제 4 장 정수론의 기본 개념과 유한체

❑ 목 차

- 모듈러 연산은 정수 연산의 한 종류
  - 모든 숫자를 어떤 숫자 n에 대한 하나의 집합으로 단축

- 두 정수의 최대공약수란 두 정수를 나누는 가장 큰 양의 정수

- 유한체 이론은 암호학의 여러 분야에서 매우 중요하게 사용됨
  - 유한체
    - 유한개의 원소를 가지는 체
    - 유한체의 위수는 n이 양의 정수일 때, 소인수의 멱승인 p^n

4.1 가분성(Divisibility)과 호제법(Division Algorithm)

❑ 가분성(可分性, Divisibility)

- ❖ a, b, m 이 정수이고 b가 0이 아닐 때, 임의의 수 m에 대해서
  a = mb가 성립한다면, b가 a를 '나눈다'라고 함
- ❖ 즉, 나눗셈 연산 후, 나머지가 0이면 'b가 a를 나눈다'라고 함
- ❖ b | a 는 b가 a를 나누는 것을 표현할 때, 주로 사용되는 표기법
- ❖ b | a 이면 b는 a의 약수

> 24의 양의 약수는 1,2,3,4,6,8,12,24이다.
> 13 | 182; -5 | 30; 17 | 289; -3 | 33; 17 | 0

❑ 나누어짐의 특성

- ❖ 만약 a | 1이면 a = 1이다
- ❖ 만약 a | b이고 b | a이면, a = ±b이다
- ❖ 만약 a | b 이고 b | c 이면, a | c이다.

4.1 가분성(Divisibility)과 호제법(Division Algorithm)

❑ 나누어짐의 특성

- ❖ 만약 b | g이고 b | h이면, 임의의 정수m과 n에 대해서 **b | (mg + nh)**이다.
  - ➢ 위의 특성은 다음과 같은 과정을 통해 만족함을 알 수 있음
    - 만약 b | g이면 g = b × g1이 되는 정수 g1이 존재한다.
    - 만약 b | h이면 h = b × h1이 되는 정수 h1이 존재한다.
    - 따라서, $mg + nh = mbg_1 + nbh_1 = b \times (mg_1 + nh_1)$ 이며, 그러므로 b는 mg + nh를 나눈다.

b = 7; g = 14; h = 63; m = 3; n = 2,
7 | 14 이고 7 | 63
7 | (3 × 14 + 2 × 63) 임을 보이려면,
(3 × 14 + 2 × 63) = 7(3 × 2 + 2 × 9)이므로,
7 | (7(3 × 2 + 2 × 9))이다.

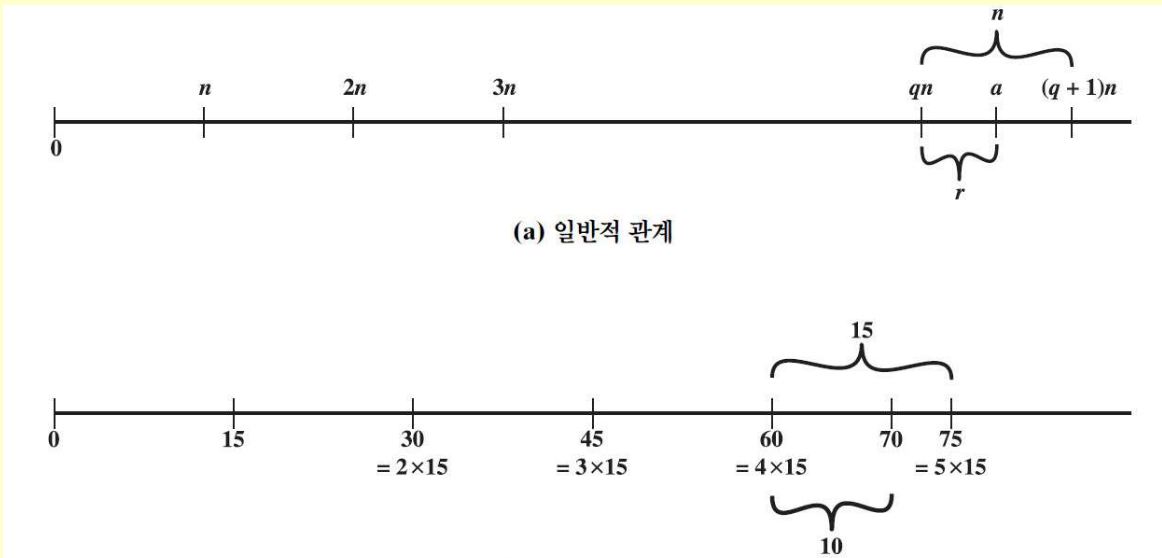
4.1 가분성(Divisibility)과 호제법(Division Algorithm)

❑ 호제법(The Division Algorithm)

❖ 임의의 양의 정수 n과 음의 정수가 아닌 정수 a에 대하여, n이 a를 나눈다면, 정수인 몫(quotient) q와 정수인 나머지(remainder) r이 존재하며, 다음의 관계식이 성립

$$a = qn + r \qquad 0 \le r < n;\ q = \lfloor a/n \rfloor \quad (4.1)$$

❖ $\lfloor x \rfloor$는 x보다 작거나 같은 가장 큰 정수이며, 위의 식을 호제법



(a) 일반적 관계

(b) 예제: 70 = (4 × 15) + 10

$a = qn+r;\ 0 \le r < n$ 의 관계

4.2 유클리드 호제법(Euclidean Algorithm)

❑ 정수론의 기본적 기술

- ❖ 두 양의 정수에 대한 최대공약수를 결정하기 위한 수행 절차
- ❖ 서로소(relatively prime) : 공약수가 1 밖에 없는 두 정수

❑ 최대공약수(GCD : Greatest Common Divisor)

- ❖ gcd(a, b) : a와 b의 최대공약수를 의미
  - ➢ 최대공약수 : a와 b를 모두 나누는 가장 큰 정수
- ❖ 다음을 만족할 경우 c는 a와 b의 최대공약수
  1. c는 a와 b의 약수
  2. a와 b에 대한 모든 공약수는 c의 약수

  → gcd(a, b) = max[k, $k \mid a$ 이고 $k \mid b$일 때] 로 나타낼 수 있음

❑ 최대공약수(Greatest Common Divisor)

❖ 양수인 최대공약수를 구하기 때문에 gcd(a, b) = gcd(a, -b) = gcd(-a, b) = gcd(-a, -b) 가 성립. 즉, gcd(a, b) = gcd(|a|, |b|)

gcd(60, 24) = gcd(60, -24) = 12

❖ 모든 0이 아닌 정수들은 0을 나누기 때문에 다음 식

gcd(a, 0) = |a| 이 성립

❖ 정수 a와 b가 공약수가 1밖에 없다면, a와 b는 서로소

➢ gcd(a, b) = 1이면, a와 b는 서로소

8과 15는 서로소이다. 왜냐하면 8은 1, 2, 4, 8을 약수로 가지며, 15의 약수는 1, 3, 5, 15를 갖는데, 이때 8과 15의 두 약수 목록에 모두 포함된 수는 1뿐이기 때문이다.

❑ 최소공배수(Least Common Multiple)

4.3 모듈러 연산(Modular Arithmetic)

❑ 법(The Modulus)

- ❖ 임의의 정수 a와 양의 정수 n에 대하여 a mod n을 a를 n으로 나눈 나머지로 정의하고, 이 때 n을 법(法)이라고 함
- ❖ 모든 정수 a에 대하여 다음과 같이 나타낼 수 있음

$$a = qn + r \qquad 0 \le r < n;\ q = \lfloor a/n \rfloor$$

$$a = \lfloor a/n \rfloor \times n + (a \bmod n)$$

$$11 \bmod 7 = 4; \qquad -11 \bmod 7 = 3$$

$$73 \equiv 4 \pmod{23}; \qquad 21 \equiv -9 \pmod{10}$$

- ❖ 만약 (a mod n) = (b mod n)이면, a ≡ b (mod n) 이라 할 수 있음
  - ➢ 이 경우 두 정수 a와 b는 법 n에 대해 합동(congruence 合同)이라 함
  - ➢ 만약 a ≡ 0 (mod n)이면, n | a 임

4.3 모듈러 연산(Modular Arithmetic)

❑ 합동에 관한 기본 특성(Properties of Congruence)

❖ 모듈러 연산은 다음과 같은 특성을 가짐

- 만약 $n \mid (a - b)$이면 $a \equiv b \bmod n$
  - $n|(a-b)$ ➔ $(a-b) = kn$ ➔ $a = kn + b$
  - 예) $23 = 8 \bmod 5$ ➔ $5|\ (23-8)$

- $a \equiv b \bmod n$은 $b \equiv a \bmod n$ 의 의미를 포함

- $a \equiv b \bmod n$이고 $b \equiv c \bmod n$이면 $a \equiv c \bmod n$
  - 예) $9 = 16 \bmod 7$, $16 = 23 \bmod 7$ ➔ $9 = 23 \bmod 7$

4.3 모듈러 연산(Modular Arithmetic)

- 모듈러 산술 연산 (Modular Arithmetic Operations)
  - mod n 연산자는 모든 정수들을 정수들의 집합 {0, 1,…,(n-1)}으로 표현할 수 있음
  - 이러한 기법을 **모듈러 연산(modular arithmetic)**이라 함
  - 모듈러 연산의 특성
    - [(a mod n) + (b mod n)] mod n = (a + b) mod n
    - [(a mod n) - (b mod n)] mod n = (a - b) mod n
    - [(a mod n) × (b mod n)] mod n = (a × b) mod n
- 11 = mod 8 = 3, 15 mod 8 =7
  - [11 mod 8) + (15 mod 8)] mod 8 = (3+7) mod 8 = 10 mod 8 = 2
    (11+15) mod 8 = 26 mod 8 = 2
  - [11 mod 8) - (15 mod 8)] mod 8 = (3-7) mod 8 = -4 mod 8 = 4
    (11-15) mod 8 = -4 mod 8 = 4
  - [11 mod 8) * (15 mod 8)] mod 8 = (3 * 7) mod 8 = 21 mod 8 = 5
    (11*15) mod 8 = 165 mod 8 = 5

4.3 모듈러 연산(Modular Arithmetic)

❑ 모듈러 연산의 특성(Properties of Modular Arithmetic)

- ❖ n보다 작은 음이 아닌 정수들의 집합을 Zn이라 정의

$$Z_n = \{0, 1, 2, 3, \ldots, (n-1)\}$$

- ❖ modulo n 상에서의 잉여집합(set of residues) 또는 잉여류(residue classes)를 나타냄
- ❖ 다음을 만족할 때, 모듈러 n의 잉여류를 ([0], [1], [2], . . . , [n - 1]) 로 표기할 수 있음

$$[r] = \{a: a\text{는 정수 } a \equiv r \pmod{n}\}$$

mod 4의 잉여류는 다음과 같다.

$$[0] = \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}$$
$$[1] = \{\ldots, -15, -11, -7, -3, 1, 5, 9, 13, 17, \ldots\}$$
$$[2] = \{\ldots, -14, -10, -6, -2, 2, 6, 10, 14, 18, \ldots\}$$
$$[3] = \{\ldots, -13, -9, -5, -1, 3, 7, 11, 15, 19, \ldots\}$$

4.3 모듈러 연산(Modular Arithmetic)

❑ 모듈러 연산의 특성(Properties of Modular Arithmetic)

- ❖ 잉여류의 모든 정수들 중에 음이 아닌 가장 작은 정수가 잉여류를 나타내기 위해 사용됨
- ❖ modulo n에서 k와 합동인 음이 아닌 가장 작은 정수를 찾는 작업을 k를 modulo n으로 환산한다라고 부름
- ❖ 만약 Z_n에 대하여 모듈러 산술연산을 수행한다면, Z_n상의 정수들은 아래 표에 기술된 속성을 만족함

특성	표현
교환 법칙	$(w + x) \bmod n = (x + w) \bmod n$ $(w \times x) \bmod n = (x + w) \bmod n$
결합 법칙	$[(w + x) + y] \bmod n = [w + (x + y)] \bmod n$ $[(w \times x) \times y] \bmod n = [w \times (x \times y)] \bmod n$
분배 법칙	$[w \times (x + y)] \bmod n = [(w \times x) + (w \times y)] \bmod n$
항등	$(0 + w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$
덧셈에 대한 역원($-w$)	각 $w \in Z_n$에 대하여, $w + z \equiv 0 \bmod n$을 만족하는 z가 존재

4.3 모듈러 연산(Modular Arithmetic)

- 항등원(恒等元 identity element)
  - 대수학에서 다루는 기본적인 개념으로, 집합의 어떤 원소와 연산을 취해도, 자기 자신이 되는 원소

- 역원(inverse element)
  - 집합 G에서 어떤 결합법 ○(2항연산)을 생각할 때,
  - G의 임의의 원소 a에 대하여 a○a'=a'○a=e(e는 항등원)가 되는
  - a'가 단 1개 존재하면, a'를 연산 ○에 대한 a의 역원

  - 집합 G에서 정의된 결합법이 덧셈일 때는 a의 역원은 - a이고
  - 곱셈일 때는 a(≠0)의 역원은 1/a

4.3 모듈러 연산(Modular Arithmetic)

- 모듈러 연산의 특성(Properties of Modular Arithmetic)
  - 일반적인 연산과 구별되는 모듈러 연산의 특징

만약 $(a + b) \equiv (a + c) \pmod{n}$ 이라면, $b \equiv c \pmod{n}$ (*)

$(5+23) \equiv (5+7) \pmod{8}$; $23 \equiv 7 \pmod{8}$

- 식 (*)는 덧셈에 대한 역원이 존재함을 의미

  a에 대한 덧셈에 대한 역원을 식 (*) 의 양변에 더함으로써 다음과 같은 수식을 얻을 수 있음

$$((-a) + a + b) \equiv ((-a) + a + c) \pmod{n}$$

$$b \equiv c \pmod{n}$$

4.3 모듈러 연산(Modular Arithmetic)

❑ 모듈러 연산의 특성(Properties of Modular Arithmetic)

- ❖ 다음 수식은 추가적인 조건을 만족할 때 성립
  - ➢ 만약 (a × b) ≡ (a × c)(mod n)이라면, b ≡ c (mod n)이다. (**)
    - 단, a는 n과 서로소이다.
- ❖ 서로소란 공약수가 1뿐인 두 정수를 의미함
- ❖ 식(*)와 비슷하게 식(**)는 곱셈에 대한 역원이 존재한다고 할 수 있음
- ❖ a에 대한 곱셈의 역원을 식(**)의 양변에 곱함
  - ➢ $((a^{-1})ab) \equiv ((a^{-1})ac)(\text{mod } n)$
  - ➢ $b \equiv c(\text{mod } n)$

이것을 알아보기 위해 식 (4.2)의 조건을 만족하지 않는 예를 들어보자. 여기서 정수 6과 8은 서로 소가 아니다. 6과 8의 공약수 2를 기반으로 다음과 같이 기술할 수 있다.

$$6 \times 3 = 18 \equiv 2 \ (\text{mod } 8)$$

$$6 \times 7 = 42 \equiv 2 \ (\text{mod } 8)$$

그러나 $3 \not\equiv 7 \text{ mod } 8$이다.

이러한 결과의 이유는 일반적인 법 n에 대해 만약 a와 n이 공통적으로 어떠한 인수를 가지고 있다면, 정수 0에서부터 $(n - 1)$까지 차례대로 a에 대한 곱셈을 적용시키더라도 완전한 형태의 나머지 집합이 구성되지 않기 때문이다.

❑ 산술 모듈러 8

+	0	1	2	3	4	5	6	7
0	0	1	2					
1	1	2	3					
2	2	3	4					
3								
4								
5								
6								
7								

*	0	1	2	3	4	5	6	7
0	0	0	0					
1	0	1	2					
2	0	2	4					
3								
4								
5								
6								
7								

W	−W	W^{-1}
0		
1		
2		
3		
4		
5		
6		
7		

$a * X_i \bmod n$

- a=6과 n=8일 경우

Zn	0	1	2	3	4	5	6	7
6 의 곱	0	6	12	18	24	30	36	42
나 머 지	0	6	4	2	0	6	4	2

- a=5과 n=8일 경우

Zn	0	1	2	3	4	5	6	7
5 의 곱	0	5	10	15	20	25	30	35
나 머 지	0	5	2	7	4	1	6	3

a * X_i mod n

- a=4과 n=8일 경우

Zn	0	1	2	3	4	5	6	7
4 의 곱								
나 머 지								

- a=7과 n=8일 경우

Zn	0	1	2	3	4	5	6	7
7 의 곱								
나 머 지								

4.3 모듈러 연산(Modular Arithmetic)

❑ 최대 공약수(greatest common divisor)

- ❖ a와 b의 최대 공약수의 경우, gcd(a, b)로 표현
- ❖ 양의 정수 c가 다음을 만족하면, 양의 정수 c는 a와 b의 최대 공약수이다
  - ➢ c는 a와 b의 약수이다.
  - ➢ a와 b에 대한 어떠한 약수는 c의 약수이다 .
- ❖ gcd(a,b) = max [k, 이때의 k는 k | a 이고, k | b 이다]
- ❖ gcd(a,b) = gcd(a,-b) = gcd(-a,b) = gcd(-a,-b)
- ❖ gcd(60,24) = gcd(60,-24) = 12

- ❖ gcd(a,0) = a
- ❖ gcd(a,b) = 1 이라면 a와 b는 서로소이다.

4.3 모듈러 연산(Modular Arithmetic)

❑ 유클리드 알고리즘

- ❖ 두 양의 정수에 대하여 최대 공약수를 결정하기 위한 절차
- ❖ 최대 공약수 찾기
  - ➢ gcd(a, b) = gcd(b, a mod b)
  - ➢ gcd(55, 22) = gcd(22, 55mod 22) = gcd(22, 11) = gcd(0, 11) = 11
  - ➢ gcd (18,12) = gcd(12, 6) = gcd(6,0) = 6
  - ➢ gcd(11,10) = gcd(10, 1) = gcd(1,0) = 1
- ❖ 알고리즘

$$r_0 = a_0 r_1 + r_2$$

$$r_1 = a_1 r_2 + r_3$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$r_{n-1} = a_{n-1} r_n + r_{n+1}$$

$$r_n = a_n r_{n+1}$$

4.3 모듈러 연산(Modular Arithmetic)

- gcd(a,0) = a
- gcd(a,b) = 1 이라면 a와 b는 서로소이다.

- gcd(128, 36)
  - 128 = 3* 36 + 20 gcd(36, 20)
  - 36 = 1* 20 + 16 gcd(20, 16)
  - 20 = 1* 16 + 4 gcd(16, 4)
  - 16 = 4* 4 + 0 gcd(4, 0)

- 그러므로 gcd(128, 36)= 4이다

4.3 모듈러 연산(Modular Arithmetic)

- gcd(1970, 1066)는???

4.3 모듈러 연산(Modular Arithmetic)

- ❖ gcd(a,0) = a
- ❖ gcd(a,b) = 1 이라면 a와 b는 서로소이다.

❑ gcd(37, 25)

- ❖ 37 = 1* 25 + 12 gcd(25,12)
- ❖ 25 = 2* 12 + 1 gcd(12, 1) =1
- ❖ 37과 25는 서로소이다.

❑ Gcd(47, 22)

- ❖ 47 = 2* 22 + 3 gcd(22, 3)
- ❖ 22 =7* 3 + 1 gcd(3, 1) = 1
- ❖ 47과 22는 서로소이다

Quiz

- ❑ 유클리드 알고리즘을 이용하여 다음의 최대 공약수를 구하시오.
  - ❖ gcd(24, 36)
  - ❖ gcd(4655, 12075)
  - ❖ gcd(24140, 16762)

- ❑ GF(5)에 대한 산술 테이블을 완성하시오.

+	0	1	2	3	4
0					
1					
2					
3					
4					

*	0	1	2	3	4
0					
1					
2					
3					
4					

4.4 군(Groups), 환(Rings), 체(Fields)

❑ 군(Groups)

- ❖ 군 *G* 는 {*G*, •} 로 정의 내림
- ❖ 이항연산 원소의 집합임

군(Groups)의 성질

✓(A1) **닫힘**: 만약 *a*와 *b*가 군*G*에 속할 경우 *a* • *b*도 군*G*에 속한다.
✓(A2) **결합 법칙**: 군*G*의 모든 *a*, *b*, *c*에 대하여 *a* • (*b* • *c*) = (*a* • *b*) • *c*가 성립한다.
✓(A3) **항등원소**: 군 *G*의 모든 *a*에 대하여 *a* • *e* = *e* • *a* = *a*와 같은 *G*의 항등원소 *e*가 존재한다.(항등원 0)
✓(A4) **역원의 존재**: 군*G*의 모든 *a*에 대하여 *a* • *a*′ = *a*′ • *a* = *e*와 같은 군*G*에 역원 *a*′가 존재한다.(역원 –a)

위와 같은 4가지의 성질에 아래와 같은 성질을 만족할 경우, 해당 군을 아벨리안(abelian) 군이라 부른다.

✓(A5) **교환법칙**: 군*G*의 모든 *a*와 *b*에 대하여 *a* • *b* = *b* • *a*가 성립한다.

4.4 군(Groups), 환(Rings), 체(Fields)

❑ 환(Rings)

❖ 2개 이상의 이항연산(가법과 승법)을 가지는 원소의 집합임

환(Rings)의 성질

✓(A1~A5) *R*은 가법측면에서 아벨리안 군이다. 즉 *R*은 A1~A5까지의 원리를 만족한다.

✓가법군의 이러한 원리에 대하여 0과 *a*의 역원 -*a*로서 항등원을 나타낸다.

✓(M1) **승법에 닫힘**: 만약 *a*와 *b*가 환 R에 속할 경우 *ab* 역시 환 *R*에 속해 있다.

✓(M2) **승법의 결합 법칙**: 환 *R*의 모든 *a, b, c*에 대하여 $a(bc) = (ab)c$가 성립한다.

✓(M3) **분배 법칙**: 환 *R*의 모든 *a, b, c*에 대하여 $a(b + c) = ab + ac$와 $(a + b)c = ac + bc$ 가 성립한다.

환에서의 교환법칙이 성립하기 위해서는 다음과 같은 추가적인 사항을 만족해야 한다.

✓(M4) **승법의 교환법칙**: 환 *R*의 모든 *a*와 *b*에 대하여 $ab = ba$가 성립한다.

4.4 군(Groups), 환(Rings), 체(Fields)

❑ 체(Fields)

❖ 정역(integral domain)의 성질을 포함함

- ➢ (M5) 곱셈의 항등원: 환 R의 모든a에 대하여, a×1 = 1×a = a 이 성립하는 원소가 존재한다.
- ➢ (M6) 0으로 나눌 수 없다: 만약 a, b가 환 R에 속하고, ab = 0이면 a = 0이거나 b = 0이다.

체(Fields)의 성질

✓(A1~M6) 체 *F*가 정역일 경우 *F*는 A1~A5와 M1~M6의 명제를 만족한다.
✓(M7) 곱셈 역원: 체 *F*에서 0을 제외한 각 *a*에 대하여 $aa^{-1} = (a^{-1})a = 1$ 을 만족하는 원소 a^{-1}가 존재한다.

❑ 본질적으로 집합 원소들 간의 가법, 감법, 승법 및 제법 결과값에 대하여 닫혀있는 집합을 체F 라 함

4.5 GF(p)상의 유한체

❑ 위수 p인 유한체

- ❖ 유한체는 암호학 분야에서 유용하게 활용되고 있음
- ❖ 유한체의 위수(체의 원소의 개수)는 소인수의 멱승인 p^n이어야 함
- ❖ GF는 갈로아 필드(Galois field)라고 함
- ❖ GF(p^n)으로 표기함
- ❖ 주로 GF(p), GF(2^n)의 유한체를 사용함

$P^n \mod n$

❑ p=5과 n=8일 경우

Zn	0	1	2	3	4	5	6	7
5의 멱승	0	5	25	125	625	3125	15625	78125
나 머 지	1	5						

❑ p=5과 n=7일 경우

Zn	0	1	2	3	4	5	6
5 의 멱 승	0	5	25	125	625	3125	15625
나 머 지	1	5					

4.5 GF(p)상의 유한체

❑ 위수 p인 유한체

- ❖ 소수 p에 대해서 위수가 p인 유한체 GF(p)는 정수{0,1,…,p-1}의 집합 Z_p로 정의됨
  - ➢ 모듈러 p의 산술연산이 수행됨
- ❖ Z_p상의 0이 아닌 모든 정수들에 대하여 곱셈 역원이 존재함
- ❖ GF(p)의 각 원소에 대한 곱셈의 역원은 확장 유클리드 호제법을 사용하여 쉽게 구할 수 있음

Z_n의 모듈러 연산속성

- ✓교환법칙: $(w+x) \bmod n = (x+w) \bmod n$
- ✓결합법칙: $[(w+x)+y] \bmod n = [w+(x+y)] \bmod n$
- ✓분배법칙: $[w(x+y)] \bmod n = [(wx)+(wy)] \bmod n$
- ✓항등: $(0+w) \bmod n = w \bmod n$, $(1w) \bmod n = w \bmod n$
- ✓덧셈에 대한 역원: Z_n의 각 원소 w에 대하여, $w+z \equiv 0 \bmod n$ 만족하는 z 존재
- ✓곱셈에 대한역원: Z_n의 각 원소 w에 대하여 $wz \equiv 1 \bmod n$ 만족하는 z 존재

4.5 GF(p)상의 유한체

❑ 위수 p인 유한체

❖ 곱셈에 대한 역원(w^{-1})

$$\text{각 } w \in Z_n \text{에 대하여}, w * z \equiv 1 \bmod n \text{을 성립시키는 } z \text{이 존재}$$

❖ 덧셈에 대한 역원(-w)

$$\text{각 } w \in Z_n \text{에 대하여}, w + z \equiv 0 \bmod n \text{을 성립시키는 } z \text{이 존재}$$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

*	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

W	−W	W^{-1}
0	0	−
1	6	1
2	5	4
3	4	5
4	3	2
5	2	3
6	1	6

❑ 산술 모듈러 8

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

*	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

W	−W	W^{-1}
0	0	–
1	7	1
2	6	–
3	5	3
4	4	–
5	3	5
6	2	–
7	1	7

4.5 GF(p)상의 유한체

- GF(1759)에서 550에 대한 곱셈의 역원 찾기
- gcd(1759, 550) = 1
  - 1759 = 3* 550 + 109
  - 550 = 5* 109 + 5
  - 109 = 21* 5 + 4
  - 5 =1* 4 + 1

  - 1 = 5 - 1*4
  - 1 = 5 – 1 * (109-21*5) = -1*109 +22*5
  - 1 = -1* 109 + 22 * (550-5*109) = 22 * 550 -111*109
  - 1 = 22 * 550 – 111 *(1759 – 3*550) = -111*1759 +355*550
    - 그러므로 550의 역원은 355이다.
      - 550 * 355 = 195250 = 111 * 1759 1

4.5 GF(p)상의 유한체

- ❑ GF(43)에서 23에 대한 곱셈의 역원 찾기
- ❑ gcd(43, 23) = 1
  - ❖ 43 = 1* 23 + 20
  - ❖ 1 =

4.5 GF(*p*)상의 유한체

- GF(43)에서 23에 대한 곱셈의 역원 찾기
- gcd(43, 23) = 1
  - 43 = 1* 23 + 20
  - 23 = 1* 20 + 3
  - 20 = 6* 3 + 2
  - 3 =1* 2 + 1

  - 1 = 3 - 1*2
  - 1 = 3 – 1 * (20-6*3) = -1*20 +7*3
  - 1 = -1* 20 + 7 * (23-1*20) = 7 * 23 -8*20
  - 1 =7 * 23 – 8 *(43 – 1*23) = -8*43 + 15*23
    - 그러므로 23의 역원은 15이다.
      - 23 * 15 = 345 = 8 * 43 1

Quiz

- GF(57)에서 22에 대한 곱셈의 역원은??

- GF(231)에서 17에 대한 곱셈의 역원은??