

정수론 13강 오일러의 공식 (Euler's Formula)

* 역원 : 소수 p에 대해 $a^{-1} \pmod p$ 는 존재한다.

$$\begin{aligned} a \cdot \overset{\text{역원}}{x} &\equiv 1 \pmod m \\ \Leftrightarrow m \mid ax-1 &\Leftrightarrow ax-1 = mk \\ \Leftrightarrow ax-mk &= 1 \Leftrightarrow \gcd(a, m) \mid 1 \\ \Leftrightarrow \gcd(a, m) &= 1 \end{aligned}$$

* $a^k \equiv 1 \pmod m$

$$\begin{aligned} \rightarrow a \quad 2a \quad 3a \quad \dots \quad (p-1)a &\Rightarrow \cancel{(p-1)!} a^{p-1} \\ \rightarrow 1 \quad 2 \quad 3 \quad \dots \quad (p-1) &\Rightarrow \cancel{(p-1)!} \pmod p \end{aligned}$$

$$\begin{aligned} \rightarrow \underline{0a \quad 2a \quad 3a \quad \dots \quad (m-1)a} &\Rightarrow \cancel{(m-1)!} a^{m-1} \\ \rightarrow 1 \quad 2 \quad 3 \quad \dots \quad (m-1) &\Rightarrow \cancel{(m-1)!} \pmod m \end{aligned}$$

\uparrow
 $\gcd(a, m) = 1$

(m과 서로소인 수) = $\{b_1, b_2, \dots, b_n\}$

$0 \sim m-1 \rightarrow n < m$

$$\rightarrow \underline{b_1 a \quad b_2 a \quad b_3 a \quad \dots \quad b_n a}$$

$$\Rightarrow \underline{b_1 \quad b_2 \quad b_3 \quad \dots \quad b_n}$$

$$b_1 \dots b_n \cdot a^n \equiv b_1 \dots b_n \pmod m$$

$$\underline{a^n \equiv 1 \pmod m} \quad n: m \text{과 서로소인 수의 수}$$

$\gcd(a, m)$

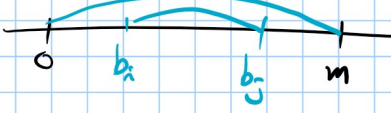
$$a^n \equiv 1 \pmod m \Leftrightarrow m \mid a^n - 1 \Leftrightarrow a^n - 1 = m \cdot k$$

$$\underline{a^n - m \cdot k = 1 \Rightarrow a(a^n) + m(-k) = 1}$$

$ax + my = 1$ 방정식 해* 없*?

* $\gcd(a, m) = 1$

m과 서로소인 수를 b_1, b_2, \dots, b_k 라 하자. $0 \leq b_i < m$

$$\begin{array}{ccccccc} b_1 a & b_2 a & b_3 a & \dots & b_k a & & \\ b_1 & b_2 & b_3 & \dots & b_k & & \end{array}$$


위의 두 목록은 순서를 무시하면 같다.

$$b_i a \quad m b_i, m a \quad m b_i a \Rightarrow b_i a \text{ 는 } m \text{과 서로소}$$

$$b_i a \not\equiv b_j a \pmod m$$

$$\Rightarrow m \mid b_i a - b_j a = a(b_i - b_j) \Rightarrow m \mid \overset{b_i}{b_i} - b_j$$

$b_i - b_j$ 가 m 의 배수. $|b_i - b_j| \leq m-1$

$$b_i - b_j = 0 \Rightarrow b_i = b_j$$

* 오일러의 공식 (페르마의 소정리)

$$\gcd(a, m) = 1 \text{ 이면 } a^{\phi(m)} \equiv 1 \pmod{m}$$

단, n 은 m 과 서로소인 수의 개수

* 오일러 phi (Totient) 함수

$\phi(m) :=$ m 과 서로소인 수의 개수
 m 보다 작고, 0 이상인

$$\phi(p) = p-1 \quad 1, 2, \dots, p-1$$

$$a^{\phi(372)} \equiv 1 \pmod{372}$$