제2장 수학적 배경

한국IT 정보보안학부

2.1.1연산의 기본 성질

정수론

- R : 실수 집합(real number)
- Z : 정수 집합(integer)
    - 집합 { ..., -2, -1, 0, 1, 2, ... } 를 정수들의 집합 Z 라 함.

- N : 자연수 집합(natural number)
- $Z_m = \{0, 1, 2, \cdots, m-1\}$
- m : 소수, 합성수

참고 : 기호설명

기호 설명

- $\mathbb{N}$: 자연수(양의 정수)의 집합
- $\mathbb{Z}$: 정수의 집합
- $\mathbb{Q}$: 유리수의 집합
- $\mathbb{R}$: 실수의 집합
- $a \mid b$: 정수 b는 정수 a로 나누어 떨어진다.
- $\displaystyle\sum_{k=1}^{n} k = 1 + 2 + \cdots + n.$
- $\displaystyle\prod_{k=1}^{n} k = 1 \times 2 \times \cdots \times n.$
- $a \equiv b \pmod{m}$: 정수 a, b가 법 m에 대하여 합동이다.
- $\gcd(a, b)$: 정수 a와 b의 최대공약수
- $\operatorname{lcm}(a, b)$: 정수 a와 b의 최소공배수
- $\phi(m)$: 양의 정수 m과 서로 소인 m이하의 양의 정수의 개수

2.1 정수 집합

2.1.1연산의 기본 성질

❖ 정수 연산

- 덧셈
  - $a, b \in Z \quad a + b \in Z$
- 덧셈의 교환법칙
  - $a, b \in Z \quad a + b = b + a$
- 덧셈의 결합법칙
  - $(a + b) + c = a + (b + c)$
- 항등원
  - $a + 0 = 0 + a = a$

  (0∈Z은 모든 a∈Z에 대하여 $a + 0 = 0 + a = a$ 만족함.)
- 역원
  - $a + (-a) = (-a) + a = 0$

  (모든 a∈Z에 대하여 $a + (-a) = (-a) + a = 0$ 만족함. 따라서, 정수 집합 Z위에는 뺄셈이 정의된다.)

2.1 정수 집합

❖ 정수 연산

- 곱셈
  - $a, b \in Z \quad a \times b \in Z$
- 곱셈의 교환법칙
  - $a, b \in Z \quad a \times b = b \times \mathrm{a}$
- 곱셈의 결합법칙
  - $a, b, c \in Z \quad (a \times b) \times c = a \times (b \times c)$
- 항등원
  - $a \times 1 = 1 \times a = a$

  (정수 1∈Z은 모든 a∈Z에 대하여 $a \times 1 = 1 \times a = a$ 만족함.)

- 역원
  - $a \times c = c \times a = 1$

  $$1 \cdot (1) = -1 \cdot (-1) = 1$$

  (곱셈에 대하여 1과 -1만 역원 존재 .
  따라서, 정수 집합 Z위에는 나눗셈이 정의되지 않는다.)

2.1 정수 집합

❖ 정수 연산

- 덧셈과 곱셈은 분배법칙 성립

$$a,b,c \in Z, \quad a\cdot(b+c)=a\cdot b+a\cdot c$$

$$(a+b)\cdot c=a\cdot c+b\cdot c$$

- 몫(quotient), 나머지(remainder)

> **두 정수** $a,b \in Z$ **이고** $a \neq 0$ **일 때,**
>
> $$b=a\cdot q+r, \quad 0 \le r < |a|$$
>
> **인** $q,r \in Z$**가 유일하게 존재한다.**

  - 이 두 정수 q, r 를 각각 b를 a로 나누었을 때의
  - 몫(quotient), 나머지(remainder)라고 한다.

2.2 약수와 배수

❖ 공약수와 공배수

- 약수와 배수
  - $b = a \cdot c$
  - $a \mid b$
- 공약수
  - $a \mid b,\ a \mid c$ (a : 공약수)
  - 최대 공약수 (gcd : greatest common divisor)
- 공배수
  - $a \mid b,\ c \mid b$ (b : 공배수)
  - 최소 공배수 (lcm : least common multiple)

❖ 서로 소 (coprime)

- *gcd(a,b) = 1*
- 두 정수 a와 b의 최대 공약수가 1일 때, 즉 gcd(a,b)=1 일 때 a와 b 는 서로 소(relatively prime, coprime) 라고 한다.
- 다시 말하면, '서로 간의 공약수가 없다'는 말이다.
- 예
  - 11과 12는 서로 소이다.
  - (25, 42) = 1

참고 : 소인수분해

❖ 소인수분해

```
2    |    280        30
     ----------------------
5    |    140        15
     ----------------------
           28         3
```

- gcd(최대공약수) = 2 * 5 = 10
- lcm(최소공배수) = 2 * 5 * 28 * 3 = 840

❖ 2.2.1유클리드 호제법(Euclidean algorithm)

- 두 정수의 최대 공약수를 계산할 때는 유클리드 호제법을 이용한다. 두 양의 정수 a, b에 대하여

$$\begin{aligned}
b &\equiv aq_1 + r_1 & 0 &< r_1 < a \\
a &\equiv r_1 q_2 + r_2 & 0 &< r_2 < r_1 \\
r_1 &\equiv r_2 q_3 + r_3 & 0 &< r_3 < r_2 \\
&\vdots \qquad \vdots & & \\
r_{n-3} &\equiv r_{n-2} q_{n-1} + r_{n-1} & 0 &< r_{n-1} < r_{n-2} \\
r_{n-2} &\equiv r_{n-1} q_n + r_n & 0 &< r_n < r_{n-1} \\
r_{n-1} &\equiv r_n q_{n+1} & &
\end{aligned}$$

- 일 때, $\gcd(a,b) = r_n$ 이 성립한다.

2.2.1유클리드 호제법(Euclidean algorithm)

예제 2.1

- $$\begin{array}{c|cc|c} 4 & 62 & 510 & 8 \\ & \underline{56} & \underline{496} & \\ 3 & 6 & 14 & 2 \\ & \underline{6} & \underline{12} & \\ & 0 & 2 & \end{array}$$

$$\begin{array}{c|cc|c} q_2 & a & b & q_1 \\ & \underline{r_1 q_2} & \underline{a q_1} & \\ & r_2 & r_1 & \\ & \vdots & \vdots & \\ q_{n+1} & \overline{} & \overline{} & q_n \\ & r_{n-1} & r_{n-2} & \\ & \underline{r_n q_{n+1}} & \underline{r_{n-1} q_n} & \\ & 0 & r_n & \end{array}$$

$$\begin{aligned} b &= a q_1 + r_1 \\ a &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \quad \vdots \\ r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1} \end{aligned}$$

그림 2.1

- $2 = 14 - 6 \times 2 = 14 - (62 - 14 \times 4) \times 2$
  $= 14 \times 9 + 62 \times (-2)$
  $= (510 - 62 \times 8) \times 9 + 62 \times (-2)$
  $= 510 \times 9 + 62 \times (-74)$

유클리드 호제법 : 최대공약수

- 수가 크면 복잡

2304 1440

1. 큰 수를 작은 수로 나눈다.
2. 나누는 수를 나머지로 계속 나눈다.
3. 나머지가 0 되면 나누는 수가 최대공약수 이다.

- 약수 찾기 어려움

403 155

유클리드 호제법 : 최대공약수

❖ Gcd(12345,123)

[예제] 510과 62의 최대 공약수를 구하고 u 와 v 를 구하라.

❖ 유클리드 호제법

$$
\begin{array}{c|cc|c}
4 & 62 & 510 & 8 \\
3 & \underline{56} & \underline{496} & 2 \\
 & 6 & 14 & \\
 & \underline{6} & \underline{12} & \\
 & 0 & 2 &
\end{array}
$$

$$510 = 62 \times 8 + 14$$

$$62 = 14 \times 4 + 6$$

$$14 = 6 \times 2 + 2$$

$$6 = 2 \times 3$$

❖ u 와 v 구하기

$$
\begin{aligned}
2 &= 14 - 6 \times 2 \\
&= 14 - (62 - 14 \times 4) \times 2 \\
&= 14 \times 9 + 62 \times (-2) \\
&= (510 - 62 \times 8) \times 9 + 62 \times (-2) \\
&= 510 \times 9 + 62 \times (-74)
\end{aligned}
$$

- ❖ gcd(a,b) = au+bv
- ❖ 2 = 510u + 62v
- ❖ u = 9, v = -74

유클리드 호제법 : 최대공약수

- gcd(222, 690)

2.3 소수

❖ 소수 (prime number)

- 1과 자신 이외의 약수가 존재하지 않는 양의 정수(p)
- 약수가 1과 자신의 수
- 2, 3, 5, 7, 11,,,

❖ 합성수 (composite number)

- 소수가 아닌 정수
- 소수 둘 이상의 곱
- 합성수 a = b · c 인 정수 b, c가 존재
- 4, 6, 8, 9, 10,,,,

- 예)
  - 2, 3, 5, 7, 11, 13, 17 등은 소수
  - 4, 6, 8, 9, 10, 12, 14 등은 합성수

2.3 소수

❖ 표준분해

$$n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

- 여기서 $p_1, p_2, \ldots, p_r$ 은 서로 다른 소수
- 위와 같은 소인수 분해 표현법을 n의 표준 분해라고 함.

- 예) 정수 12의 표준 분해 ➔ 4 x 3 ➔ 2^2 x 3^1

- [실습] 정수 252를 표준 분해 하여라.

2.3 소수

❖ 소수판정

❖ [참고] 소수 판정 알고리즘

- 양의 정수가 소수인지를 판정하는 문제는 **암호학, 부호이론, 정보이론 등의 통신이론에서는 대단히 중요한 문제**

- 실제로 100자리 이상의 소수를 찾는 일은 암호학에서 대단히 중요한 문제

❖ 예) AKS 알고리즘

- 결정적소수판정알고리즘
- AKS Primality Test

[참고] 소수 판정 알고리즘

```c
#include <math.h>
#include <stdio.h>
#include <stdlib.h>

static bool IsPrime(unsigned int n)
{
    if (n < 2) return false;
    if (n < 4) return true;
    if (n % 2 == 0) return false;

    unsigned int iMax = (unsigned int)sqrt((double)n) + 1;
    unsigned int i;
    for (i = 3; i <= iMax; i += 2)
        if (n % i == 0)
            return false;

    return true;
}
```

```c
int main()
{
    unsigned int NumLast = 100;
    for(unsigned int i=0; i<NumLast; ++i)
    {
```

```
C:\WINDOWS\system32\cmd.exe
2 3 5 7 11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97
계속하려면 아무 키나 누르십시오 . . .
```

2.3 소수

❖ 소수의 분포

- 무수히 많음

$$p_1 \times p_2 \times \cdots \times p_k + 1 = N_k$$

$$2+1=3$$
$$2\times3+1=7$$
$$2\times3\times5+1=31$$
$$2\times3\times5\times7+1=211$$
$$2\times3\times5\times7\times11+1=2311$$

$$2\times3\times5\times7\times11\times13+1=30031=59\times509$$

- 소수의 개수

x	$\pi(x)$	$x/\ln x$
10	4	4
10^2	25	22
10^3	168	145
10^4	1229	1086
10^5	9592	8686
10^6	78498	72382
10^7	664579	620421

2.4 합동식

❖ 법 연산 (modular arithmetic)

- 합동식
  - $a \equiv b \bmod m, \quad m \mid (a - b)$
- 완전 잉여계
  - $Z_m = \{0, 1, 2, \cdots, m - 1\}$
- 기약 잉여계
  - $Z_m^* = \{a \in Z_m \mid \gcd(a, m) = 1\}$
- Euler 함수
  - $\varphi(m) = |Z_m^*|$

Euler φ 함수

❖ Euler의 ϕ 함수(ϕ -function)

- m이 양의 정수일 때 $\phi(m)$ 은 m보다 크지 않으면서 m과 서로소인 정수의 개수이다.
- 즉, $\phi(m) = \left|Z_m^*\right|$ 예) $\phi(9) = \left|Z_9^*\right| = \left|\{1,2,4,5,7,8\}\right| = 6$

- Z_2^* = {1}
- Z_3^* = {1, 2}
- Z_4^* = {1, 3}
- Z_5^* = {1, 2, 3, 4} ...

- φ(1) = 1 **로 정의**
- φ(2) = 1
- φ(3) = 2
- φ(4) = 2
- φ(5) = 4 ...

n	1	2	3	4	5	6	7	8	9	10	11	12
∅(n)	1	1	2	2	4	2	6	4	6	4	10	4

Euler φ 함수

- **특히** p **가 소수일 때,** $\phi(p) = p - 1$

- **또한,** $\phi(p^e) = p^e - p^{e-1}$
  - 1 ~ p^e 까지의 정수 중, p^e 와 서로소가 아닌 것. 즉, p로 나누어지는 것은 $1 \times p, 2 \times p, \cdots, p^{e-1} \times p$ 이므로 총 p^{e-1}개
  - 그러므로, $\phi(p^e) = p^e - p^{e-1}$ 이 성립한다.

- **또한,** $\phi(m)$의 $m = p^\alpha q^\beta r^\gamma \cdots (p, q, r \cdots$은 서로다른소수$)$

$$\phi(m) = m(1 - \frac{1}{p})(1 - \frac{1}{q})(1 - \frac{1}{r}) \cdots$$

$$\phi(m) = (p^\alpha - p^{\alpha-1})(q^\beta - q^{\beta-1})(r^\gamma - r^{\gamma-1}) \cdots$$

Euler 함수 φ(*m*)의 계산

$\phi(m)$의 $m = p^{\alpha} q^{\beta} r^{\gamma} \cdots (p, q, r \cdots$은 서로다른소수$)$

$$\phi(m) = m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\cdots$$

$$\phi(m) = (p^{\alpha} - p^{\alpha-1})(q^{\beta} - q^{\beta-1})(r^{\gamma} - r^{\gamma-1})\cdots$$

- 예

  $\varphi(7) = (7^1 - 7^0) = 6$

  $\varphi(15)=\varphi(3)\times\varphi(5)=(3^1-3^0)\ (5^1-5^0) = 8$

  $\varphi(9) = \varphi(3^2) = (3^2 - 3^1) = 6$

[연습문제 2.2]

- 252를 소인수 분해하고 φ(252)을 구하여라.

문 제

❖ 풀 수 있는 문제

- 쉬운 문제
  - 다항식 문제 (P 문제)

- 어려운 문제
  - 지수식 문제 (NP 문제)
    - **소인수분해 문제**
      - » $n = p \times q$ p, q : **소수**
    - **이산대수 문제**
      - » $y \equiv g^x \bmod p$
    - **Knapsack 문제**

❖ 풀 수 없는 문제

[참고] 공개키 암호 방식의 수학적 분류

❖ 공개키 암호 방식의 수학적 분류

- 이산대수학에 기초한 공개키 암호
  - ECC(Elliptic Curve Cryptosystem)
  - ElGamal
- 소인수분해에 기초한 공개키 암호
  - RSA(Rivest, A.Shamir, L.Adleman)
  - Rabin

연습문제

1. **두 정수 4864, 3458 에 대하여**

   ① 유클리드 호제법을 이용하여 gcd(4864,3458)을 구하고

   ② ①의 해를 p라 할 때 확장 유클리드 호제법을 이용하여 p=a * 4864+b * 3458 을 만족하는 a,b를 구하여라

2. **252를 소인수 분해 하고** $\phi(252)$**를 구하여라**

3. **NP문제로 알려진 문제들을 조사하고, 이 중 암호학에 이용될 수 있는 문제에는 어떤것이 있는지 알아보라**