0(x) \pmod{p}.$$

따라서, (31)에서와 같이 f 가 최소가 되려면 그 것의 최소 조건이 다음의 0이 아닌 모듈로 p^2 을 만족하여야 한다. 이 때, (24)와 같이 $1 \leq i \leq p-2$ 과 $w_{p-1}=1$ 에 대해 $w_i = \prod_{j=i+1}^{p-1} f'_0(f_0^j(0))$ 이다. (36)의 pz_i 를 (39)로 대체하면 f 에 대한 최소 조건이 제공되며, 이는 계수로 표현된다. (23)에서와 같이 (39)에서 f 의 최소 조건은 다음 선형 다항식의 0이 아닌 모듈로 p 에 의해 주어진다.

$$l(z_0, \dots, z_d) = \frac{1}{p} f_0^p(0) + \frac{1}{f'_0(0)} z_0 + \sum_{i=1}^{p-1} w_i f_1(f_0^i(0)) \pmod{p}, \quad (40)$$

이 때, w_i 는 위와 같이 주어진다. 위와 같은 논의는 다음과 같은 결과로 요약된다.

정리 6.5.

다항식 $f(x) = a_0 + a_1x + \dots + a_dx^d \in \mathbb{Z}/p\mathbb{Z}[x]$ 는 오직 다음과 같을 때 최소이다.

$$f(x) = f_0(x) + pf_1(x),$$

이 때,

(i) $f_0(x) = \sum_{i=0}^{2p-1} e_i x^i \in \mathbb{Z}/p\mathbb{Z}[x]$ 는 정리 6.2.의 (i)과 같이 결정되고,

(ii) (38)의 다항식 $f_1(x)$ 는 (40)의 $l(z_0, \dots, z_d)$ 선형 다항식의 0이 아닌 모듈로 p 를 충족한다.

모든 최소 다항식 $f \in \mathbb{Z}_p[x]$ 는 전체 길이의 순열 F_p 의 φ 를 유도하므로 임의의 차수의 최소 다항식을 찾는 작업은 먼저 다음과 같은 라그랑주 보간 공식으로 얻은 축소 함수 모듈로 p 의 계수 벡터 $[B_0, \dots, B_{p-1}] \pmod{p}$ 를 찾는 것이다.

$$f_\varphi(x) = \sum_{\alpha \in \mathbb{F}_p} \varphi(\alpha)(1 - (x - \alpha)^{p-1}). \quad (41)$$

실제로, 이 공식을 사용하여 각 j 에 대해, B_j 는 다음과 같이 주어진다.

$$B_j = - \sum_{\alpha \in \mathbb{F}_p} \varphi(\alpha) \alpha^{p-1-j}.$$

[0569]

[0571] 다음으로, 명제 6.1.의 조건 (ii)를 만족하고 이들 $p-1$ 이 0이 아닌 요소를 무작위로 선택한 후 곱 $D_0 \cdots D_{p-2}$ 의 역 모듈로 p 를 찾음으로써 쉽게 수행될 수 있는 벡터 $[D_0, \dots, D_{p-1}] \pmod{p}$ 를 선택한다. 명제 6.1의 조건 (i) 및 (ii)를 만족하는 모든 $(p-1)!(p-1)^{p-1}$ 의 상수 벡터 $\mathbf{b} = [B_0, \dots, B_{p-1}, D_0, \dots, D_{p-1}]^t$ 의 목록이 완전히 발견되면 계수와 관련하여 다항식 $f \in \mathbb{Z}_p[x]$ 에 대한 가능한 모든 최소 조건의 전체 목록을 찾을 수 있다. 주어진 다항식 $g \in \mathbb{Z}_p[x]$ 가 최소인지 결정하는 것이 중요하다. 이를 위해 δ 로 축소를 통해 g 에 대한 $f(x)$ 의 나머지를 찾기 위한 정리 3.1.을 사용한다.

[0572] R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, 1997.의 정리 7.4. 또는 본 명세서의 정리 6.9의 기준을 사용하여 $f(x)$ 가 전단사 모듈로 p 인지 아닌지를 결정하고, 그것이 전체주기인지 여부를 결정한다. 만약 그렇다면 $x = 0, \dots, p-1$ 에서 그것의 파생물을 찾아 f 가 명제 6.1.의 조건 (ii)를 충족하는지 여부를 확인해야 한다. f 가 이 과정을 통과하면 얻은 벡터 $\mathbf{b}$ 에 대해 (27)의 선형 시스템을 풀면 f_0 을 찾을 수 있다. f_0 을 사용하여 f_1 을 찾은 후 f 가 (23)의 최소 조건을 충족하는지 확인할 수 있다. 그렇다면 f (따라서 g)는 최소로 선언된다. 이제 유한 소수 체 위의 순열 다항식 F_p 에 대한 헤르마이트 기준을 진술한다.

[0574] **정리 6.9.**(Hermite`s Criterion)

[0575] F_p 를 소수 필드라고 하면 $f \in F_p[x]$ 는 다음 두 조건을 유지할 때 F_p 위의 순열 다항식이라고 한다.

[0576] (i) f 는 정확히 F_p 에서 하나의 루트를 가진다. 그리고,

[0577] (ii) $1 \leq t \leq p-1$ 인 각 정수에 대해, $f(x)^{t \bmod (x^p - x)}$ 의 축소는 $p-2$ 이하의 차수를 가진다.

[0579] **따름정리 6.10.**

[0580] 만약, $d > 1$ 이 $p-1$ 의 제수이면 $\mathbb{Z}_p$ 에서 차수 d 에 대한 최소 다항식이 존재하지 않는다.

[0582] 증명. 그러한 최소 다항식이 존재한다고 가정한다. 그러면 그것은 풀 사이클의 순열 다항식 모듈로 p 이다. 그러나 이러한 순열 다항식은 R. Lidl and H. Niederreiter, Finite Fields, Cambridge University Press, 1997.의 따름 정리 7. 5.의 헤르마이트의 기준에서 존재하지 않는다. 따라서 증명이 되었다.

[0584] **예제 2.** 29차 다항식 $f(x) = \sum_{i=0}^{29} a_i x^i \in \mathbb{Z}_5[x]$ 의 최소 조건을 찾기 위해 위에서 기술한 조건 $\mathbf{b} = [B_0, \dots, B_{p-1}, D_0, \dots, D_{p-1}]^t \pmod{5} = [2 \ 1 \ 0 \ 0 \ 0 \ 1 \ 4 \ 4 \ 1 \ 1]$ 에 대해 위에서 설명한 방법을 사용한다. (35)의 확대 계수 행렬의 축소된 행 사다리꼴 형식에서 매개변수 표현은 다음 방정식으로 제공된다.

$$\begin{aligned}
 a_0 &= 2 + 5z_0; \\
 a_1 &= 1 + 5z_1; \\
 a_2 &= 3 + 5z_2 + a_{10} + 2a_{14} + 3a_{18} + 4a_{22}; \\
 a_3 &= 0 + 5z_3 + a_{11} + 2a_{15} + 3a_{19} + 4a_{23}; \\
 a_4 &= 1 + 5z_4 + a_{12} + 2a_{16} + 3a_{20} + 4a_{24}; \\
 a_5 &= 4 + 5z_5 + a_{13} + 2a_{17} + 3a_{21} + 4a_{25}; \\
 a_6 &= 2 + 5z_6 + 3a_{10} + 2a_{14} + a_{18} + 4a_{26}; \\
 a_7 &= 0 + 5z_7 + 3a_{11} + 2a_{15} + a_{19} + 4a_{27}; \\
 a_8 &= 4 + 5z_8 + 3a_{12} + 2a_{16} + a_{20} + 4a_{28}; \text{ and} \\
 a_9 &= 1 + 5z_9 + 3a_{13} + 2a_{17} + a_{21} + 4a_{29}.
 \end{aligned} \tag{42}$$

[0586]

[0587] 따라서, $f(x) = f_0(x) + 5f_1(x)$, 이 때,

[0588] $f_0(x) = 2 + x + 3x^2 + x^4 + 4x^5 + 2x^6 + 4x^8 + x^9$ 이고,

[0589] $f_1(x) = \sum_{i=0}^9 z_i x^i + \frac{1}{5} \sum_{i=10}^{29} a_i h_i(x)$,
 이며, 이 때, $2 \leq i \leq 5$ 에 대해,

[0590] $h_{8+i}(x) = x^i + 3x^{4+i} + x^{8+i}, h_{12+i}(x) = 2x^i + 2x^{4+i} + x^{12+i}, h_{16+i}(x) = 3x^i + x^{4+i} + x^{16+i}$ 이고, $2 \leq i \leq 9$ 에 대해,

$h_{20+i}(x) = 4x^i + x^{20+i}$ 이다. $f_0 \equiv 2 + x \pmod{5}$ 의 계도 mod 5는 (0 2 4 1 3)에 의해 주어지고,

[0591] $[f'_0(0), f'_0(1), f'_0(2), f'_0(3), f'_0(4)] \pmod{5} = [1, 4, 4, 1, 1]$ 이기 때문에 $[w_1, w_2, w_3, w_4] \pmod{5} = [4, 4, 1, 1]$ 을 얻는다. 따라서, (39)에 의해 다음을 얻는다.

[0592] $f^5(0) \equiv 5 + 5f_1(0) + 5f_1(1) + 20f_1(2) + 5f_1(3) + 20f_1(4) \pmod{5^2}.$

[0594] $0 \leq \alpha \leq 4$ 와 $i \geq 10$ 에 대하여 $h_i(\alpha)$ 모듈로 5^2 은 다음과 같이 계산하기 쉽다.

$$\begin{aligned}
 f^5(0) &\equiv 5a_{11} + 15a_{13} + 5a_{15} + 15a_{17} + 5a_{19} + 15a_{21} + 5a_{23} + 15a_{25} + 5a_{27} \\
 &\quad + 15a_{29} + 5z_0 + 15z_1 + 5z_3 + 15z_5 + 5z_7 + 15z_9 + 5 \pmod{5^2}.
 \end{aligned}$$

[0596]

[0598] (42)의 $5z_i$ 를 위의 방정식으로 대체하면 다음과 같은 f 의 최소 조건이 생성된다.

$$\begin{aligned}
 a_0 + 3a_1 + a_3 + 3a_5 + a_7 + 3a_9 + a_{11} + 3a_{13} + a_{15} + 3a_{17} + a_{19} \\
 + 3a_{21} + a_{23} + 3a_{25} + a_{27} + 3a_{29} + 10 \not\equiv 0 \pmod{5^2}.
 \end{aligned} \tag{43}$$

[0600]

[0602] (42)와 (43)의 조건을 만족하는

[0603] $[a_0, \dots, a_{29}] = [2, 1, 26, 3, 28, 14, 19, 13, 29, 23, 0, 1, 2, 0, 3, 1, 2, 0, 3, 0, 3, 2, 2, 0, 3, 1, 2, 2, 3, 5]$ 을 취하면, 29차수의 최소 다항식 f 는 다음과 같이 주어지고,

$$f(x) = 5x^{29} + 3x^{28} + 2x^{27} + 2x^{26} + x^{25} + 3x^{24} + 2x^{22} + 2x^{21} + 3x^{20} + 3x^{18} + 2x^{16} + x^{15} + 3x^{14} + 2x^{12} + x^{11} + 23x^9 + 4x^8 + 13x^7 + 19x^6 + 14x^5 + 3x^4 + 3x^3 + x^2 + x + 2, \quad (44)$$

그것의 단일 사이클 궤도 모듈로 5^2 은 다음과 같이 결정된다.

$$(0, 2, 4, 16, 3, 20, 22, 9, 21, 23, 15, 17, 14, 1, 18, 10, 12, 19, 6, 13, 5, 7, 24, 11, 8).$$

주어진 다항식 $g \in \mathbb{Z}_p[x]$ 가 최소인지 결정하는 것이 중요하다. 이를 위해 δ 로 축소를 통해 g 에 대한 $f(x)$ 의 나머지를 찾기 위한 정리 3.1.을 사용함에 따라 (44)의 다항식이 최소임을 다시 보여주도록 한다. 위 다항식을 $\binom{x}{10}$ 으로 나누면 그것의 나머지는 다음과 같은 축소된 모듈로 25가 된다.

$$f(x) = 6x^9 + 24x^8 + 5x^7 + 2x^6 + 24x^5 + 21x^4 + 15x^3 + 3x^2 + 16x + 2.$$

정리 6.2.으로부터 f 는 다음과 같은 합으로 분해되고 $f = f_0 + 5f_1$, 이 때,

$$f_0 = x^9 + 4x^8 + 2x^6 + 4x^5 + x^4 + 3x^2 + x + 2 \quad \text{이고,}$$

$$f_1 = x^9 + 4x^8 + x^7 + 4x^5 + 4x^4 + 3x^3 + 3x \quad \text{이다.}$$

이 분해를 사용하여 (23)에 의해 f 의 최소 조건은 $l(z_0, \dots, z_9) = z_0 + 1$ 의 0이 되지 않는 모듈로 5에 의해 결정된다. f_1 의 계수가 이 조건을 충족하기 때문에 f 는 최소이므로 (44)의 다항식도 마찬가지로이다.

전술한 본 발명의 설명은 예시를 위한 것이며, 본 발명이 속하는 기술분야의 통상의 지식을 가진 자는 본 발명의 기술적 사상이나 필수적인 특징을 변경하지 않고서 다른 구체적인 형태로 쉽게 변형이 가능하다는 것을 이해할 수 있을 것이다. 그러므로 이상에서 기술한 실시 예들은 모든 면에서 예시적인 것이며 한정적이 아닌 것으로 이해해야만 한다. 예를 들어, 단일형으로 설명되어 있는 각 구성 요소는 분산되어 실시될 수도 있으며, 마찬가지로 분산된 것으로 설명되어 있는 구성 요소들도 결합된 형태로 실시될 수 있다.

본 발명의 범위는 상기 상세한 설명보다는 후술하는 특허청구범위에 의하여 나타내어지며, 특허청구범위의 의미 및 범위 그리고 그 균등 개념으로부터 도출되는 모든 변경 또는 변형된 형태가 본 발명의 범위에 포함되는 것으로 해석되어야 한다.

도면

도면1

