Euclidean Algorithm

KYB

Thrn, it's a Fact

mathrnfact@gmail.com

February 17, 2021

Overview

유클리드 호제법

- Well-odering principle on $\mathbb{N}$
- Euclidean Alhorithm
- Examples

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

Every nonempty subset S of $\mathbb{N}$ has a minimal element m, i.e., there is no $n \in S$ such that $n < m$.

Theorem (Mathematical Induction)

(1) $P(0)$ *is true.*

(2) $P(n)$ *is true implies* $P(n+1)$ *is true.*

If (1) and (2) both hold, then for all $n \in \mathbb{N}$ $P(n)$ *is true.*

Proof.

Let $S = \{n : P(n) \text{ is false}\}$. We want to show that $S = \varnothing$. Suppose not. By WOP, there is minimal element $m \in S$. Then for all $n < m$, $P(n)$ is true. In particular, $P(m-1)$ is true. (Since $0 \notin S$ by (1), such $m-1$ exists.) By (2), $P(m)$ is also true. (contradiction) $\square$

Remark

- d is a divisor of n is there is $k \in \mathbb{Z}$ such that $n = kd$, denote $d|n$.
- d is a common divisor of m and n if $d|m$ and $d|n$.
- d is a greatest common divisor of m and n if d is a common divisor of m and n, and if d' is another common divisor, then $d'|d$.

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

proposition

If $m, n \in \mathbb{Z}$, then there is $q, r \in \mathbb{Z}$ such that $n = qr$ and $0 \leq r < m$.

Proof.

Let $S = \{|n - xm| : x \in \mathbb{Z}\} \neq \varnothing$. Then there is a minimal element r, with $|n - xm| = r$.
Then either $n - xm = r$ or $-n + xm = r$. The latter case,
$n = xm - r = (x-1)m + m - r$.

Claim $0 \leq r < m$.
Suppose $r \geq m$. Then $n - xm = (r - m) + m$ implies $n - (x+1)m = r - m \geq 0$. So
$r - m \in S$ and $r - m < r$ (contradiction). $\square$

Theorem

Let m, n in $\mathbb{Z}$ be nonzero integers, and let $d = (m, n)$. Then there are $x, y \in \mathbb{Z}$ such that $mx + ny = d$.

Proof.

Let $S = \{|mx + ny| : x, y \in \mathbb{Z}\} \neq \varnothing$. Thus there is a minimal element $d' \in S$, say $d' = mx + ny$.

Claim $d' = d$.
Let q, r be such that $m = qd' + r$ where $0 \leq r < d'$. Then $r = m - qd' = m - q(mx + ny) = (1 - qx)m + (-qy)n$. If $r > 0$, contradiction, so $r = 0$, or $d'|m$. In the same way, $d'|n$, and hence $d'|d$.
Since $d|m$ and $d|n$, $d|mx + ny$, and $d|d'$. Hence $d = d'$. $\square$

Application

If p is prime, for any $0 < a < p$, $(p, a) = 1$. Then there are x, y such that $ax + py = 1$. Thus

$$ax \equiv 1 \mod p, \text{ or } a^{-1} \equiv x \mod p.$$

Euclidean Algorith

(How to find x, y) Let $a, b \in \mathbb{N}$. We may assume $a > b$. Choose q_k, r_k so that

- $a = q_0 b + r_0$ with $0 \leq r_0 < b$. (If $r_0 = 0$, stop).
- $b = q_1 r_0 + r_1$ with $0, r_1 < r_0$
- $\ldots$
- $r_{n-2} = q_n r_{n-1} + r_n$ with $0 < r_n < r_{n-1}$
- $r_{n-1} = q_{n+1} r_n$.

Then $r_n = (a, b)$.
From $r_n = r_{n-2} - q_n r_{n-1}$, we can find x and y such that $r_n = ax + by$.

Example

In $\mathbb{Z}_{257}$, $144^{-1} \equiv 141 \mod 257$ as follows:

$$\begin{aligned}
257 &= 1 \cdot 144 + 113 & 1 &= 9 - 4 \cdot 2 \\
144 &= 1 \cdot 113 + 31 & &= 9 - 4(11 - 9) = -4 \cdot 11 + 5 \cdot 9 \\
113 &= 3 \cdot 31 + 20 & &= -4 \cdot 11 + 5(20 - 11) = 5 \cdot 20 - 9 \cdot 11 \\
31 &= 1 \cdot 20 + 11 & &= 5 \cdot 20 - 9(31 - 20) = -9 \cdot 31 + 14 \cdot 20 \\
20 &= 1 \cdot 11 + 9 & &= -9 \cdot 31 + 14(113 - 3 \cdot 31) = 14 \cdot 113 - 51 \cdot 31 \\
11 &= 1 \cdot 9 + 2 & &= 14 \cdot 113 - 51(144 - 113) = -51 \cdot 144 + 65 \cdot 113 \\
9 &= 4 \cdot 2 + 1. & &= -51 \cdot 144 + 65(257 - 144) = 65 \cdot 257 - 116 \cdot 144.
\end{aligned}$$

So

$$1 = 65 \cdot 257 - 116 \cdot 144 = 64 \cdot 257 + (257 - 116) \cdot 144 = .64 \cdot 257 + 141 \cdot 144.$$

Hence,

$$144^{-1} \cong 141 \mod 257.$$

The End