14강 중국인 나머지 정리와 오일러 피 함수

(Chinese remainder theorem & Euler's phi function)

* 오일러 피 (토션트) 함수

$\phi(m)$:= 1이상 m 미만의 정수 중에서 m과 서로소인 수의 개수

① p가 소수일 때, $\phi(p) = p-1$ $1, 2, \cdots, p-1$

② p가 소수일 때, $\phi(p^k) = p^k - p^{k-1}$

pf) $1, 2, \cdots, p^k \Rightarrow p^k$개 p^k와 서로소가 아닌 수의 개수를 빼주면 된다.

↳ 공약수가 1만 존재하는 관계

α, p^k

↳ $1, p, p^2, \cdots, p^k$

↳ p를 소인수로 가지지 않는다. $p \nmid \alpha \Rightarrow$ p의 배수가 아니어야 한다.

$p \quad 2p \quad 3p \quad 4p \quad \cdots \quad \beta p$ $p^{k-1} \cdot p = p^k$

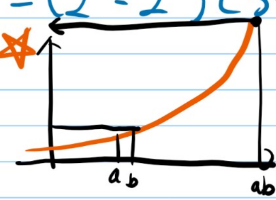
$1 \quad 2 \quad 3 \quad \cdots \quad p^{k-1}$

③ $\gcd(m,n) = 1$ 일때, $\phi(mn) = \phi(m)\phi(n)$

m과 n이 서로소

ex) $\phi(12) = \phi(2^2 \cdot 3) = \phi(2^2)\phi(3) = (2^2 - 2^1)(3-1) = 4$

☆ 숫자를 소인수분해 해야 한다.   소인수분해 알고리즘 ☆



ab

양자. 소어. 다항

pf) $A = \{x \mid 1 \le x < mn,\ \gcd(x, mn) = 1\}$

$B = \{x \mid 1 \le x < m,\ \gcd(x, m) = 1\}$

$C = \{x \mid 1 \le x < n,\ \gcd(x, n) = 1\}$

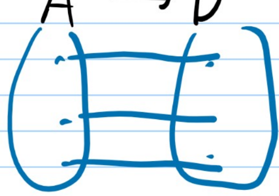
$(a, b) : B \times C$

B C

$D = \{(a, b) \mid a \in B,\ b \in C\}$

bijection (일대일 대응 함수)

$f : A \rightarrow D$ f가 bijection



→ 무한 (농도) $\mathbb{Z} \neq \mathbb{R}$

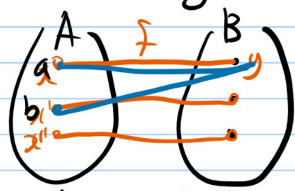
$A = \{ x \mid 1 \le x < mn,\ \gcd(x, mn) = 1 \}$

$B = \{ (a,b) \mid 1 \le a < m,\ \gcd(a,m)=1,\ \ 1 \le b < n,\ \gcd(b,n)=1 \}$

$f : A \to B$

$f(x) = (x \pmod m,\ x \pmod n)$

전단사 함수. $\forall y \in B$ $f(x) = y$ ①유일한 $x \in A$가 ②존재한다.



① 유일성 (귀류법)

$a, b \in A$ $\quad a \neq b \quad 1 \le a, b < mn$

$f(a) = f(b)$ 라고 하자.

$(a \pmod m,\ a \pmod n) = (b \pmod m,\ b \pmod n)$

$a \equiv b \pmod m \qquad a \equiv b \pmod n$

$\Rightarrow m \mid a-b \qquad n \mid a-b \ \Rightarrow\ mn \mid a-b \ \Rightarrow\ a \equiv b \pmod{mn}$

$\gcd(m,n) = 1 \qquad\qquad a = b$

② 존재성 $\quad \forall (b,c) \in B$

$\gcd(m,n)=1$, $x \equiv b \pmod m$, $x \equiv c \pmod n$를 만족하는 x가 $1 \le x < mn$에 존재한다.

* 중국인 나머지 정리

$\gcd(m,n)=1$ 일 때 $\begin{cases} x \equiv b \pmod m \\ x \equiv c \pmod n \end{cases}$ 을 동시에 만족하는 해는

$0 \le x < mn$에 유일하게 존재한다.

pf) $x \equiv b \pmod m \iff x = m \cdot y + b$

$my + b \equiv c \pmod n$

$my \equiv c - b \pmod n \qquad m_n^{-1}$ 존재

$y \equiv m_n^{-1}(c-b) \pmod n$

$y = n \cdot k + m_n^{-1}(c-b)$

$x = m(n \cdot k + m_n^{-1}(c-b)) + b$

$$= mn \cdot k + \boxed{m m_n^{-1}(c-b) + b} \text{ 고정}$$

$$x \equiv m m_n^{-1}(c-b) + b \pmod{mn}$$