

# 정수론 19강 2차 잉여와 르장드르 기호 (Quadratic residue and Legendre symbol)

\* 암호, 일차 합동방정식,  $x^n \equiv a \pmod{b}$   
 $\hookrightarrow$  해  $x$   $ax \equiv b \pmod{m}$

$a$ 의 역원의 존재성

$$\gcd(a, m) = g \quad \hookrightarrow g=1$$

$$g \nmid b \Rightarrow \text{해} x \text{ 없음}$$

$$g \mid b \Rightarrow g \text{ 개}$$

판별식

$$x^2 \equiv a \pmod{p} \rightarrow \text{존재성}$$

$\hookrightarrow$  2차 잉여 (QR)  $\Rightarrow$  제곱수

0은 NR도 QR도 아니다.

$$x^2 \equiv 0 \pmod{p} \Rightarrow \text{QR}$$

$$\begin{matrix} 2^2 & 3^2 \\ \equiv & \equiv \\ 4 & 9 \end{matrix} \pmod{5}$$

$$\begin{matrix} 4^2 \\ \equiv \\ 16 \end{matrix} \pmod{5}$$

$$\pmod{p}$$

Thm 2가 아닌 소수  $p$ 에 대해서 QR과 NR의 개수는 서로 같다.

$$\pmod{p} \quad 1 \sim p-1 \quad \text{QR: } \frac{p-1}{2} \quad \text{NR: } \frac{p-1}{2}$$

$$p \nmid a_i \quad 1^2, 2^2, 3^2, \dots, (p-2)^2, (p-1)^2 \pmod{p}$$

$$a_i \equiv a_j \pmod{p}$$

중복제거 후 남은 것의 개수  
 $\hookrightarrow$  모든 QR의 개수

$$(p-b)^2 \equiv p^2 - 2pb + b^2 \equiv b^2 \pmod{p}$$

$$1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2 \Rightarrow \text{전부다 QR 이려면}$$

$\Rightarrow$  이들 중 중복은 없다.

귀류법 증명이 있다.  $\alpha^2 \equiv \beta^2 \pmod{p}$

$$\alpha \neq \beta$$

$$\alpha^2 - \beta^2 \equiv (\alpha - \beta)(\alpha + \beta) \equiv 0 \pmod{p}$$

$$p \mid (\alpha - \beta)(\alpha + \beta) \Rightarrow p \mid (\alpha - \beta) \text{ or } p \mid (\alpha + \beta)$$

$$1 \leq \alpha \leq \frac{p-1}{2}$$

$$1 \leq \beta \leq \frac{p-1}{2}$$

$$2 \leq \alpha + \beta \leq p-1$$

$$\alpha \not\equiv \beta \pmod{p}$$



$$* x^2 \equiv a \pmod{p} \quad a: QR \text{ or } NR$$

해답을 찾는 방법

[49]

7x7 QR

$$QR \times QR = QR$$

$$QR \times NR = ?$$

$$NR \times NR = ?$$

$$i) QR \times QR = QR$$

$$a_1, a_2 \Rightarrow a_1 \equiv b_1^2 \pmod{p}, a_2 \equiv b_2^2 \pmod{p}$$

$$a_1 \cdot a_2 \equiv b_1^2 b_2^2 \equiv (b_1 b_2)^2 \pmod{p}$$

$$ii) QR \times NR = NR \quad \text{가정 QR 가정} \Rightarrow \text{모순}$$

$$a_1, a_2 \Rightarrow a_1 \equiv b_1^2 \pmod{p} \quad a_1 \cdot a_2 \equiv b_2^2 \pmod{p}$$

$$a_1 \cdot a_2 \equiv b_1^2 \cdot a_2 \equiv b_2^2 \pmod{p} \quad a_2 \equiv (b_1^{-1})^2 b_2^2 \pmod{p}$$

$$\equiv (b_1^{-1} b_2)^2$$

$$\gcd(b_1, p) = 1 \quad b_1 \not\equiv 0 \pmod{p} \quad a_1 \equiv b_1^2 \equiv 0^2 \pmod{p}$$

QR: 0이 아닌 수

$$iii) NR \times NR = QR$$

pf)  $a: NR$  이라고 하자.

$$\begin{pmatrix} a \cdot 1 & a \cdot 2 & a \cdot 3 & \dots & a \cdot (p-1) \\ 1 & 2 & 3 & \dots & (p-1) \end{pmatrix} \pmod{p}$$

$$(p-1)! \equiv a^{p-1} (p-1)! \pmod{p} \quad \left( \frac{p-1}{2} \text{ 개} \right) \rightarrow \text{QR만 남았다.}$$

QR:  $\frac{p-1}{2}$  개

a가 NR

$$NR \cdot QR \text{ 는 } \frac{p-1}{2} \text{ 회 등장한다.}$$

$$\equiv NR$$

$$NR \cdot NR$$

$$* QR \cdot QR = QR$$

$$1 \cdot 1 = 1$$

$$QR \cdot NR = NR$$

$$1 \cdot (-1) = (-1)$$

$$NR \cdot NR = QR$$

$$(-1) \cdot (-1) = 1$$

$$\left( \frac{a}{p} \right) = \begin{cases} 1 & \text{if } QR \\ -1 & \text{if } NR \end{cases}$$

$$\left( \frac{a}{p} \right) = 1$$

$$\left( \frac{b}{p} \right) = -1$$

$$\left( \frac{ab}{p} \right) = -1$$



$$\star \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \quad \text{은 장 드른 } > | \text{호}$$

$$4 \times 2 \begin{array}{ccc} 1 & 1 & = 1 \\ 1 & -1 & = -1 \\ -1 & 1 & = -1 \\ -1 & -1 & = 1 \end{array}$$

$$\star \left(\frac{a}{p}\right) = \begin{cases} 1 & (a \text{가 mod } p \text{에 대해 QR인 경우}) \\ -1 & ( \quad , \quad , \quad \text{NR} \quad ) \end{cases}$$

$$\star \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \quad \text{NR}$$

$$\left(\frac{a}{\cancel{p}}\right) = \left(\frac{\cancel{a} \cancel{b}}{\cancel{p}}\right) = \left(\frac{b}{\cancel{a}}\right) = \left(\frac{a}{\cancel{b}}\right) = \left(\frac{2}{\cancel{b}}\right)$$