Q4

$p \geq 7$ p는 prime

$\mathbb{Z}_p^* = \{1, 2, 3, \cdots, p-1\}$

→ There is a pair of Consecutive integers which are both Quadratic Nonresidues Modulo P.

pf) a가 quadratic residue modulo p in the set $\mathbb{Z}_p^* = \{1, 2, \cdots, p-1\}$

$\leftrightarrow \{\phi_p(0^2), \phi_p(1^2), \phi_p(2^2), \cdots, \phi_p\left(\left[\frac{p-1}{2}\right]^2\right)\}$ (by remark 1.16)

$\leftrightarrow \{0, 1, 4, \phi_p(3^2), \phi_p(4^2) \cdots \phi_p\left(\left[\frac{p-1}{2}\right]^2\right)\}$ --- ①

$\left(\because p \geq 7\right)$

suppose that

귀류법 "There is Not a pair of Consecutive integers which are both Quadratic Nonresidues modulo p //

$\mathbb{Z}_p^* = \{1, 2, 3, 4, 5, 6, \cdots, p-1\}$ --- (I)

○ 표시 : quadratic nonresidue modulo p

△ 표시 : quadratic Residue modulo p --- (by ①)

2, 3은 둘다 quadratic Nonresidue modulo p 될 가능.

둘 중 하나가 quadratic Nonresidue modulo p 이거나 둘다 quadratic nonresidue modulo p 아니다. --- ②

(두번째로 작은 quadratic nonresidue modulo p) ≥ 5

$|\mathbb{Z}_p^*| = p-1$

① $\mathbb{Z}_p^*$의 quadratic residue modulo p의 개수 $= \frac{p-1}{2}$ … ②

$\mathbb{Z}_p^*$의 quadratic nonresidue modulo p의 개수 $= \frac{p-1}{2}$ … ③

Let $\mathbb{Z}_p^{**} = \{5, 6, 7, 8, \cdots, p-1\}$

$\mathbb{Z}_p^* = \{1, 2, 3, 4\} \cup \mathbb{Z}_p^{**}$

$\mathbb{Z}_p^{**}$의 quadratic residue modulo p의 개수 : $\frac{p-1}{2} - 2$ (by ①+②)

$|\mathbb{Z}_p^{**}| = p-1-4 = p-5$

$\mathbb{Z}_p^{**}$의 quadratic nonresidue modulo p의 개수 $\begin{cases} \frac{p-1}{2} - 1 & \cdots \text{Case 1} \\ \frac{p-1}{2} & \cdots \text{Case 2} \end{cases}$

(by ② + ③)

Case 1) $|\mathbb{Z}_p^{**}|$ = $\mathbb{Z}_p^{**}$의 quadratic residue modulo p의 개수 + $\mathbb{Z}_p^{**}$의 quadratic nonresidue modulo p의 개수

$|\mathbb{Z}_p^{**}| = (p-5) \neq \left(\frac{p-1}{2} - 2\right) + \left(\frac{p-1}{2} - 1\right) = (\mathbb{Z}_p^{**}\text{의 quadratic residue} + \text{quadratic nonresidue modulo p의 개수})$

$\neq p-4$

따라서 모순이다.

Case 2) $|\mathbb{Z}_p^{**}|$ = $\mathbb{Z}_p^{**}$의 quadratic residue modulo p의 개수 + $\mathbb{Z}_p^{**}$의 quadratic nonresidue modulo p의 개수

$|\mathbb{Z}_p^{**}| = (p-5) \neq \left(\frac{p-1}{2} - 2\right) + \left(\frac{p-1}{2}\right) = (\mathbb{Z}_p^{**}\text{의 quadratic residue} + \text{quadratic nonresidue modulo p의 개수})$

$\neq p-3$

따라서 모순이다.

∴ Case 1), Case 2)에 의해 모순이 생겼으므로 가정이 틀렸다.

→ There is a pair of Consecutive integers which are both quadratic nonresidues modulo p.

ibis