Q7 (a) $a = 2k+1$ $(k \in \mathbb{Z})$

$\rightarrow a^2 = 4k^2+4k+1$

$a^2-1 = 4k^2+4k$

$= 4k(k+1)$

[k가 짝수 $\rightarrow$ $8 \mid 4k(k+1)$

[k가 홀수 $\rightarrow$ $8 \mid 4k(k+1)$

$\therefore 8 \mid 4k(k+1)$ $(k \in \mathbb{Z})$

$\rightarrow 8 \mid a^2-1$

$\rightarrow a^2 \equiv 1 \pmod 8$

(b) p는 홀수 소수

$\left(\frac{-2}{p}\right) = 1 \longleftrightarrow p \equiv 1$ or $3 \pmod 8$

pf) $(\longrightarrow)$ $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)$ (by Thm 131)

$= 1.$

경우의 수는

	$\left(\frac{-1}{p}\right)$	$\left(\frac{2}{p}\right)$
Case1)	$+1$	$+1$
Case2)	-1	-1

$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$ (by Cor 133)

$\left(\frac{-1}{p}\right), (-1)^{\frac{p-1}{2}} \in \{1, -1\}$ (by Lemma 134)

$\rightarrow \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ ...... Ⓐ

Case1) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$ (by Ⓐ)

$\rightarrow \frac{p-1}{2} = 2k$ (for some $k \in \mathbb{Z}$) --- ①

$\left(\frac{2}{p}\right) = 1$

$\rightarrow p \equiv 1$ or $p \equiv 7 \pmod 8$ (by Thm 140) --- ②

①에서

$p = 4k+1$ $(k \in \mathbb{Z})$

②에서

$p = 8k_1 + 1$ $(k_1 \in \mathbb{Z})$ $\boxed{or}$ $p = 8k_2 + 7$ $(k_2 \in \mathbb{Z})$

$\downarrow$ by ①

$4k+\cancel{1} = 8k_1 + \cancel{1}$

$4(k-2k_1) = 0$

$k-2k_1 \in \mathbb{Z}$ 이므로

식이 성립.

$\hookrightarrow p \equiv 1 \pmod 8$

$\downarrow$ by ①

$4k+1 = 8k_2+7$

$4(k-2k_2) = 6$

$k-2k_2 \in \mathbb{Z}$ 이므로

식이 성립하지 않음.

$\cancel{p \equiv 7 \pmod 8}$

Case2) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1$ (by Ⓐ)

$\rightarrow \frac{p-1}{2} = 2k+1$ for some $k \in \mathbb{Z}$. --- ①

$\left(\frac{2}{p}\right) = -1$

$\rightarrow p \equiv 3$ or $p \equiv 5 \pmod 8$ (by Thm 140) --- ②

①에서

$p = 4k+3 \quad (k \in \mathbb{Z})$

②에서

$p = 8k_1 + 3 \quad (k_1 \in \mathbb{Z})$ $\boxed{or}$ $p = 8k_2 + 5 \quad (k_2 \in \mathbb{Z})$

$\downarrow$ by ①

$4k+\cancel{3} = 8k_1 + \cancel{3}$

$4(k-2k_1) = 0$

$k-2k_1 \in \mathbb{Z}$ 이므로

식이 성립

$\hookrightarrow p \equiv 3 \pmod 8$

$\downarrow$ by ①

$4k+3 = 8k_2+5$

$4(k-2k_2) = 2$

$k-2k_2 \in \mathbb{Z}$ 이므로

식이 성립하지 않는다.

$\cancel{p \equiv 5 \pmod 8}$

$\therefore$ Case1), Case2) 에 의해

$p \equiv 1$ or $p \equiv 3 \pmod 8$ $\boxed{///}$

pf) ($\longleftarrow$) Case1) $p \equiv 1 \pmod 8$

Case2) $p \equiv 3 \pmod 8$

Case1) $p \equiv 1 \pmod 8$

$\rightarrow \left(\frac{2}{p}\right) = 1 \quad$ (by Thm 140) ------ Ⅰ

$\rightarrow p-1 = 8k \quad (k \in \mathbb{Z})$

$p-1 = 4 \cdot (2k)$

$\rightarrow 4 \mid p-1$

$\rightarrow p \equiv 1 \pmod 4$

$\leftrightarrow \left(\frac{-1}{p}\right) = 1 \quad$ (by Thm 135) ------ Ⅱ

Ⅰ + Ⅱ 에 의해

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1.$$

Case2) $p \equiv 3 \pmod 8$

$\rightarrow \left(\frac{2}{p}\right) = -1$ ------ Ⅲ

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

$p-3 = 8k \quad (k \in \mathbb{Z})$

$p-1 = 8k+2$

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

$\rightarrow \left(\frac{-1}{p}\right) = (-1)^{4k+1} = (-1)$ ------ Ⅳ

$\therefore$ Ⅲ + Ⅳ 에 의해

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)(-1) = 1$$

▨

Q7 (c) Prove that there are infinitely many primes $\equiv 3 \pmod 8$

귀류법. there are finitely many primes, say

$p_1 < p_2 < \cdots < p_n$ s.t. $p_j \equiv 3 \pmod 8$ $(1 \le j \le n)$ ---- Ⅰ

Consider the number

$N = (p_1 p_2 \cdots p_n)^2 + 2$

Since $N > 3$,

There is an prime factor p of N. ---- Ⅱ

$p \ne p_1, p_2, \cdots, p_n$

$p \mid N \longrightarrow (p_1 p_2 \cdots p_n)^2 \equiv -2 \pmod p$

$\longrightarrow (p_1 p_2 \cdots p_n)$ is a solution of $x^2 \equiv -2 \pmod p$

$\rightarrow -2$ is a qudratic residue modulo p.

$\longrightarrow \left(\frac{-2}{p}\right) = 1$.

by (b),

$\longrightarrow p \equiv 1$ or $3 \pmod 8$ ---- ①

처음가정에 따라,

$p_1 \equiv 3 \pmod 8$, $p_2 \equiv 3 \pmod 8$, $\cdots$, $p_n \equiv 3 \pmod 8$

$\longrightarrow p_i \equiv 3 \pmod 8$ $(1 \le i \le n)$

$\longrightarrow p_1 p_2 p_3 \cdots p_n \equiv 3 \cdot 3 \cdot 3 \cdots 3 \equiv 3^n \pmod 8$

$\longrightarrow (p_1 p_2 p_3 \cdots p_n)^2 \equiv 3^{2n} \pmod 8$

$\equiv 9^n \pmod 8$

$\equiv (\phi_8(9))^n \pmod 8$

$\equiv 1^n \pmod 8$

$\equiv 1 \pmod 8$

$\longrightarrow (P_1P_2P_3\cdots P_n)^2+2 \equiv 3 \pmod 8$

$\longrightarrow N \equiv 3 \pmod 8$ ---- ②

N의 모든 소인수를 $q_1, q_2, \cdots, q_k$ 라 하자. ---- Ⅲ

$p = q_i$ for some $1 \le i \le k$

$N = q_1^{a_1} \cdot q_2^{a_2} \cdot q_3^{a_3} \times \cdots \times q_k^{a_k}$ ---- ③

①에 따라

$q_i \equiv 1$ or $3 \pmod 8$

$\boxed{\text{가정}}$ 모든 q_i가

$q_i \equiv 1 \pmod 8$ 의 식을 만족한다.

$\longrightarrow$ ③에서

$q_1^{a_1} q_2^{a_2} \cdot q_3^{a_3} \times \cdots \times q_k^{a_k} \equiv N \pmod 8$

$(\phi_8(q_1))^{a_1} \cdot (\phi_8(q_2))^{a_2} \cdot (\phi_8(q_3))^{a_3} \times \cdots \times (\phi_8(q_k))^{a_k} \equiv N \pmod 8$

$1^{a_1} \cdot 1^{a_2} \cdot 1^{a_3} \times \cdots \times 1^{a_k} \equiv N \pmod 8$

$N \equiv 1 \pmod 8$

그러나 이 식은 ②에서의 식

$N \equiv 3 \pmod 8$ 과 모순이다. $\longrightarrow$ 가정이 틀림

$\therefore$ 모든 q_i는

$q_i \equiv 1 \pmod 8$의 식을 만족하지 않는다.

$\xrightarrow{\text{①에 의해}}$ 모든 q_i 중

$q_i \equiv 3 \pmod 8$ 을 만족하는 식이 존재한다. ---- Ⅳ

Ⓘ + Ⓘ 에 따라

$p \neq p_1, p_2, \cdots, p_n$

$p = q_i$ for some $1 \le i \le n$

$\rightarrow q_i \neq p_1, p_2, \cdots, p_n$ ———— Ⓐ

Ⓘ + Ⓘ 에 따라

$q_i \equiv 3 \pmod 8$ 인 q_i가 존재하고

$p_1 < p_2 < \cdots < p_n$ 이고

$p_j \equiv 3 \pmod 8$ $(1 \le j \le n)$ 인

모든 유한한 소수 p_i가 있다는 처음가정 에 따라

$q_i = p_j$ 이다. ———— Ⓑ

Ⓐ와 Ⓑ는 모순이므로,

처음 가정이 틀렸다.

↳ There are infinitely many primes $\equiv 3 \pmod 8$ $\boxed{/\!/\!/}$