# 나눗셈 알고리즘과 Euclid 호제법

**정리 1.1.10** 나눗셈 알고리즘(division algorithm): 학부 대수학의 절반

정수 $a \in \mathbb{Z}$ 와 자연수 $n \in \mathbb{N}$ 에 대하여

$$a = nq + r,\ 0 \le r < n$$

을 만족하는 정수 $q, r$ 이 유일하게 존재한다.

**정리 1.1.11** 나눗셈 알고리즘

정수 $a \in \mathbb{Z}$ 와 $b \neq 0$ 에 대하여

$$a = bq + r,\ 0 \le r < |b|$$

을 만족하는 정수 $q, r$ 이 유일하게 존재한다.

**Note**

$\mathbb{Z}$ 의 나눗셈 알고리즘에서 나머지의 조건에 대응하는 함수 절대값 $|\ |$ 에 주목하자.

나눗셈 알고리즘은 존재성을 보이는 존재정리이다. 이 때 자연수의 정렬성과 짝을 이룰 수 있다.

예: $\mathbb{Z}$ 의 부분군은 순환군이다. $\mathbb{Z}$ 는 주이데알 정역이다.

생성원의 존재성을 보일 때 나눗셈 알고리즘을 이용한다.

정수 $\mathbb{Z}$ 로부터 $\mathbb{Z}_n$ 을 유도하는 과정에서 핵심 역할을 하는 나눗셈 알고리즘은

대수학에서 여러 가지 모습(모두 중요한 정리)으로 변형되어 나타난다.

**정리 5.7.12** $F[x]$ 의 나눗셈 알고리즘(division algorithm)

체 $F$ 위의 다항식 $f(x), g(x) \in F[x],\ g(x) \neq 0$ 에 대하여

$$f(x) = q(x)g(x) + r(x),\ r(x) = 0 \text{ 또는 } \deg r(x) < \deg g(x)$$

로 표현할 수 있는 $q(x), r(x) \in F[x]$ 가 유일하게 존재한다.

**정의 5.11.7** 유클리드 정역(Euclidean domain, ED)

정역 $D$ 위에 다음을 만족하는 함수 $d : D - \{0\} \to \mathbb{N} \cup \{0\}$

1. 모든 $a, b \in D$ 에 대하여 $d(a) \le d(ab)$
2. $a, b \in D,\ b \neq 0$ 에 대하여

$$a = bq + r,\ r = 0 \text{ 또는 } d(r) < d(b)$$

를 만족하는 $q, r \in D$ 가 존재한다.

가 존재하면 $D$ 를 유클리드 정역이라 하고, $d$ 를 유클리드 노옴이라 한다.

**Note**

유클리드 정역에서 몫과 나머지 $q, r$ 이 유일할 필요는 없다.

**정리 5.11.9**

가우스 정수환 $\mathbb{Z}[i]$는 $N(x+yi)=x^2+y^2$이 유클리드 노옴인 유클리드 정역이다.

**Note**

유클리드 정역 $\mathbb{Z}[i]$에서 몫과 나머지 $q,r$은 유일하지 않다.

**정리 1.1.8**

정수 $a,b,q,r$에 대하여 $a=bq+r$이면 $\gcd(a,b)=\gcd(b,r)$이다.

**Note**

정리 1.1.8에서 $r$은 나눗셈 알고리즘의 조건 $0\le r<|b|$을 만족할 필요가 없다.

나눗셈 알고리즘이 대수학(정수론) 계산의 핵심이 되는 이유이다.

**정리 1.1.17** Euclid 알고리듬(Euclid 호제법)

$$\begin{aligned}
a &= bq_1 + r_1 && 0 < r_1 < |b| \\
b &= r_1q_2 + r_2 && 0 < r_2 < r_1 \\
r_1 &= r_2q_3 + r_3 && 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= r_{n-1}q_n + r_n && 0 < r_n < r_{n-1} \\
r_{n-1} &= r_nq_{n+1}
\end{aligned}$$

이면 $\gcd(a,b)=r_n$이다.

**Note**

유클리드 호제법을 거꾸로 거슬러 올라가서

$a,b$의 최대 공약수 $d=\gcd(a,b)$를 $a$와 $b$의 일차결합 $d=ax+by$로 나타낼 수 있다.

Euclid 호제법은 최대공약수를 구하는 정석적이고 범용적인 방법이다.

범용성은 Euclid 호제법의 최대 장점이다.

**예** $(33371,69184219)=13 \Rightarrow 13=-642687\times 33371+310\times 69184219$

**예** $\mathbb{Q}[x]$에서 $\left(x^5+2x^4+2x^3+7x^2+x+5,\ 4x^4+2x^3+5x^2+2x+1\right)=x^2+1$

$$\Rightarrow x^2+1=\frac{8}{37}\left(x^5+2x^4+2x^3+7x^2+x+5\right)+\left(-\frac{2}{37}x-\frac{3}{37}\right)\left(4x^4+2x^3+5x^2+2x+1\right)$$

**Notε**

그러나 두 정수 $a,b$를 결정하면, 예를 들어 $(9005,\ 3003)$만 계산하면 된다면 범용성은 무의미하다.
특정한 두 수의 최대공약수를 구할 때 반드시 Euclid 호제법을 사용할 필요는 없다.
임용시험에서는 크지 않은 수(2~3자리의 수 정도) 한 쌍만 계산하면 된다.
따라서 범용성이 장점인 정석적인 방법을 고집할 필요가 없다.
임용시험에 알맞은 계산 방법을 익히자. (계산연습의 핵심)
대수학(정수론)의 계산에서 Euclid 호제법(나눗셈 알고리즘)을 이용할 필요가 없다면
나눗셈 알고리즘의 이론적인 역할에 주목할 필요가 있다.

**정리 1.1.12** 일차결합으로 최대 공약수 표현하기

정수 $a,b\in\mathbb{Z}$의 최대 공약수 $d=\gcd(a,b)$를 $a$와 $b$의 일차결합

$$d=ax+by$$

로 쓸 수 있는 정수 $x$와 $y$가 존재한다. 정확하게

$$\gcd(a,b)=\min\{ax+by>0\mid x,y\in\mathbb{Z}\}=\min\{|ax+by|:ax+by\neq 0\}$$

이 성립한다.

**증명**

$S=\{ax+by>0|x,y\in\mathbb{Z}\}$로 정의하면 $a^2+b^2\in S$이므로 $S\neq\varnothing$이고,
자연수의 정열성에 의해서 $t=\min S=au+bv\in S$가 존재한다.
나눗셈 알고리즘에 의해서 $\exists q,r\in\mathbb{Z}$, $a=tq+r$, $0\le r<t$이므로
$r=a-tq=a-(au+bv)q=a(1-qu)+b(-vq)$이다.
만일 $r>0$이면 $r\in S$이고 $t=\min S$에 모순이다. 따라서 $r=0$이고 $t\mid a$이다.
같은 방법으로 $t\mid b$, 즉 $t$는 $a,b$의 공약수임을 알 수 있다.
$c$가 $a,b$의 공약수이면 $\exists m,n\in\mathbb{Z}$, $a=cm$, $b=cn$이므로
$t=au+bv=cmu+cnv$이고 $c\mid t$이다.
따라서 $c\le|t|=t$이므로 $t=au+bv=\min S=\gcd(a,b)$이다.

**Notε**

정리 1.1.12는 나눗셈 알고리즘의 아바타로 정역의 기호로 쓰면 다음과 같다.
정수 $a\in\mathbb{Z}$의 배수의 집합($a$가 생성하는 주이데알)을 $(a)$로 쓰면

$$(\gcd(a,b))=\{ax+by|x,y\in\mathbb{Z}\}=(a)+(b)$$

이다. (학부 대수학의 Main Theme)
정리 1.1.12의 증명은 여러 정리(예: $\mathbb{Z}$는 PID 등) 증명의 기본 패턴이다.

$S\neq\varnothing$의 선택 $\Longrightarrow$ $\exists\min S$ $\Longrightarrow$ 나눗셈 알고리즘, 나머지 $r$ $\Longrightarrow$ $r\neq 0$이면 모순

## 기본 패턴 5.7.13

정역 $D$ 위의 다항식 $f(x), g(x) \in D[x]$에 대하여
$g(x)$ 의 최고차항의 계수가 가역원이면

$$f(x) = q(x)g(x) + r(x),\ r(x) = 0 \text{ 또는 } \deg r(x) < \deg g(x)$$

로 표현할 수 있는 $q(x), r(x) \in D[x]$가 유일하게 존재한다.

**Notε**

정리의 증명이나 문제의 풀이과정에서

$$(a,b) = d \ \Rightarrow\ \exists s,t,\ as+bt = d$$
$$(a,b) = 1 \ \Leftrightarrow\ \exists s,t,\ as+bt = 1$$

을 사용하였다면 나눗셈 알고리즘을 적용한 것이지만 답안에는 나눗셈 알고리즘을 언급하지 않는다.
정리 1.1.12가 나눗셈 알고리즘의 결과이므로 정리 1.1.12로부터 유도된 많은 정리들도
나눗셈 알고리즘의 결과이다.
그러나 증명과정에 나눗셈 알고리즘은 언급되지 않고, 정리 1.1.12를 언급해서 증명한다.
예를 들어 나눗셈 알고리즘의 결과인 다음 정리의 증명에는 나눗셈 알고리즘이 언급되지 않는다.

## 정리 1.1.14

두 정수 $a,b$에 대하여 다음이 성립한다.

1. $d \mid ab$ 이고 $(d,a) = 1$ 이면 $d \mid b$ 이다.
2. $(a,b) = d$ 이고 $c \mid a,\ c \mid b$ 이면 $c \mid d$ 이다.
3. 소수 $p$ 가 $p \mid ab$ 이면 $p \mid a$ 또는 $p \mid b$ 이다.
4. $a \mid m,\ b \mid m$ 이고 $(a,b) = 1$ 이면 $ab \mid m$ 이다.
5. $|ab| = \gcd(a,b)\,\mathrm{lcm}(a,b)$ 이다.

**Notε**

나눗셈 알고리즘의 수학적인 중요성은 아무리 강조해도 모자라지만,
임용시험의 답안에는 핵심정리(예: 정리 1.1.12)를 증명할 때에만 언급될 가능성이 크다.

## 정리 3.2.13

순환군의 부분군은 순환군이다.

**증명**

순환군 $G = \langle a \rangle$ 의 자명한 부분군은 순환군 $\{e\} = \langle e \rangle$ 이다.
$H \neq \{e\}$ 이면 $S = \left\{ k \in \mathbb{N} \mid a^k \in H - \{e\} \right\} \neq \varnothing$ 이므로 $m = \min S$ 가 존재하고 $\langle a^m \rangle \subset H$ 이다.
역으로 $a^k \in H$ 에 대하여 $k = mq + r,\ 0 \le r < m = \min S$ 이고 $a^r = a^k a^{-mq} \in H$ 이다.
만일 $0 \neq r < m$ 이면 $m = \min S$ 에 모순이므로 $r = 0$ 이다.
따라서 $a^k = a^{mq} = (a^m)^q \in \langle a^m \rangle$ 이고 $H \subset \langle a^m \rangle$ 이다.

**정리 5.7.15**

체 $F$ 위의 다항식환 $F[x]$는 주이데알 정역이다.

**증명**

정역 $F[x]$의 이데알 $I \neq (0)$가 주이데알임을 보이면 된다.

$\mathbb{N} \cup \{0\}$의 부분집합 $S = \{\deg f(x) \mid f(x) \in I - \{0\}\} \neq \varnothing$에 대하여 $\min S = n$가 존재한다.

따라서 $\deg p(x) = n$인 $p(x) \in I$가 존재하고, $(p(x)) \subset I$이다.

역으로 $f(x) \in I$에 대하여

$$f(x) = q(x)p(x) + r(x),\ r(x) = 0 \text{ 또는 } \deg r(x) < \deg p(x) = n$$

을 만족하는 다항식 $q(x), r(x) \in F[x]$가 존재한다.

$f(x), p(x)$가 이데알 $I$의 원소이므로 $r(x) = f(x) - q(x)p(x) \in I$이다.

만일 $r(x) \neq 0$이면 $\deg r(x) \in S$이고 $\deg r(x) < \deg p(x) = n = \min S$이므로 모순이다.

따라서 $r(x) = 0$이고, $f(x) = q(x)p(x) \in (p(x))$이므로 $I \subset (p(x))$이다.

**정리 5.11.8** ED $\Rightarrow$ PID

유클리드 정역은 주이데알 정역이다.

**Notε**

"정리 5.7.15 $F[x]$는 PID"의 증명에서 $\deg$를 $d$로 바꾸면 정리 5.11.8의 증명을 얻는다.

유클리드 정역의 이데알 $I \neq (0)$에 대하여 $\min\{d(b) : b \in I - \{0\}\} = k$가 존재한다.

따라서 $d(a) = k$인 $a \in I$가 존재하고 $I = (a)$이다.

유클리드 정역은 $\mathbb{Z}$와 $F[x]$의 작업을 거의 흉내 낼 수 있는 정역이다.

**정리 5.8.1**

체 $F$ 위의 다항식 $f(x) \in F[x]$의 차수가 $\deg f(x) = n$일 때

$$F[x]/(f(x)) = \left\{ a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 + (f(x)) \,\middle|\, a_k \in F \right\}$$

이 성립한다.

**증명** $g(x) \in F[x]$에 대하여 나눗셈알고리즘에 의해서

$$g(x) = q(x)f(x) + r(x),\ r(x) = 0 \text{ 또는 } \deg r(x) < \deg f(x) = n$$

을 만족하는 $q(x), r(x) \in F[x]$가 존재한다. 따라서

$$\begin{aligned} g(x) + (f(x)) &= r(x) + (f(x)) \\ &= a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 + (f(x)) \in F[x]/(f(x)) \end{aligned}$$

이다.

**Note**

대수학(정수론)의 아주 많은 정리가 나눗셈 알고리즘의 아바타이지만
임용시험의 답안에 나눗셈 알고리즘을 언급할 가능성은 높지 않다.
존재성을 보이는 문제라면 나눗셈 알고리즘을 이용한 문제일 수 있다.
이 때 존재성의 변형된 표현을 찾을 수 있어야 한다.
대수학(정수론)의 계산에서도 나눗셈 알고리즘이 정석적인 방법이지만
임용시험에서는 특별한 경우의 문제가 출제되므로 다른 방법으로 푸는 것이 효율적이다.
만일을 대비해서 정석적이고 범용적인 방법인 Euclid 호제법의 표를 이용한 계산을 익히고,
임용시험에 알맞은 계산 방법을 익히자. (계산연습의 핵심)

✓ Euclid 호제법을 이용하여 다음 최대공약수를 구하시오.

1. $(9005,\ 3003)$
2. $(1508, 462)$
3. $(2793,\ 1953)$
4. $(18183, 6069)$

✓ Euclid 호제법을 이용하지 말고 다음 최대공약수를 구하시오.

1. $(9005,\ 3003)$
2. $(1508, 462)$
3. $(2793,\ 1953)$
4. $(18183, 6069)$

✓ Euclid 호제법을 이용하여 최대공약수 $(a,b)$를 $(a,b)=as+bt$ 형태로 표현하시오.

1. $(9005,\ 3003)$
2. $(1508, 462)$
3. $(2793,\ 1953)$
4. $(18183, 6069)$

✓ Euclid 호제법을 이용하지 말고 최대공약수 $(a,b)$를 $(a,b)=as+bt$ 형태로 표현하시오.

1. $(9005,\ 3003)$
2. $(1508, 462)$
3. $(2793,\ 1953)$
4. $(18183, 6069)$