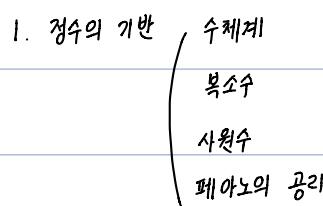


# I 수체계와 소인수분해

1. 정수의 기반
2. 수의 표현
3. 약수·배수
4. 유clidean 알고리즘과 부정방정식
5. 소수
6. 소인수분해



Thm 1.2) 정수의 경계성 (Well-ordering Principle)

어떤 성질  $P$ 를 만족하면서 주어진  $a$  보다 큰 모든 정수의 집합  $S \neq \emptyset$ 에는 최소의 정수가 존재한다.

Thm 1.4) 유한 귀납법의 원리

$N$ 의 부분집합  $S$ 가 조건

$$(i) 1 \in S \quad (ii) k \in S \Rightarrow k+1 \in S$$

을 만족할 때,  $S = N$ 이다.

(P) (정수의 경계성을 이용한 증명) **귀류법**

$S \neq N$  이면  $N-S$ 는 공집합이 아님으로 최소원  $n$ 을 가진다.

$1 \in S$  이므로  $1 < n$ 이고 여기서  $0 < n-1 < n$ 이다.

$n = \min(N-S)$  이므로  $n-1 \in N-S$  이고 따라서  $n-1 \in S$ 이다.

이제 조건 (ii)에 의하여  $n \in S$ 이고 이는  $n \in N-S$ 라는 사실에 모순.

2223  $N-S = \emptyset$ , 즉  $S = N$ 이다.

Thm 1.5) 제 2 유한 계법법의 원리

$N$ 의 부분집합  $S$ 가 조건

$$(i) 1 \in S \quad (ii) \{1, 2, \dots, k\} \subset S \Rightarrow k+1 \in S \text{ 를 만족할 때, } S = N$$

• 나눗셈 알고리즘

Thm 1.6) 정수  $a$  와 정수  $b$ 에 대하여  $a = bq + r$ ,  $0 \leq r < |b|$  을 만족하는 정수  $q, r$  이 유일하게 존재.

$q$ : 몫 (quotient),  $r$ : 나머지 (remainder)

## 2. 수의 표현

• 정수의 여러가지 표현

Thm) 진법에 대한 기본정리

$b \in \mathbb{Z}$ ,  $b \geq 2$  일 때, 임의의 자연수  $a$ 에 대하여

$$a = r_m b^m + r_{m-1} b^{m-1} + \dots + r_1 b^1 + r_0$$

을 만족하는 정수  $m, r_0, r_1, \dots, r_m$  이 존재.

(단,  $m \geq 0$ ,  $r_m > 0$ ,  $0 \leq r_i < b$ ,  $0 \leq i \leq m$ )

Proof (1)  $a = r_m b^m + r_{m-1} b^{m-1} + \dots + r_1 b^1 + r_0$

$\nearrow b \times [q] + [r] \text{ 의 form.}$

$$= b(r_m b^{m-1} + r_{m-1} b^{m-2} + \dots + r_1) + r_0$$

이므로  $r_0$ 은  $a$ 를  $b$ 로 나눈 나머지이다.

(2)  $r_m b^{m-1} + r_{m-1} b^{m-2} + \dots + r_1 = b(r_m b^{m-2} + r_{m-1} b^{m-3} + \dots + r_0) + r_1$

이므로  $r_1$ 은  $a$ 를  $b$ 로 나눈 몫을  $b$ 로 나눈 것의 나머지이다.

(3) 비슷하게  $r_2, \dots, r_m$  을 각각 구할 수 있다.

표시법  $a = (r_m r_{m-1} \dots r_0)_b$  라 쓴다.

이것을 정수  $a$ 의  $b$ 진법 표현이라 한다.

$$\begin{array}{r} b | a \\ 2 | 4 - 0 \rightarrow r_0 \\ 2 | 2 - 0 \rightarrow r_1 \\ \hline 1 \rightarrow r_2 \end{array}$$

• 실수의 소수 표현

→ 10 진수로 변환하는 방법을 원박히게 읽힌다.

→ 10진수에서 2진수 / 8진수 / 16진수로 각각 변환한다.

10진수	일상생활에서 사용(0~9)	10진수를 변환...	정수의 변환 - 해당 진법으로 나누어준 후에 나머지 부분만을 역으로 취한다. 소수의 변환 - 해당 진법으로 곱한 결과의 정수 부분을 취하여 소수부분이 0이 되거나 반복수가 나올 때까지 진행
2진수	0,1 (2비트)		
8진수	0,1,2,3,4,5,6,7 (8비트)		8진수 1자리는 2진수 3자리(421)에 대응
16진수	0~9, A~F (16비트)		16진수 1자리는 2진수 4자리(8421)에 대응
	10~15는 A~F로 표현		

※ 10진수로의 변환

2, 8, 16진수에서 → 10진수로 변환할 경우

진수의 전개식 사용하여 자리값을 곱하여 계산 (모든 수의 0제곱은 1: 약속)

▶ 2진수를 10진수로

$$(예제) 101101.101_{(2)} \rightarrow 45.625$$

$$1 \times 32 + 0 \times 16 + 1 \times 8 + 1 \times 4 + 0 \times 2 + 1 \times 1 + 1 \times 0.5 + 0 \times 0.25 + 1 \times 0.125$$

▶ 8진수를 10진수로

$$(예제) 132.5_{(8)} \rightarrow 90.625_{(10)}$$

$$1 \times 8^2 + 3 \times 8 + 2 \times 1 + 5 \times 0.125 \\ (= \frac{1}{8})$$

▶ 16진수를 10진수로

$$(예제) 1AD.5_{(16)} \rightarrow 429.3125_{(10)}$$

$$1 \times 256 + A(10) \times 16 + D(13) \times 1 + 5 \times \frac{1}{16} (= 0.0625)$$

※ 10진수로의 변환

① 정수부분 - 해당 진법으로 나누어 끊이 진수보다 작아질 때까지 진행하며 나머지를 역으로 취한다.

② 소수부분 - 해당 진법으로 곱한 결과의 정수부분을 취하여 소수부분이 0이 되거나 반복수가 나올 때까지 진행한다.

▶ 29. 895<sub>(10)</sub> 를 2진수로 변환

정수부분 소수부분

$$\begin{array}{r}
 2 | 29 \\
 2 | 14 \cdots 1 \\
 2 | 7 \cdots 0 \\
 2 | 3 \cdots 1 \\
 \hline
 1 \cdots 1
 \end{array}
 \quad
 \begin{array}{r}
 0.895 \\
 \times 2 \\
 \hline
 1.790 \\
 \times 2 \\
 \hline
 1.0
 \end{array}
 \quad
 \begin{array}{r}
 0.450 \\
 \times 2 \\
 \hline
 0.900 \\
 \times 2 \\
 \hline
 0.0
 \end{array}
 \quad
 \begin{array}{r}
 0.50 \\
 \times 2 \\
 \hline
 1.0
 \end{array}$$

0. 111

$$\therefore 29.895_{(10)} = 11101.111$$

▶ 129.895<sub>(10)</sub> 를 10진수로 변환

정수부분 소수부분

$$\begin{array}{r}
 8 | 129 \\
 8 | 16 \cdots 1 \\
 \hline
 2 \cdots 0
 \end{array}
 \quad
 \begin{array}{r}
 0.895 \\
 \times 8 \\
 \hline
 1.000
 \end{array}$$

0. 1

*0을 때까지*

201

$$\therefore 129.895_{(10)} = (201.1)_8$$

▶ 408.8125<sub>(10)</sub> 를 16진수로

$$\begin{array}{r}
 16 | 408 \\
 16 | 25 \cdots 8 \\
 \hline
 1 \cdots 9
 \end{array}
 \quad
 \begin{array}{r}
 0.8125 \\
 \times 16 \\
 \hline
 13 \ 000
 \end{array}$$

198

0. D

$$\therefore 408.8125_{(10)} = (198.D)_{16}$$

3. 약수 배수

\* 정수의 정렬성

\* 수학적 귀납법

Def)  $a|b$  ( $a$ 는  $b$ 를 나누다)  $\Leftrightarrow b=aq, q \in \mathbb{Z}$        $a \in S (\neq \emptyset), S$ 의 최소원 존재.

(1)  $p(n)$ : 참

$a$ :  $b$ 의 약수 (divisor) 또는 인수 (factor)

\* 유한귀납법의 원리

(2)  $p(n)$ : 참  $\Rightarrow p(n+1)$ : 참

$b$ :  $a$ 의 배수 (multiple)

(1)  $| \in S$     (2)  $k \in S \Rightarrow k \cdot h \in S$     이면  $S = N$

Thm) 정수  $a, b$ 의 정수배의 합, 즉  $ax+by, (x, y \in \mathbb{Z})$  꼴의 표현을  $a, b$ 의 일차결합이라 한다.

Thm) (1)  $a|0, 1|a, a|a, \forall a \in \mathbb{Z}$

(2)  $a|1 \Rightarrow a = \pm 1$

(3)  $a|b$  and  $c|d \Rightarrow ac|bd$

(4)  $a|b$  and  $b|c \Rightarrow a|c$

\* (5)  $a|b$  and  $b|a \Rightarrow a = \pm b$

(6)  $a|b$  and  $b \neq 0 \Rightarrow |a| \leq |b|$

(7)  $a|b$  and  $a|c \Rightarrow a|bx+cy, \forall x, y \in \mathbb{Z}$

Def)  $a \in \mathbb{Z}, a\mathbb{Z} = \{ax \mid x \in \mathbb{Z}\}$  :  $a$ 의 배수의 집합

Thm)  $a, b \in \mathbb{Z}$

(1)  $a\mathbb{Z} \supseteq b\mathbb{Z} \Leftrightarrow a|b$  [예]  $2|4$  일 때  $2\mathbb{Z} \supseteq 4\mathbb{Z}$

(2)  $a\mathbb{Z} = b\mathbb{Z} \Leftrightarrow b = \pm a$

• 공약수와 공배수

Def)  $a, b, x \in \mathbb{Z}$ 에 대하여,  $x|a$ 이고  $x|b$  일 때  $x$ 를  $a$ 와  $b$ 의 공약수라 한다.

$a, b \in \mathbb{Z}, (a, b) \neq (0, 0)$  공약수 중 최대의 수를  $a, b$ 의 최대공약수(greatest common division) 라 하고  $\gcd(a, b)$ 로 표시

\*  $\gcd(a, b) = 1$  일 때,  $a$ 와  $b$ 를 서로 소(relatively prime)

Thm)  $a, b$ 의 공약수는  $a, b$ 의 일차결합의 약수.

$k|a, k|b \Rightarrow k|ax+by \Rightarrow a=km, b=kn \quad \forall m, n \in \mathbb{Z}$

$$ax+by = kmx+kn$$

$$= k(mx+ny)$$

$$\therefore k|ax+by$$

Rmk)  $\gcd(a, b) = \gcd(\pm a, \pm b)$

Thm 3.4)  $\gcd$ 은 일차결합

$(a, b) \neq (0, 0)$ 인 정수  $a, b$ 에 대하여  $\gcd(a, b) = ax+by$  를 만족하는 정수  $x, y$ 가 존재한다.

(예)  $\gcd(8, 20) = 4 = 8 \times 3 + 20 \times (-1)$

Thm)  $p > 0, \gcd(pa, pb) = p \gcd(a, b)$

$$(예) \ gcd(80, 200) = 10 \ gcd(8, 20) = 10 \cdot 4 = 40$$

$$gcd(12, 30) = 2 \ gcd(6, 15) = 2 \cdot 3 \ gcd(2, 5) = 6$$

Thm 3.6)  $(a, b) \neq (0, 0)$  인 경우  $a, b$ 에 대하여  $gcd(a, b) = 1$  일 필요충분 조건은 어떤 정수  $x, y$ 가 있어서  $ax + by = 1$  일 것이다.

$$\text{Coroll} ) \ gcd(a, b) = g \Rightarrow gcd\left(\frac{a}{g}, \frac{b}{g}\right) = 1$$

$$\therefore ax + by = g \Rightarrow \frac{1}{g}(ax + by) = 1 \Leftrightarrow \left(\frac{a}{g}\right)x + \left(\frac{b}{g}\right)y = 1$$

$$\text{Coroll} ) \ a|k, b|k \ \& \ gcd(a, b) = 1 \Rightarrow ab|k$$

$$\text{Coroll} ) \ a|bk \ \& \ gcd(a, b) = 1 \Rightarrow a|k$$

$$\therefore ax + by = 1 \Rightarrow akx + bky = k, \ a|ak \ \& \ a|bky \Rightarrow a|k$$

$$\text{Thm}) \ gcd(a, b) = 1, \ \forall m \in \mathbb{Z}, \ gcd(am, b) = gcd(m, b)$$

여러 정수의 최대공약수

Def) (1)  $a_1, a_2, \dots, a_n \in \mathbb{Z}$  ( $n \geq 2$ ),  $e$ :  $a_1, \dots, a_n$  의 공약수

$$\Leftrightarrow e|a_i, \ i=1, 2, \dots, n$$

(2)  $d$ :  $a_1, \dots, a_n$  의 최대공약수

$$\Leftrightarrow \begin{array}{l} \textcircled{1} \ d \geq 0 \\ \textcircled{2} \ d|a_i \ (i=1, 2, \dots, n) \end{array}$$

$$\textcircled{3} \ e|a_i \ (i=1, 2, \dots, n) \Rightarrow e|d$$

Thm 3.12) 짝수도 핵심은 0이 아닌  $a_1, a_2, \dots, a_n$ 에 대하여

$$gcd(a_1, a_2, \dots, a_n) = gcd(gcd(a_1, a_2), a_3, \dots, a_n)$$

$$(예) \ gcd(12, 18, 21) = gcd(gcd(12, 18), 21) = gcd(6, 21) = 3$$

Def) (1)  $a_1, a_2, \dots, a_n \in \mathbb{Z}$  ( $n \geq 2$ ) : 서로소 (mutually prime)

$$\Leftrightarrow gcd(a_1, a_2, \dots, a_n) = 1$$

(2)  $a_1, a_2, \dots, a_n \in \mathbb{Z}$  ( $n \geq 2$ ) : 서로 소 (pairwise relatively prime)

$$\Leftrightarrow \gcd(a_i, a_j) = 1 \quad (1 \leq i \neq j \leq n)$$

Note) 서로다른 서로소  $\Rightarrow$  서로소, 서로소  $\not\Rightarrow$  서로다른 서로소

Def)  $a, b, n \in \mathbb{Z}$ 에 대하여,  $a|b$ 이고  $b|c$ 일 때,  $c$ 를  $a$ 와  $b$ 의 공배수라 한다.

$a, b \in \mathbb{Z}$  ( $a \neq 0 \neq b$ ) 양의 공배수 중 최소의 수를  $a, b$ 의 최소공배수 (least common multiple) 이라고 하고  $\text{lcm}(a, b)$ 로 표시한다.

Thm 3.11)  $a, b \in N$ .  $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$

Corol)  $a, b \in N$ .  $\text{lcm}(a, b) = ab \Leftrightarrow \gcd(a, b) = 1$

• 여러 정수의 최소공배수

Thm 3.13) 0이 아닌 정수  $a_1, a_2, \dots, a_m$ 에 대하여

$$\text{lcm}(a_1, a_2, \dots, a_n) = \text{lcm}(\text{lcm}(a_1, a_2), a_3) = \text{lcm}(30, 20) = 60$$

Thm)  $\gcd(a, b) = 1 \Rightarrow \forall m \in \mathbb{Z}, \gcd(am, b) = \gcd(m, b)$

#### 4. 유clidean 알고리즘과 부정방정식

• 유clidean 알고리즘

Lemma 4.1)  $a, b, q, r \in \mathbb{Z}$  and  $a = bq + r \Rightarrow \gcd(a, b) = \gcd(b, r)$

p 46에 Lemma 3.3 안에서 책대로 증명 X

보조 3.3 안쓰고 다른 방법으로 하기 위해 몇몇 정리 → 정리 #1#2

Thm #1)  $a_1 + a_2 + \dots + a_n = b_1 + b_2 + \dots + b_k$  일 때 하나의 항을 제외하고 모든 항이 q의 배수이면 그 하나의 항 또한 q의 배수이다.

Thm #2)  $\gcd(a, b) = d$  일 때  $\gcd(a, a-b) = d$  이다.

### Thm 4.3) 유clidean 알고리즘

만약  $a$  와  $b$  ( $\neq 0$ ) 가 양의 정수이고

$$a = b q_1 + r_1, \quad 0 < r_1 < b \quad \Rightarrow \quad \gcd(a, b) = \gcd(b, r_1)$$

$$b = r_1 q_2 + r_2, \quad 0 < r_2 < r_1 \quad \Rightarrow \quad \gcd(b, r_1) = \gcd(r_1, r_2)$$

$$r_1 = r_2 q_3 + r_3, \quad 0 < r_3 < r_2 \quad \Rightarrow \quad \gcd(r_1, r_2) = \gcd(r_2, r_3)$$

$$\vdots \quad \vdots$$

$$r_{n-2} = r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1} \quad \Rightarrow \quad \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n)$$

$$r_{n-1} = r_n q_{n+1} + 0 \quad \Rightarrow \quad \gcd(r_{n-1}, r_n) = \gcd(r_n, 0)$$

$$\Rightarrow \gcd(a, b) = r_n \quad = r_n \quad \text{* } 0 \notin 모든 수의 약수}$$

•  $\gcd(a, b)$  을  $ax+by$  를 형태로

Thm 3.4)  $\gcd(a, b) = d$  일 때  $ax+by = d$  인 정수  $x, y$ 가 반드시 존재한다.

Thm)  $p > 0, \gcd(pa, pb) = p \gcd(a, b)$

(예)  $\gcd(299, 247)$  을 유clidean 알고리즘을 이용하여 구하라.

$$(sol) \quad 299 = 247 \times 1 + 52$$

$$\Rightarrow 247 = 52 \times 4 + 39$$

$$\Rightarrow 52 = 39 \times 1 + 13$$

$$\Rightarrow 39 = 13 \times 3 + 0 \\ = r_7$$

(예)  $\gcd(299, 247) = 13$  일 때,  $299x + 247y = 13$  일 때  $x, y$ 를 찾으라.

$$(sol) \quad \gcd(299, 247) = 13$$

$$= 52 - 39 \cdot 1$$

$$= 52 - (247 - 52 \cdot 4)$$

$$= 52 \cdot 5 - 247$$

$$= 5(299 - 247) - 247$$

$$= 299.5 + 247 \cdot (-6)$$

$$\text{247으로 } x=5, y=-6$$

• 부정방정식  $ax+by=c$  : (이지수 계수) > (방정식 개수)

• 부정방정식, 디오판투스 방정식 : 해가 정수로서 결정되는 정수계수 방정식

Thm)  $a, b, c$ 가 임의의 정수이고,  $\gcd(a, b) = d$  일 때,

(1) 일차부정방정식  $ax+by=c$  가 해를 가질 필요충분조건은  $d|c$ 이다.

(2) (1)의 경우에  $x_0, y_0$ 을 이 부정방정식의 하나의 해(특수해) 라 할 때 이 방정식의 해는  $\begin{cases} x = x_0 + \frac{b}{d}k \\ y = y_0 - \frac{a}{d}k \end{cases} \quad (k \in \mathbb{Z})$

(Ex 4.7) 부정방정식  $89x + 29y = 624$  ( $x \geq 0, y \geq 0$ ) 을 풀어라.

(sol) ①  $\gcd(89, 29)$  구하기.  $\gcd(89, 29) = 3 \Rightarrow \gcd(89, 29) | 624$  이므로 해가 존재.

$$89 = 29 \times 3 + 6$$

$$29 = 6 \times 4 + 5$$

$$6 = 5 \times 1 + 1$$

②  $89x + 29y = 3$  을 만족하는  $x, y$  구하기.

$$3 = 29 - 6 \times 4$$

$$= 29 - 4(89 - 29 \times 3)$$

$$= 89 \times (-4) + 29 \times 13 \rightarrow x = -4, y = 13$$

$$624 \div 3 = 208$$

③  $89x + 29y = 624$  를 만족하는 특수해

$$\begin{cases} x_0 = (-4) \times 208 = -832 \\ y_0 = 13 \times 208 = 2704 \end{cases}$$

$$\therefore x = -832 + 29m \geq 0 \quad \text{을 만족하는 } m = 93 \Rightarrow x = 5, y = 7$$

$$y = 2704 - 29m \geq 0$$

$$\begin{array}{r} +\frac{29}{3} \\ \hline \end{array}$$

$$\begin{array}{r} -\frac{832}{3} \\ \hline \end{array}$$

Coroll)  $\gcd(a, b) = 1$ 인 정수  $a, b$ 에 대하여  $(x_0, y_0)$ 가 부정방정식  $ax+by=c$ 의 특수해라고 할 때,

일반해는  $(x, y) = (x_0 + bk, y_0 - ak)$  ( $k \in \mathbb{Z}$ )

정수  $x, y, z$ 에 관한 다음 방정식의 일반해를 구하시오.

$$3x + 4y + 5z = 2$$

(P6)  $\gcd(3, 4) = 1$  이므로 임의의 정수  $t$ 에 대하여  $3x + 4y = 2 - 5z$ 는 해를 갖는다.

$$3(-1) + 4 \cdot 1 = 1 \text{ 이므로 } x_0 = 5t - 2, y_0 = 2 - 5t \text{ 는 } 3x + 4y = 2 - 5z \text{의 특수해}$$

$$\begin{aligned} 4 &= 3 \times 1 + 1 \quad \Rightarrow \quad 1 = 4 - 3 \\ 1 &= 1 \times 1 + 0 \quad = 4 + 3 \times (-1) \end{aligned} \quad \left. \begin{array}{l} x_0 = (-1) \times (2 - 5t) = 5t - 2 \\ y_0 = 2 - 5t \end{array} \right\}$$

$\gcd(4, 3) = 1$

따라서 일반해는  $x = 5t - 2 + 4s, y = 2 - 5t - 3s, z = t \quad (s, t \in \mathbb{Z})$ 이다.

정답)  $x = 5t - 2 + 4s, y = 2 - 5t - 3s, z = t, (s, t \in \mathbb{Z})$

## 5. 소수 (Prime)

- 소수 : 1과 자기 자신만을 양의 약수로 가지는 자연수

- 합성수 : 소수가 아닌 2 이상의 자연수

자기 자신보다 작은 두 자연수의 곱으로 표현되는 수

- 자연수  $a$ 의 약수 중 소수를  $a$ 의 소인수라고 한다.

Thm 5.1) 1이 아닌 모든 자연수  $n$ 은 소인수를 갖는다. ( $n \geq 2$ )

(P6) 수학적 귀납법 이용

- 소수의 판정 (제곱근 판정법)

Thm) 합성수  $n$ 은  $1 < p \leq \sqrt{n}$ 인 소수인 약수  $p$ 를 갖는다.

\* 소수의 판정 (제곱근 판정법)

$\sqrt{n}$  이하의 소인수를 가지지 않는 자연수  $n$ 은 소수

Rmk) 애각호스테네스의 체