

기초 정수론

2003. 03. 25

목 차

- 정수의 성질 및 연산
- 잉여류의 성질 및 연산
- Legendre and Jacobi symbols

정수의 성질 및 연산

- $-18 \div 3 =$

- 정수 a, b 가

어떤 c 에 대해 $b = ac$ 이면

a 가 b 를 나눈다라고 하고

$$a \mid b$$

로 표시한다.

- $3 \mid (-18)$

정수의 성질 및 연산

- $-19 = (-7) \times 3 + 2$
 $= (-6) \times 3 - 1$
 $= 6 \times (-3) - 1$

- 정수의 나눗셈 알고리즘:

a, b가 정수이면($b > 1$)

다음을 만족하는 정수 q, r이 존재한다.

$$a = qb + r, (0 \leq r < b).$$

이 q와 r은 유일하다.

- 이때 나머지 r을 $a \bmod b$ 로 표시한다.

정수의 성질 및 연산

- 최대 공약수(Greatest Common Divisor):

- 1) d 는 0보다 큰 정수이다.
- 2) d 는 정수 a 와 b 의 약수이다. ($d|a, d|b$)
- 3) d 는 약수 중 가장 크다.
(만약 $c|a$ 이고 $c|b$ 인 c 가 있으면 $c|d$ 이다.)

이 때 d 를 a 와 b 의 최대공약수라 부르고,
 $\gcd(a, b)$ 로 표시한다.

- 12의 약수 = { 1, 2, 3, 4, 6, 12 }
- 18의 약수 = { 1, 2, 3, 6, 9, 18 }
- $\gcd(12, 18) =$ 6

정수의 성질 및 연산

- $\gcd(2, 1293451) =$
- 서로소(coprime or relatively prime):
두 정수 a, b 의 최대공약수인 $\gcd(a, b) = 1$ 일 때
 a, b 를 서로소라 한다.
- 최소공배수(Least Common Multiple):
 - 1) d 는 a 와 b 의 배수이다. ($a|d$ 이고 $b|d$)
 - 2) d 는 배수 중에서 가장 작다.
($a|c$ 이고 $b|c$ 이면 $d|c$ 이다.)

정수의 성질 및 연산

- 소수(Prime)

2 보다 큰 정수로 1과 자기 자신 이외의 약수를
가지 않는 정수.

- 합성수(Composite)

소수가 아닌 정수

- 소수 p 에 대해 $p \mid ab \Rightarrow p \mid a$ 또는 $p \mid b$

- 합성수 $n \mid ab \Rightarrow n \mid a$ 또는 $n \mid b$?

정수의 성질 및 연산

- 1, 2, 3, 4, 5, 6, 7, 8, 9, 10

10과 서로소인 수는?

10과 서로소인 수의 개수는?

- 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11

11과 서로소인 수는?

11과 서로소인 수의 개수는?

- Euler phi 함수:

$\phi(n)$: 1과 n 사이의 정수에서 n 과 서로소인
정수의 개수

정수의 성질 및 연산

- Euler phi 함수의 성질:

1) p 가 소수이면

$$\phi(p) = p - 1.$$

2) $\gcd(m, n) = 1$ 이면

$$\phi(mn) = \phi(m) \phi(n).$$

예) $\phi(3) =$

$$\phi(8) =$$

$$\phi(24) =$$

정수의 성질 및 연산

- Euler phi 함수의 성질

1	2	3	...	p
p+1	p+2	p+3	...	2p
...				$(p^{e-1}-1)p$
$(p^{e-1}-1)+1$	$(p^{e-1}-1)+2$	$(p^{e-1}-1)+3$	...	$p^{e-1}p$

$$3) \phi(p^e) = (p^e - 1) - (p^{e-1} - 1) = p^e(1 - 1/p)$$

$$4) \phi(p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_n^{e_n}) =$$

정수의 성질 및 연산

- $a = qb + r$
a와 b를 나누는 정수는 r을 나누는가?
- $\gcd(a, b) = \gcd(b, a \bmod b)$
- Euclidean algorithm:

$$\gcd(4864, 3458) = ?$$

$$4864 = 1 \cdot 3458 + 1406$$

$$3458 = 2 \cdot 1406 + 646$$

$$1406 = 2 \cdot 646 + 114$$

$$646 = 5 \cdot 114 + 76$$

$$114 = 1 \cdot 76 + 38$$

$$76 = 2 \cdot 38$$

정수의 성질 및 연산

- Euclidean algorithm의 복잡도:

$$O((\lg n)^2)$$

- $38 = (4864)(32) + (3458)(-45)$

- Extended Euclidean algorithm:

정수 a 와 b 의 gcd인 d 와

$$ax + by = d$$

를 만족하는 정수 x, y 를 구하는 알고리즘.

➤ 복잡도: $O((\lg n)^2)$

잉여류의 성질과 연산

- Congruence:

정수 a, b 에 대해

$n \mid (a - b)$ 이면 a 가 n 을 법(modulus)으로

b 와 congruent 하다고 하며,

$a \equiv b \pmod{n}$ 으로 표기한다.

- $7 \mid (11 - (-31))$

$$\Rightarrow 11 \equiv -31 \pmod{7}$$

잉여류의 성질과 연산

- 11을 7로 나눈 나머지는?
-31을 7로 나눈 나머지는?
- Congruence의 성질:
 - 1) $a \equiv b \pmod{n} \Leftrightarrow$
a와 b는 n으로 나눈 나머지가 같다.
 - 2) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$
 - 3) $a \equiv b \pmod{n}$ 이고 $b \equiv c \pmod{n}$
 $\Rightarrow a \equiv c \pmod{n}$

잉여류의 성질과 연산

- Congruence의 성질:

4) $a \equiv x \pmod{n}$ 이고 $b \equiv y \pmod{n}$

$$\Rightarrow a + b \equiv x + y \pmod{n}$$

5) $a \equiv x \pmod{n}$ 이고 $b \equiv y \pmod{n}$

$$\Rightarrow ab \equiv xy \pmod{n}$$

6) $a \equiv b \pmod{n}$

$$\Rightarrow \text{임의의 } k \text{에 대해 } a^k \equiv b^k \pmod{n}$$

잉여류의 성질과 연산

- $a = qn + r$, $0 \leq r < n$

$$\Rightarrow a \equiv r \pmod{n}$$

- 잉여류 집합 Z_n

n 을 법으로 나눈 나머지의 집합

$$Z_n = \{ 0, 1, 2, \dots, n-1 \}.$$

- $Z_{15} = \{ 0, 1, 2, \dots, 15 \}$

$$11 + 13 = \quad , \quad 3 + 12 =$$

$$3 \cdot 12 = \quad , \quad 3 \cdot 5 =$$

잉여류의 성질과 연산

- Z_{15} 에서 두 수를 곱해서 1인 수를 찾아라.

0	1	2	3	4	5	6	7
8	9	10	11	12	13	14	

잉여류의 성질과 연산

- Z_n 에서 곱셈에 대한 역원(inverse):

$a \in Z_n$ 에서

$$ax = 1$$

을 만족하는 x 가 있으면

이것을 a 의 곱셈에 대한 역원이라고 한다.

- 1) 곱셈에 대한 역원은 유일하다.
- 2) a 를 invertible 하다 또는 unit 이라 부른다.
- 3) a 의 곱셈에 대한 역원을

$$a^{-1}$$

로 표시한다.

잉여류의 성질과 연산

- $\mathbb{Z}_{15}$ 에서 invertible 한 원소는?
- $\mathbb{Z}_{15}$ 에서 4^{-1} 은?
- $\mathbb{Z}_n$ 에서
a: invertible $\Leftrightarrow \gcd(a, n) = 1$
- $\mathbb{Z}_{15}$ 에서 4^{-1} 은 어떻게 구하나?

잉여류의 성질과 연산

- 중국인의 나머지 정리(Chinese remainder theorem):

1) $n_1, n_2, \dots, n_k$ 가 coprime 일 때

$$x \equiv a_1 \pmod{n_1}$$

$$x \equiv a_2 \pmod{n_2}$$

...

$$x \equiv a_k \pmod{n_k}$$

이 방정식은 $n = n_1 n_2 \dots n_k$ 를 법으로
유일한 해를 갖는다.

잉여류의 성질과 연산

- 중국인의 나머지 정리(Chinese remainder theorem):

2) Gauss 알고리즘

$$x = a_1 N_1 M_1 + a_2 N_2 M_2 + \dots + a_k N_k M_k$$

$$N_i = \frac{n}{n_i}, \quad M_i \equiv N_i^{-1} \pmod{n_i}$$

$$\Rightarrow O((\lg n)^2)$$

잉여류의 성질과 연산

- $x \equiv 2 \pmod{3}$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 2 \pmod{7}$$

$$: n = 3 \cdot 5 \cdot 7 = 105$$

$$N_1 = n/3 = 35, N_2 = n/5 = 21, N_3 = n/7 = 15$$

$$M_1 = 35^{-1} \pmod{3} = 2$$

$$M_2 = 21^{-1} \pmod{5} = 1$$

$$M_3 = 15^{-1} \pmod{7} = 1$$

$$\Rightarrow x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \equiv 23 \pmod{105}$$

잉여류의 성질과 연산

- Z_n 의 곱셈군 :

$$Z_n^* = \{ a \in Z_n \mid \gcd(a, n) = 1 \}$$

- $Z_{15}^* = \{ \quad \quad \quad \}$

- p 가 소수이면

$$Z_p^* = \{ \quad \quad \quad \}$$

- Order of Z_n^* :

Z_n^* 의 원소의 개수

$|Z_n^*|$ 로 표시

잉여류의 성질과 연산

- $|Z_{15}^*| =$

- $|Z_n^*| = \phi(n)$

- Z_7^* 에서

$$2^1 \equiv \quad (\text{mod } 7) \qquad 2^2 \equiv \quad (\text{mod } 7)$$

$$2^3 \equiv \quad (\text{mod } 7) \qquad 2^4 \equiv \quad (\text{mod } 7)$$

$$2^5 \equiv \quad (\text{mod } 7) \qquad 2^6 \equiv \quad (\text{mod } 7)$$

잉여류의 성질과 연산

- $\mathbb{Z}_7^*$ 에서

$$3^1 \equiv 3 \pmod{7} \qquad 3^2 \equiv 2 \pmod{7}$$

$$3^3 \equiv 6 \pmod{7} \qquad 3^4 \equiv 4 \pmod{7}$$

$$3^5 \equiv 5 \pmod{7} \qquad 3^6 \equiv 1 \pmod{7}$$

- Fermat의 정리:

p: 소수

$$\gcd(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$$

잉여류의 성질과 연산

- Euler의 정리:

$$a \in \mathbb{Z}_n^* \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

- $a^{30} \pmod{15} =$

- $r \equiv s \pmod{\phi(n)} \Rightarrow a^r \equiv a^s \pmod{n}$

잉여류의 성질과 연산

- 원소의 order:

$a \in \mathbb{Z}_n^*$ 일 때

$a^t \equiv 1 \pmod{n}$ 을 만족하는 최소의 양의 정수 t 를
원소 a 의 order라 하며, $\text{ord}(a)$ 로 표시한다.

1) $\text{ord}(a) = t$ 이고 $a^s \equiv 1 \pmod{n}$

$$\Rightarrow t \mid s$$

2) $\text{ord}(a) \mid \phi(n)$

- 소수 p 에 대해 $a \in \mathbb{Z}_p^*$ 의 order는?

잉여류의 성질과 연산

• $Z_{15}^* = \{ 1, 2, 4, 7, 8, 11, 13, 14 \}$

원소	1	2	4	7	8	11	13	14
order	1	4						

$$2^2 \equiv 4 \pmod{15}$$

$$2^3 \equiv 8 \pmod{15}$$

$$2^4 \equiv 1 \pmod{15}$$

잉여류의 성질과 연산

• $Z_9^* = \{ 1, 2, 4, 5, 7, 8 \}$

원소	1	2	4	5	7	8
order	1	6	3			

$$2^2 \equiv 4 \pmod{9}$$

$$2^3 \equiv 8 \pmod{9}$$

$$2^4 \equiv 16 \equiv 7 \pmod{9}$$

$$2^5 \equiv 14 \equiv 5 \pmod{9}$$

$$2^6 \equiv 10 \equiv 1 \pmod{9}$$

$$4^2 \equiv 16 \equiv 7 \pmod{9}$$

$$4^3 \equiv 28 \equiv 1 \pmod{9}$$

잉여류의 성질과 연산

- 원시원(generator or primitive element):

$\alpha \in \mathbb{Z}_n^*$, $\text{ord}(\alpha) = \phi(n)$ 일 때

α 를 원시원이라 한다.

- Cyclic:

$\mathbb{Z}_n^*$ 이 원시원을 가질 때

$\mathbb{Z}_n^*$ 를 cyclic이라 부른다.

- 원시원을 단 하나 밖에 없는가?

잉여류의 성질과 연산

- 원시원의 성질:

1) Z_n^* : cyclic $\Leftrightarrow$

소수 p 에 대해 $n = 2, 4, p^k$ 또는 $2p^k$

2) $\alpha \in Z_n^*$: 원시원 $\Rightarrow$

$$Z_n^* = \{ \alpha^i \bmod n : 0 \leq i < \phi(n) \}$$

3) $\alpha \in Z_n^*$: 원시원

$$\alpha^i \bmod n : \text{원시원} \Leftrightarrow \gcd(i, \phi(n)) = 1$$

➤ 원시원의 개수는 $\phi(\phi(n))$

잉여류의 성질과 연산

- 원시원의 성질:

4) $\alpha \in \mathbb{Z}_n^*$: 원시원 $\Leftrightarrow$

$\phi(n)$ 을 나누는 모든 소수 p 에 대해

$$\alpha^{\phi(n)/p} \not\equiv 1 \pmod{n}$$

이 성립한다.

잉여류의 성질과 연산

- Z_n 의 덧셈:

$$a, b \in Z_n$$

$$\Rightarrow 1) a + b = \begin{cases} a + b & \text{if } a + b < n \\ a + \{b - n\} & \text{if } a + b \geq n \end{cases}$$

$$2) a - b = \begin{cases} a - b & \text{if } a > b \\ a + n - b & \text{if } a < b \end{cases}$$

잉여류의 성질과 연산

- $5^{100} \bmod 17 =$

잉여류의 성질과 연산

- Z_n 의 멍승 알고리즘:

Input: $a \in Z_n$. $k = k_t 2^t + k_{t-1} 2^{t-1} + \dots + k_0 2^0$

Output: $a^k \bmod n$

1. Set $b \leftarrow 1$, $k = 0 \Rightarrow \text{return}(b)$
2. Set $A \leftarrow a$
3. $k_0 = 1 \Rightarrow \text{set } b \leftarrow a$
4. For $i = 0 \dots t$
 - 4.1 Set $A \leftarrow A^2 \bmod n$
 - 4.2 $k_i = 1 \Rightarrow b \leftarrow A \cdot b \bmod n$
5. $\text{return}(b)$

잉여류의 성질과 연산

- Z_n 에서 역원:

$a \in Z_n$ 에 대한 a^{-1} ?

- 1) 확장된 유클리드 알고리즘 이용

$\gcd(a, n)$ 를 구하기 위해 확장된 유클리드
알고리즘을 이용하여

$$ax + ny = d$$

만족하는 x, y, d 를 구함.

만약 d 가 1이면

$$ax \equiv 1 \pmod{n}$$

잉여류의 성질과 연산

2) 오일러의 정리 이용

$$a^{\phi(n)} \equiv 1 \pmod{n} \text{ 이므로}$$

$$a \cdot a^{\phi(n)-1} \equiv 1 \pmod{n}$$

* $\gcd(a, n) = 1$ 임을 알고 있어야 함.

$\phi(n)$ 값을 알아야 함.