Q8/ There exist infinitely many primes which are congruent to 3 modulo 4

pf) We see that

$3, 7, 11, 19, 23, 31, \cancel{39}, 43, 47 \cdots$

are primes which are congruent to 3 modulo 4.

$\boxed{\text{귀류법}}$ Suppose on the contrary that there are only finitely many primes which are congruent to 3 modulo 4

$$\left.\begin{array}{l} P_1, P_2, \cdots, P_n \\ \text{with } P_1 < P_2 < \cdots < P_n \end{array}\right\} \cdots (1)$$

Consider the integer

$M = 4P_1P_2P_3 \cdots P_n - 1 \rightarrow 4 \mid (M-3) = 4(P_1P_2 \cdots P_n - 1) \rightarrow M \equiv 3 \pmod 4$

Since $P_n(4P_1P_2P_3 \cdots P_{n-1} - 1) > 1$, $\left(\because P_n \geq 2, \ (4P_1P_2 \cdots P_{n-1} - 1) \geq 2 \right)$

$4P_1P_2 \cdots P_{n-1}P_n - P_n > 1$

$4P_1P_2 \cdots P_n - 1 > P_n$

$\rightarrow M > P_n$.

Since $M > P_n$

P_n is the largest prime by (1),

M is a composite number.

$\rightarrow$ The set

$S = \{ d \in \mathbb{N} \mid d \text{ is a divisor of } M \text{ s.t. } 1 < d < M \}$

is a nonempty subset of $\mathbb{N}$. Let

$m = \min S \ (\geq 2)$

ibis

There are two possible cases:

m is a prime and $m \equiv 3 \pmod 4$

m is a 합성수 and $m \equiv 3 \pmod 4$

Case 1) If m is prime, then

$m = p_2$ s.t. $\begin{cases} p_2 \equiv 3 \pmod 4 \\ 4 \mid p_2 - 3 \end{cases} \rightarrow \begin{matrix} m \equiv 3 \pmod 4 \\ 4 \mid m-3 \end{matrix}$ ---- (1)

$M \equiv 3 \pmod 4$ 이므로
$4 \mid M-3$.

$\begin{cases} M-3 = 4Q \\ M-3 \neq 0 \end{cases}$ $(Q = p_1 p_2 p_3 \cdots p_n - 1)$

$\rightarrow M = 4Q + 3$.

$m \mid M$ 이므로

$\rightarrow M = mq$ $(q \in \mathbb{Z})$ (단 $M > 0$ 이므로 $q \neq 0$)

따라서 $M = 4Q + 3 = mq = 4p_1 p_2 \cdots p_n - 1$

$\rightarrow m = \dfrac{4Q+3}{q}$ $(q \in \mathbb{Z} \setminus \{0\})$ -- (2)

(1)에 의해

$m = p_2$, $\begin{matrix} m \equiv 3 \pmod 4 \\ 4 \mid m-3 \\ \begin{cases} m-3 = 4q_2 \\ m-3 \neq 0 \end{cases} \end{matrix}$ 이 만족해야 한다. ... (3)

(2) (3)에 의해

$m - 3 = \dfrac{4Q+3}{q} - 3 = \dfrac{4Q+3-3q}{q} = 4q_2$

$4Q + 3 = 4q q_2 + 3q$ $(Q = p_1 p_2 p_3 \cdots p_n - 1)$

$4p_1 p_2 p_3 \cdots p_n - 1 = 4q q_2 + 3q$

$\underbrace{p_1 p_2 p_3 \cdots p_n}_{\text{정수}} = \underbrace{q q_2 + \dfrac{3q+1}{4}}_{\text{정수}}$

즉 $\frac{3q+1}{4}$이 정수가 되어야 하는데 이를 만족시키는 $q = 4k+1$ $(k \in \mathbb{Z})$ 형태뿐이다.

예를 들어, $q = 2$ 이면, $\frac{3q+1}{4}$은 정수가 안된다.

따라서, $m \not\equiv 3 \pmod 4$ 인 반례가 존재 $\rightarrow$ (1)과 모순이다.

ibis

Case 2) If m is a composite number,

there is a divisor ℓ of m s.t.

$1 < \ell < m$ ($< M$ because $m \in S$) ---- (3)

Since

$\ell \mid m$ and $m \mid M$,

$\ell \mid M$ ($\because$ Thm 12) ---- (4)

Thus we get by (3) and (4) that

$\ell \in S$ and $1 < \ell < m$.

그러나 이는 가정의 $m = \min S$ 으로부터 모순.

Therefore, we conclude that

there are infinitely many primes

which are congruent to 3 modulo 4