ユークリッドの互除法（別表現）の証明

自然数 a，b について，$a \geqq b$ のとき

$$(a,\ b)=(a-b,\ b)$$

が成り立つことを証明せよ。

証明

$(a,\ b)=g_1$，$(a-b,\ b)=g_2$ とする。

このとき，

$$\begin{cases} a=a_1g_1 \\ b=b_1g_1 \end{cases} \cdots ① \quad (a_1,\ b_1 \text{ は互いに素な自然数})$$

$$\begin{cases} a-b=a_2g_2 \\ b=b_2g_2 \end{cases} \cdots ② \quad (a_2,\ b_2 \text{ は互いに素な自然数})$$

と表せる。

(ア) $g_1 \geqq g_2$ を示す。

② の 2 式を辺々足して，

$a = a_2g_2 + b_2g_2 = g_2(a_2+b_2)$

よって，g_2 は a の約数である。

ここで，g_2 は b の約数でもあるから，g_2 は a と b の公約数。

g_1 が a と b の最大公約数であることから，

$g_1 \geqq g_2$ [(最大公約数)≧(公約数)]

(イ) $g_1 \leqq g_2$ を示す。

① の 2 式を辺々引いて，

$a-b = a_1g_1-b_1g_1 = g_1(a_1-b_1)$

よって，g_1 は $a-b$ の約数である。

ここで，g_1 は b の約数でもあるから，g_1 は $a-b$ と b の公約数。

g_2 が $a-b$ と b の最大公約数であることから，

$g_1 \leqq g_2$ [(公約数)≦(最大公約数)]

(ア)，(イ) より，

$g_1=g_2$ （証明終了）