유클리드 호제법 (algorithm to find g.c.d of m,n)

- Well-ordering principle on $\mathbb{N}$

- Euclid algorithm

- Examples

- Well-ordering principle on $\mathbb{N}$

Every nonempty subset of $\mathbb{N}$ has a minimal element m,

$\nexists\, n \in \mathbb{N}$ s.t. $n < m$.

Thm Mathematical Induction

① $P(0)$ true

② $P(n)$ true implies $P(n+1)$ true.

If ① and ② hold, $\forall n$, $P(n)$ true.

□ Let $S = \{n \mid P(n) \text{ false}\}$.

WTS $S = \emptyset$.

Sps not. $S \neq \emptyset$. By WOP, $\exists$ minimal $m \in S$.

$\forall n < m$, $P(n)$ true. $m-1 < m$ & $P(m-1)$ true.

By ②, $P(m)$ true. $\Rightarrow\Leftarrow$

Recall
- d is a divisor of n if $\exists k \in \mathbb{Z}$ s.t. $n = kd$, denote $d \mid n$
- d is a common divisor of m and n if $d \mid m$ and $d \mid n$
- d is a greates common divisor >0 of m and n
  if d is a common divisor of m and n,
  and if d' is " , $d' \mid d$

Denote $(m, n) = d$ if d is a g.c.d of m, n

Prop if m, n in $\mathbb{Z}$, $\exists q, r \in \mathbb{Z}$ s.t. $n = qm + r$ and $0 \leq r < m$.

$\square$ Let $S = \{|n - xm| \mid x \in \mathbb{Z}\} \neq \phi$. $\exists$ minimal elt r.

$\Rightarrow |n - xm| = r$ $\begin{cases} \boxed{n - xm = r} \\ -n + xm = r \Rightarrow n = xm - r \\ \qquad = (x-1)m + m - r \end{cases}$

Claim $0 \leq r < m$

Sps $r \geq m \Rightarrow n - xm = (r - m) + m$

$n - (x+1)m = r - m \geq 0$

$r - m \in S$

$r - m < r$ $\Rightarrow\Leftarrow$

Thm

Let m, n in $\mathbb{Z}$ not zeros, and $d = (m, n)$. Then $\exists x, y \in \mathbb{Z}$ s.t $mx + ny = d$.

$\square$ $S = \{ |mx + ny| : x, y \in \mathbb{Z} \} \neq \emptyset$

$\exists$ minimal $d' \in S$. Let $d' = mx + ny$

Claim $d' = d$

$\exists q, r$ s.t. $m = qd' + r$ where $0 \leq r < d'$

$\Rightarrow r = m - qd' = m - q(mx + ny) = (1 - qx)m + (-qy)n$

if $r > 0$, contradiction $\Rightarrow r = 0 \Rightarrow d' \mid m$

In the same way $d' \mid n \Rightarrow d' \mid d$

Since $d \mid m$ and $d \mid n$, $d \mid mx + ny \Rightarrow d \mid d'$

Hence $d = d'$.

If p is prime, for any $0 < a < p$, $(p, a) = 1$.

$\Rightarrow \exists x, y$ s.t. $ax + py = 1$

$$\Downarrow$$

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

$$a^{-1} \equiv x \pmod{p}$$

Euclid Algorithm (How to fin x, b)

Let $a, b \in \mathbb{N}$. Choose q_0, r_0 s.t. We may assume $a > b$

$$a = q_0 b + r_0 \quad , \quad 0 \le r_0 < b$$

If $r_0 = 0$, stop. Otherwise

$$b = q_1 r_0 + r_1 \qquad 0 < r_1 < r_0$$

$$\vdots$$

← 유한번 안에 끝남

$$r_{n-2} = q_n r_{n-1} + r_n \qquad 0 < r_n < r_{n-1}$$

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

→ $r_n = (a, b)$

$$r_n = r_{n-2} - q_n r_{n-1}$$

$$\vdots$$

$$= ax + by$$

12. An integer N satisfying $1 \leq N \leq 256$ represents a secret to be shared among five individuals. Any three of the individuals are allowed access to the information. The secret is encoded in a polynomial p, according to the secret sharing scheme described in Section 2.8.1, lying in $\mathcal{P}_2(\mathbf{Z}_{257})$. Suppose three of the individuals get together, and their data points are $(15, 13)$, $(114, 94)$, and $(199, 146)$. What is the secret?

$143^{-1} = 133$

$$L_0(x) = \frac{(x-114)(x-199)}{(15-114)(15-199)} = \frac{x^2 - 56x + 42}{(-99)\cdot(-184)} = \frac{x^2 - 56x + 42}{143} = 133(x^2 - 56x + 42)$$

$$= 133x^2 + 5x + 189$$

$$L_1(x) = \frac{(x-15)(x-199)}{(114-15)(114-199)} = \frac{x^2 + 43x + 158}{66} = 74(x^2 + 43x + 158)$$

$$= 74x^2 + 98x + 127$$

$143^{-1} = 133$

$$144^{-1} \equiv 133 \pmod{257}$$

$$257 = 1 \cdot 144 + 113$$
$$144 = 1 \cdot 113 + 31$$
$$113 = 3 \cdot 31 + 20$$
$$31 = 1 \cdot 20 + 11$$
$$20 = 1 \cdot 11 + 9$$
$$\boxed{11 = 1 \cdot 9 + 2}$$
$$9 = 4 \cdot 2 + 1$$

$$1 = 9 - 4 \cdot 2$$
$$= 9 - 4(11 - 9)$$
$$= -4 \cdot 11 + 5 \cdot 9$$
$$= -4 \cdot 11 + 5(20 - 11)$$
$$= 5 \cdot 20 - 9 \cdot 11$$
$$= 5 \cdot 20 - 9(31 - 20)$$
$$= -9 \cdot 31 + 14 \cdot 20$$
$$= -9 \cdot 31 + 14(113 - 3 \cdot 31)$$
$$= 14 \cdot 113 - 51 \cdot 31$$
$$= 14 \cdot 113 - 51(144 - 113)$$
$$= -51 \cdot 144 + 65 \cdot 113$$
$$= -51 \cdot 144 + 65(257 - 144)$$