정수론 20강 오일러 판정법 (Euler's Criterion)

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

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

Q.R. 이차잉여 N.R 이차 비잉여

* 2를 제외한 소수 p에 대해 $\left(\frac{-1}{p}\right)=\begin{cases}1 & (p\equiv 1 \pmod 4)\\ -1 & (p\equiv 3 \pmod 4)\end{cases}$

Thm 오일러 판정법

홀수인 소수 p에 대해 $\boxed{a^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)} \pmod p$

pf) $\left(\frac{a}{p}\right)=\begin{cases}1 & \equiv 1 \pmod p \quad a\text{가 QR일때}\\ -1 & \equiv p-1 \pmod p \quad a\text{가 NR일때}\end{cases}$

$$a^{\frac{p-1}{2}}\equiv\begin{cases}1 & a\text{가 QR일때} \pmod p\\ -1\ (p-1) & a\text{가 NR일때} \pmod p\end{cases}$$

i) a가 QR일 경우 ⇒ $a\equiv b^2 \pmod p$

$$a^{\frac{p-1}{2}}\equiv(\cancel{b^2})^{\frac{p-1}{\cancel{2}}}\equiv b^{p-1}\equiv 1 \pmod p$$

ii) a가 NR일 경우

홀수인 소수

$$a^{p-1}\equiv 1 \pmod p \Rightarrow a^{p-1}-1\equiv(a^{\frac{p-1}{2}}+1)\boxed{(a^{\frac{p-1}{2}}-1)}$$

$$\equiv 0 \pmod p \qquad \not\equiv 0$$

$x^2+2x+1=0$ → 중근 허근, 서로 다른 2개

x^n → n개 x

「n차 합동방정식은 n개 보다 많은 해를 가지지 않는다.」

$X^{\frac{p-1}{2}}\equiv 1 \pmod p$ (p → 홀수인 소수) 최대 $\frac{p-1}{2}$개의 해를 가진다.

QR의 개수: $\frac{p-1}{2}$개 ⇒ QR이 전부다.

$$\therefore a^{\frac{p-1}{2}}+1\equiv 0 \pmod p$$

$$a^{\frac{p-1}{2}}\equiv -1 \pmod p \quad //$$

* $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \frac{p-1}{2}: \text{짝수} \Rightarrow p \equiv 1 \pmod 4 \\ -1 & \frac{p-1}{2}: \text{홀수} \Rightarrow p \equiv 3 \pmod 4 \end{cases}$

* $p = 4k+1 \Rightarrow \frac{p-1}{2} = \frac{4k+1-1}{2} = \frac{4k}{2} = 2k.$

  $p = 4k+3 \Rightarrow \frac{p-1}{2} = \frac{4k+3-1}{2} = \frac{4k+2}{2} = \underline{2k+1}$

* $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1 \text{ or } 7 \pmod 8 \\ -1 & p \equiv 3 \text{ or } 5 \pmod 8 \end{cases}$ $\quad \left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}}$

  $2^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \mod 8 \\ -1 & \end{cases}$

* $p = 19$

  큰 숫자는 음수로 바꿔서 계산하자.

  $2 \cdot 3 \equiv 6 \pmod{19}$ $\qquad 2 \cdot 18 \equiv 2 \cdot (-1) \equiv -2 \equiv 17 \pmod{19}$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
									−9	−8	−7	−6	−5	−4	−3	−2	−1

* 페르마 소정리 아이디어

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

  $a \quad 2a \quad \cdots \quad (p-1)a \quad \pmod p \quad a^{p-1}\cancel{(p-1)!}$

  $a^{p-1} \equiv 1 \pmod p$

* 증명의 아이디어

  홀수: p (2를 제외한 소수)

  $\underline{2} \times \underline{4} \times \underline{6} \cdots (p-3) \times (p-1) = 2^{\frac{p-1}{2}} \cdot \boxed{\cancel{\left(\frac{p-1}{2}\right)!}}$

  $2\cdot1 \quad 2\cdot2 \quad 2\cdot3 \quad 2\cdot4 \quad \cdots \quad 2\cdot\frac{p-1}{2}$

  → 음수로 바꿔서 계산.

  $\cdots -3 \cdot -1$

  $\frac{p-1}{2}$ 이하

  $\underbrace{2 \overset{+2}{\times} 4 \overset{+2}{\times} 6 \cdots}_{\text{짝수}} \Big| \underbrace{\cdots -5 \overset{2}{\times} -3 \overset{2}{\times} -1}_{\text{홀수}} = (-1)^{\frac{p-1}{2}} \cdot \cancel{\left(\frac{p-1}{2}\right)!}$

① (-1) 항의 갯수를 세어보자.

② $\left(\frac{p-1}{2}\right)!$ 항이 잘 나올 것인가.

p	$\frac{p-1}{2}$
$8k+1$	$(8k+1-1)/2 = 8k/2 = 4k$
$8k+3$	$(8k+3-1)/2 = (8k+2)/2 = 4k+1$
$8k+5$	$(8k+5-1)/2 = (8k+4)/2 = 4k+2$
$8k+7$	$4k+3$

	짝수	홀수
$8k+1$)	$2k$개	$2k$개
$8k+3$)	$2k$개	$2k+1$개
$8k+5$)	$2k+1$개	$2k+1$개
$8k+7$)	$2k+1$개	$2k+2$개

개수 차이가 한개 이하.

$$\underbrace{2 \times 4 \times 6 \times \cdots 4k+2 \mid 4k+4 \times \cdots \times (-3) \times (-1)}_{\frac{p-1}{2}\text{개}}$$

$p-1$

$4k+3$

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

$1 \sim \frac{p-1}{2}$ 까지

2 4 6 8 10 12

1 3 5 7 9 11 13

11개