정수론 13강 오일러의 공식 (Euler's Formula)

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

존재

$a\cdot x \equiv 1 \pmod m$

$\Leftrightarrow m \mid ax-1 \Leftrightarrow ax-1 = mk$

$\Leftrightarrow ax - mk = 1 \Leftrightarrow \gcd(a,m) \mid 1$

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

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

$\rightarrow a \quad 2a \quad 3a \quad \cdots \quad (p-1)a \Rightarrow \cancel{(p-1)!}\, a^{p-1}$

$\equiv$

$\rightarrow 1 \quad 2 \quad 3 \quad \cdots \quad (p-1) \Rightarrow \cancel{(p-1)!} \pmod p$

$1 \cdots (m-1)$

$\rightarrow 0a \quad 2a \quad 3a \quad \cdots \quad (m-1)a \Rightarrow (m-1)!\, a^{m-1}$

$\gcd(a,m)=1$

$\equiv$

$\rightarrow 1 \quad 2 \quad 3 \quad \cdots \quad (m-1) \Rightarrow (m-1)! \pmod m$

$1 \cdots (m-1)$

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

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

$\rightarrow b_1 a \quad b_2 a \quad b_3 a \quad \cdots \quad b_n a$

$\Rightarrow b_1 \quad b_2 \quad b_3 \quad \cdots \quad b_n$

$\cancel{b_1}\cdots\cancel{b_n}\cdot a^n \equiv \cancel{b_1}\cdots\cancel{b_n} \pmod m$

$a^n \equiv 1 \pmod m$ n: m과 서로소인 수의 수.

$\gcd(a,m)$

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

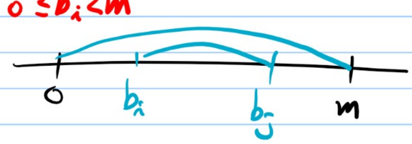
$a^n - \cancel{m\cdot k} = 1 \Rightarrow a\cdot a^{n-1} + m\cdot(-k) = 1$

$ax+my=1$ 방정식 해~~가~~ 없~~으면~~?

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

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

$b_1 a \quad b_2 a \quad b_3 a \quad \cdots \quad b_k a$



$b_1 \quad b_2 \quad b_3 \quad \cdots \quad b_k$

위의 두 목록은 순서를 무시하면 같다.

$b_i a \qquad m \nmid b_i,\ m \nmid a \qquad m \nmid b_i a \Rightarrow$ $b_i a$는 m과 서로소

$\| \; b_\alpha$

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

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

$b_i - b_j$ 가 m의 배수. $|b_i - b_j| \le m-1$

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

* 오일러의 공식 (페르마의 소정리)

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

단, n은 m과 서로소인 수의 개수

* 오일러 phi (Totient) 함수

$\phi(m) :=$ m과 서로소인 수의 개수

m보다 작고, 0 이상 인

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

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