Q6. $p \geq 5$

3 is a quadratic residue modulo p

$\longleftrightarrow p \equiv 1$ or $11 \pmod{12}$

pf) ($\longrightarrow$)

3 is a quadratic residue modulo p, $\gcd(3, p) = 1$

$\longleftrightarrow \left(\frac{3}{p}\right) = 1$ (by Def 121)

$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{3-1}{2}} \cdot \left(\frac{p}{3}\right)$ (by 가우스 상호법칙)

$= 1$

경우의 수는

$\frac{p-1}{2}$	$\left(\frac{p}{3}\right)$
(Case1) 짝수	1
(Case2) 홀수	-1

(Case1) $\frac{p-1}{2} = 2k_1$ ($k_1 \in \mathbb{Z}$)

$p = 4k_1 + 1 \longrightarrow p \equiv 1 \pmod 4$ --- Ⅰ

$\left(\frac{p}{3}\right) = 1 \longleftrightarrow p^{\frac{3-1}{2}} \equiv 1 \pmod 3$ (gcd (3, p) = 1 by 오일러의 Criterion)

$\longrightarrow p \equiv 1 \pmod 3$ --- Ⅱ

(I)+(II) 에 의해

$$\boxed{\begin{aligned} p &\equiv 1 \pmod 4 \\ p &\equiv 1 \pmod 3 \end{aligned}}$$

$4, 3 \in \mathbb{N}$ 각각 pairwise relatively prime

$\rightarrow$ by CRT,

$$p \equiv \underset{3}{N_1} x_1 \cdot 1 + \underset{4}{N_2} x_2 \cdot 1 \pmod{12}$$

$3x_1 \equiv 1 \pmod 4$

$-x_1 \equiv 1 \pmod 4$

$\rightarrow x_1 = -1$

$4x_2 \equiv 1 \pmod 3$

$x_2 \equiv 1 \pmod 3$

$\rightarrow x_2 = 1$

$\therefore p \equiv 3 \cdot (-1) \cdot 1 + 4 \cdot 1 \cdot 1 \equiv 1 \pmod{12}$

$p \equiv 1 \pmod{12}$

(Case 2) $\frac{p-1}{2} = 2k_2 + 1$ $\quad (k_2 \in \mathbb{Z})$

$p = 4k_2 + 3 \longrightarrow p \equiv 3 \pmod 4$ --- ①

$\left(\frac{p}{3}\right) = -1 \longrightarrow p^{\frac{3-1}{2}} \not\equiv 1 \pmod 3$ $\quad$ ($\gcd(3, p) = 1$ by 오일러의 Criterion 의 대우)

$\longrightarrow p \not\equiv 1 \pmod 3$

$p \equiv 0 \pmod 3$ 불가능. 왜냐 $p \geq 5$의 소수이기 때문.

$p \equiv 2 \pmod 3$ 가능.

$\longrightarrow p \equiv 2 \pmod 3$ --- ②

① + ② 에 의해

$$\boxed{\begin{aligned} p &\equiv 3 \pmod{4} \\ p &\equiv 2 \pmod{3} \end{aligned}}$$

4, 3 ∈ ℕ 각각 pairwise relatively prime

$\longrightarrow$ by CRT,

$$p \equiv \underset{3}{n_1} x_1 \cdot 3 + \underset{4}{n_2} x_2 \cdot 2 \pmod{12}$$

$3x_1 \equiv 1 \pmod{4}$

$-x_1 \equiv 1 \pmod{4}$

$\rightarrow x_1 = -1.$

$4x_2 \equiv 1 \pmod{3}$

$x_2 \equiv 1 \pmod{3}$

$\rightarrow x_2 = 1.$

$\therefore p \equiv 3 \cdot (-1) \cdot 3 + 4 \cdot 1 \cdot 2$

$\equiv -1 \pmod{12}$

$p \equiv 11 \pmod{12}$

$\therefore$ Case1), Case2) 에 의해

$p \equiv 1$ or $11 \pmod{12}$ ▨

pf) ($\Longleftarrow$) Case1) $p \equiv 1 \pmod{12}$

Case2) $p \equiv 11 \pmod{12}$

Case1) $p \equiv 1 \pmod{12}$

$p = 12k+1 \quad (k \in \mathbb{Z})$

$\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2}\frac{p-1}{2}}\left(\frac{p}{3}\right)$ (by 가우스 상호법칙)

$= \cancel{(-1)^{1 \cdot 6k}} \cdot \left(\frac{12k+1}{3}\right)$ (by lemma 114)

$= \left(\frac{1}{3}\right)$ (1 은 quadratic residue modulo 3)

$= 1.$

$\Longleftrightarrow$ 3 is a quadratic residue modulo p.

Case2) $p \equiv 11 \pmod{12}$

$p = 12k+11 \quad (k \in \mathbb{Z})$

$\left(\frac{3}{p}\right) = (-1)^{\frac{3-1}{2}\frac{p-1}{2}}\left(\frac{p}{3}\right)$ (by 가우스 상호법칙)

$= (-1)^{1 \cdot \frac{12k+10}{2}} \cdot \left(\frac{12k+11}{3}\right)$ (by lemma 114)

$= (-1)^{6k+5}\left(\frac{3(4k+3)+2}{3}\right)$

$= (-1) \cdot \left(\frac{2}{3}\right)$ ($3 \equiv 3 \pmod{8}$, by Thm 140)

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

$= 1.$

$\Longleftrightarrow$ 3 is a quadratic residue modulo p.

$\therefore$ Case1), Case2) 에 의해

3 is a quadratic residue modulo p. ▨