16강 n차 합동방정식

$ax \equiv b \pmod{m}$ $\gcd(a, m) = g$ $g \mid b$, $g \nmid b$

$x^n \equiv b \pmod{p}$ 소수

① $\gcd(n, \phi(p)) = 1$ 일 때만 생각해보자.

$x^n \equiv b \pmod{p} \Rightarrow x \equiv ? \pmod{p}$

$(x^n)^c \equiv x^1 \pmod{p} \rightarrow b^c \equiv x \pmod{p}$

$\equiv x^{t\cdot\phi(p)+1} \equiv x \pmod{p}$

$n\cdot c = t\cdot\phi(p)+1$ c, t를 찾자.

$n\cdot c \equiv 1 \pmod{\phi(p)}$ $\gcd(n, \phi(p)) = 1$ p 소수

$c \equiv n^{-1} \pmod{\phi(p)}$

$x^{nn^{-1}} \equiv b^{n^{-1}} \equiv x \pmod{p}$ $(b^{n^{-1}})^n \equiv b^{t\cdot\phi(p)+1}$

$\gcd(b, p) = 1$ $\equiv b \pmod{p}$

② $\gcd(2, \phi(p)) = g$

$x^2 \equiv b \pmod{p}$

$p \equiv 3 \pmod{4}$ 공식
홀수인 소수
$p \equiv 1 \pmod{4}$ 결정적 → 확장된 리만가설

→ 있는 지 없는지
해의 존재성 판별은 가능

$x^n \equiv b \pmod{m}$

① ① $\gcd(n, \phi(m)) = 1$, ② $\gcd(b, m) = 1$

↳ $n^{-1} \pmod{\phi(m)}$

$b^{n^{-1}} \equiv x \Rightarrow (b^{n^{-1}})^n \equiv b^{t\cdot\phi(m)+1} \equiv b \pmod{m}$

* 해의 유일성

p, q 라는 2개의 해가 존재한다고 가정하자.

$nu = k\cdot\phi(m)+1$ $n\cdot u \equiv 1 \pmod{\phi(m)}$ $p^{nu} \equiv b^u$

$1 = nu - k\cdot\phi(m)$

$p^1 = p^{nu-k\cdot\phi(m)} = p^{nu}\cdot p^{-k\cdot\phi(m)} \equiv b^u \pmod{m}$

$q = q^{nu-k\cdot\phi(m)} = q^{nu}\cdot 1 \equiv b^u \pmod{m}$

$x^n \equiv b \pmod{m}$ $\quad (tA)^n = t^n A^n = t^{g\alpha}A^n = \cancel{t^{p\alpha}}A^n$

$= A^n \equiv b \pmod{m}$

$\gcd(b, m) = 1$, $\gcd(n, \phi(m)) = g \neq 1$ $\quad \boxed{\phi(m)}$

⇒ 해가 존재하지 않거나 혹은 해가 존재한다면 적어도 2개 이상씩 존재한다. $\quad n = g\alpha \quad \phi(m) = g\beta$ $\quad$ 소수 $p|g \Rightarrow p \mid \phi(m)$

실로우. $\quad t^p \equiv 1 \pmod{m}$ $(t \not\equiv 1)$ $\quad g = p \cdot \gamma$

「소수 p가 $p \mid \phi(m) \Rightarrow \gcd(t, m) = 1$ 인 수 중에서 $t^p \equiv 1 \pmod{m}$인 수가 존재한다」

pf) $p \mid \phi(m) \Rightarrow \phi(m) = p \cdot \alpha$

$G = \{ t \mid \gcd(t, m) = 1 \}$

$\forall t \in G$, $t^p \not\equiv 1 \pmod{m} \Rightarrow t^{p\alpha} \not\equiv 1 \pmod{m}$

$t^{\phi(m)} \not\equiv 1 \pmod{m}$

☆ $x^n \equiv b \pmod{m}$ $\quad 12 = 2^2 \cdot 3$

① ① $\gcd(n, \phi(m)) = 1$ $\quad \gcd(b, m) \neq 1$

② m이 서로 다른 소수의 곱으로 이루어진 경우.

$b^{n^{-1} \pmod{\phi(m)}} \equiv x \pmod{m}$