

i) $m=2$,

$a_1, a_2, N \in \mathbb{Z}$ s.t. $N \neq 0$ o/e

$$\gcd(a_1, N) = 1$$

$$\gcd(a_2, N) = 1$$

$$\rightarrow \gcd(a_1, a_2, N) = 1 \dots (i) \quad (\because \text{Lemma 48})$$

So the assertion is true for $m=2$

ii) Assume that the assertion holds for every $m = 2, 3, 4, \dots, k$ ($k \geq 2$)

iii) Now, consider the case where $m=k+1$.

$m=k$ 일 때 H_0 가정

$$\gcd(a_1, a_2, \dots, a_k, N) = 1 \dots (i) \quad (a_1, a_2, \dots, a_k, N \in \mathbb{Z} \text{ s.t. } N \neq 0)$$

$m=k+1$ 일 때, $a_{k+1}, a_1, a_2, \dots, a_k, N \in \mathbb{Z}$ s.t. $N \neq 0$ o/e

$$\gcd(a_{k+1}, N) = 1$$

$$\xrightarrow{\text{gcd}(a_1, a_2, \dots, a_k, N) = 1 \text{ (i)}} \gcd(a_1, a_2, \dots, a_{k+1}, N) = 1 \quad (\because \text{Lemma 48})$$

Thus the assertion is true for $m=k+1$.

iv) Therefore we conclude that

the assertion is true for every $m \geq 2$ \square