6-(a)

Q6. $n \geq 2$, $n = \prod_{k=1}^{r} p_k^{e_k}$, $\ell \in \mathbb{Z}$.

(a) $\Leftarrow$ $\gcd(\ell, n) = 1$ $\left(\xrightarrow[\text{To show}]{} \gcd(\ell, p_k) = 1 \text{ for all } k = 1, 2, \ldots, r \right)$

Let p_ℓ, p_n are primes s.t. $p_\ell \mid \ell$, $p_n \mid n$

$p_\ell = p_n$ 라 가정하자.

이때 $p_\ell = p_n \mid \gcd(\ell, n)$ 이므로

$p_\ell \leq \gcd(\ell, n) = 1 \longrightarrow p_\ell \leq 1$

그러나 처음 소수가정에 의해 $p_\ell \geq 2$ 모순.

따라서 처음 가정 $p_\ell = p_n$ 는 거짓이다.

$\therefore p_\ell \neq p_n$

ℓ은 두 가지 경우 있다.

Case1) $\ell = 0$ or Case2 $\begin{cases} \ell \neq 0 \\ \ell = p_\ell \cdot q \quad q \in \mathbb{Z} \end{cases}$ --- (ㄱ)

$\gcd(\ell, n) = 1 \longrightarrow \ell \nmid n$ 이고, $\ell \neq 0$ 이다.

따라서 ℓ은 Case 2만 가능.

$\ell \nmid n \rightarrow p_\ell q \nmid n \rightarrow p_\ell \nmid n$ ---(1)

Lemma 59에 의해 p가 소수면

$p \mid n \longleftrightarrow p$는 $\prod_{k=1}^{r} p_k$ 에서 등장한다.

$p \mid n \longleftarrow p$는 $\prod_{k=1}^{r} p_k$ 에서 등장한다. ---- (2)

(2)의 대우도 성립하므로

$p \nmid n \longrightarrow p$는 $\prod_{k=1}^{r} p_k$ 에서 등장하지 않는다. --- (3)

즉 ℓ의 소인수 p_ℓ에 대해 (1)과 (3)을 만족하므로

$p_\ell \nmid n \longrightarrow p_\ell$는 $\prod_{k=1}^{r} p_k$ 에서 등장하지 않는다.

따라서 $P_\ell \neq P_k$ 이다. ---(4)

Suppose that $\gcd(\ell, P_k) \neq 1$ for all $k=1,2,\dots r$.

$\gcd(\ell, P_k)$는 P_k의 약수이므로

$\gcd(\ell, P_k) = \cancel{1}$ or P_k

$\gcd(\ell, P_k) = P_k$

$\rightarrow P_k \mid \ell$, (5)에 의해 $\ell = P_\ell \cdot q$ 이므로

$\rightarrow P_k \mid P_\ell q \quad (q \in \mathbb{Z})$

$q=1$ 이라면, $\underline{P_k \mid P_\ell}$

그러나 (4)에 의해 $P_\ell \neq P_k$, P_ℓ와 P_k는 소수이므로

$\gcd(P_\ell, P_k) = 1$

$\longrightarrow \underline{P_k \nmid P_\ell}$

따라서 반례에 따라 모순이 생기므로

처음 가정 $\gcd(\ell, P_k) \neq 1$ for all $k=1,2\dots r$ 이 틀림

$\rightarrow \gcd(\ell, P_k) = 1$ for all $k=1,2\dots r$ ▨

$(\Leftarrow)$ $\gcd(\ell, P_k) = 1$ for all $k=1,2,\dots r$ $\left(\xrightarrow[\text{To show}]{} \gcd(\ell, n) = 1 \right)$

ℓ은 두가지 경우 존재.

(Case 1) $\ell = 0 \longrightarrow \gcd(\ell, P_k) = P_k \longrightarrow$ 이는 처음가정과 모순.

(Case 2) $\ell \neq 0$

$\left.\ell = P_\ell q \ (q \in \mathbb{Z})\right] \longrightarrow \gcd(\ell, P_k) = 1$ 가능. $\therefore \ell \neq 0$.

----(5)

$\gcd(\ell, P_k) = 1 \rightarrow \ell \nmid P_k$ for all $k=1,2\dots r$ $(\because (5))$

$\rightarrow \ell \nmid P_k \rightarrow P_\ell q \nmid P_k \rightarrow P_\ell \nmid P_k$

$\rightarrow P_\ell \nmid P_1, P_\ell \nmid P_2, \dots P_\ell \nmid P_k \longrightarrow P_\ell \nmid P_1 P_2 P_3 \cdots P_k$

$\rightarrow P_\ell \nmid \prod_{k=1} P_k$ $(\because$ Lemma 57) $(P_\ell$은 소수, $P_k \in \mathbb{Z}$ for all $k=1,2,\dots r)$

$\rightarrow P_\ell \nmid n$ ---- (II)

Suppose that $\gcd(\ell, n) \neq 1$.

$d = \gcd(\ell, n)$ 이라 하면

$d \mid \ell$, $d \mid n$

$\ell = P_\ell q$ 이므로

$d \mid P_\ell q$

만약 $q = 1$ 이면

$d \mid P_\ell$, $d = \cancel{1}$ or P_ℓ

$\rightarrow d = P_\ell$

$d \mid n$ 이므로 $P_\ell \mid n$

허나 이는 (II)와 모순.

즉 반례가 존재하므로

$\gcd(\ell, n) = 1$

$\boxed{///}$

6-(b)

Q6 (b)

$n \geq 2$, $n = \prod_{k=1}^{r} p_k^{e_k}$, $\ell \in \mathbb{Z}$

n의 divisor 中 하나를 d라 하면

$d \mid n \longleftrightarrow d = \prod_{k=1}^{r} p_k^{f_k}$ $(0 \leq f_k \leq e_k)$ (by Thm 64)

$d = \prod_{k=1}^{r} p_k^{f_k}$ 이고 d는 f_k의 값에 따라 변한다. --- (1)

d의 경우의 모든수를 A라 하자. f_k의 모든 경우의 수를 g_k라 하자.

(1)에 따라 A는 $g_1 \times g_2 \times g_3 \cdots \times g_k$ 이 된다

$$A = \prod_{k=1}^{r} g_k \quad \text{---} (2)$$

g_k는 f_k의 범위의 크기 이고 $0 \leq f_k \leq e_k$ 이다.

$g_k = e_k + 1$ --- (3)

(2)(3)에서 $A = \prod_{k=1}^{r} g_k = \prod_{k=1}^{r} (e_k + 1) = (e_1 + 1)(e_2 + 1) \cdots (e_r + 1)$

☐