ユークリッドの互除法（基本表現）の証明

自然数 a，b，q，r が関係式

$$a = bq + r \cdots (☆)$$

を満たすとき，

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

が成り立つことを証明せよ。

証明

$a = bq + r \cdots (☆)$

$(a,\ b) = g_1$，$(b,\ r) = g_2$ とする。

このとき，

$$\begin{cases} a = a_1 g_1 \\ b = b_1 g_1 \end{cases} \cdots ① \quad (a_1,\ b_1 \text{ は互いに素な自然数})$$

$$\begin{cases} b = b_2 g_2 \\ r = r_2 g_2 \end{cases} \cdots ② \quad (b_2,\ r_2 \text{ は互いに素な自然数})$$

と表せる。

(ア) $g_1 \geqq g_2$ を示す。

(☆) と ② より，

$a = bq + r = b_2 g_2 q + r_2 g_2 = g_2(b_2 q + r_2)$

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)$\geqq$(公約数)]

(イ) $g_1 \leqq g_2$ を示す。

(☆) と ① より，

$r = a - bq = a_1 g_1 - b_1 g_1 q = g_1(a_1 - b_1 q)$

よって，g_1 は r 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 b と r の公約数。

g_2 が b と r の最大公約数であることから，

$g_1 \leqq g_2$　[(公約数)$\leqq$(最大公約数)]

(ア)，(イ) より，

$g_1 = g_2$　（証明終了）