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

QR

* 암호, 일차 합동방정식 $x^n \equiv a \pmod b$

↳ 해x $ax \equiv b \pmod m$ a의 역원의 존재성 $\gcd(a,m)=g$ $g \nmid b \Rightarrow$ 해x

↳ $g=1$ $g \mid b \Rightarrow g$개

판별식

$x^2 \equiv a \pmod p \rightarrow$ 존재성

$2^2\ (5)^2\ 3^2\ 4^2$

$4\ \cancel{25}\ 9\ 16 \pmod p$

↳ 2차 잉여 (QR) ⇒ 제곱수

2차 비잉여 (NR)

0은 NR도 QR도 아니다. $x^2 \equiv 0 \pmod p \Rightarrow QR$

Thm 2가 아닌 소수 p에 대해서 QR과 NR의 개수는 서로 같다.

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

pf) $1^2\ 2^2\ 3^2 \cdots (p-2)^2\ (p-1)^2 \pmod p$

$a_1\ a_2 \cdots a_{p-1}$

$a_i \equiv a_j \pmod p$

{ } 중복제거 후 남은 것의 갯수

↳ 모든 QR의 갯수

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

$1^2\ 2^2 \cdots \left(\frac{p-1}{2}\right)^2$ ⇒ 전부다 QR이어면

$\alpha^2 \quad \beta^2$ ⇒ 이들 중 중복은 없다.

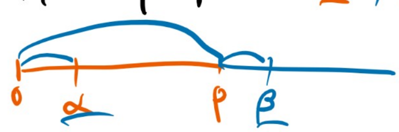
귀류법 중복이 있다. $\alpha^2 \equiv \beta^2 \pmod p$

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

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

$1 \le \alpha \le \frac{p-1}{2}$ $2 \le \alpha+\beta \le p-1$ $\alpha \not\equiv \beta \pmod p$

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



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

합동식 → 정수 $\boxed{49}$ 7×7 QR

$QR \times QR = QR$
$QR \times NR = ?$
$NR \times NR = ?$

i) $\underset{a_1}{QR} \times \underset{a_2}{QR} = QR$

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

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

ii) $\underset{a_1}{QR} \times \underset{a_2}{NR} = NR$ 귀류 QR가정 ⇒ 모순

$\Rightarrow a_1 \equiv b_1^2 \pmod p \qquad a_1 \cdot a_2 \equiv b_2^2 \pmod p$

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

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

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

QR : 0이 아닌 수

iii) $NR \times NR = QR$

pf) a : NR 이라고 하자.

$\frac{p-1}{2}$개

$a \cdot \underline{1} \quad \cancel{a \cdot 2} \quad \cancel{a \cdot 3} \quad \cdots \quad \cancel{a} \cdot (\underline{p-1}) \pmod p$

$1 \quad \cancel{2} \quad 3 \quad \cancel{\cdots} \quad (p-1)$ → QR만 남았다.

$\cancel{(p-1)!} \equiv \underline{a^{p-1}} \cancel{(p-1)!} \pmod p$ $\quad \frac{p-1}{2}$개 → QR $\quad \left\{ \begin{array}{l} \frac{p-1}{2}\text{개 QR} \\ \frac{p-1}{2}\text{개 NR} \end{array} \right\}$

QR : $\frac{p-1}{2}$개

a가 NR

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

$\equiv NR$

$NR \cdot NR$

* $QR \cdot QR = QR \qquad 1 \cdot 1 = 1$
$QR \cdot NR = NR \qquad 1 \cdot (-1) = (-1)$
$NR \cdot NR = QR \qquad (-1) \cdot (-1) = 1$

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

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

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

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$ 르장드르 기호

4가지

1	1	=	1
1	-1	=	-1
-1	1	=	-1
-1	-1	=	1

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

* $\boxed{\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)}$ $\cancel{\frac{ab}{p}}$ NR

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