ユークリッドの互除法

城北中学校・高等学校　数学科
清水団（しみず・だん）

互除法に関する定理

AとBを自然数とする。AをBで割ったときの商をQ，余りをRとおく。

AとBの最大公約数を$(A,\ B)$で表すことにすると，

$$(A,\ B) = (B,\ R)$$

が成り立つ。(AとBの最大公約数とBとRの最大公約数は等しい)

互除法の証明（1）

$(A,\ B)=k$とおくと，

$$A=ak,\ B=bk,\ a\text{と}b\text{は互いに素}$$

となる。$A=BQ+R$より，

$$ak=bkQ+R$$

$$\therefore R=k(a-bQ)$$

よって，Rはkの倍数となる。

よって，BとRの最大公約数はkの倍数となる。

$$\therefore (A,\ B)\leqq(B,\ R)\cdots(1)$$

互除法の証明（2）

$(B,\ R)=l$とおくと，

$$B=bl,\ R=rl,\ b\text{と}r\text{は互いに素}$$

となる。$A=BQ+R$より，

$$A=blQ+rl=l(bQ+r)$$

よって，Aはlの倍数となる。

よって，AとBの最大公約数はlの倍数となる。

$$\therefore (A,\ B)\geqq(B,\ R)\cdots(2)$$

(1)(2)より，$(A,\ B)=(B,\ R)$

互除法の例

$A=270,\ \ B=120$とすると,

$$270 = 120 \times 2 + 30 \qquad \therefore (270,\ 120) = (120,\ 30)$$

120は30で割りきれるので,

$$(270,\ 120) = (120,\ 30) = 30$$

補題

aとbを互いに素な自然数とする。いま，b個の数

$$a,\ 2a,\ 3a,\ \cdots,\ ba$$

を考える。これらのb個の数をそれぞれbで割ると，0から$b-1$までの余りがすべてでそろう。

補題の証明

自然数k, lを$1 \leqq k < l \leqq b$を満たすものとして，kaとlaをbで割った余りが等しいと仮定すると，

$$ka = bq_1 + r \cdots (1)$$

$$la = bq_2 + r \cdots (2)$$

$(2) - (1)$より，

$$a(l-k) = b(q_2 - q_1)$$

aとbは互いに素なので，$l-k$はbの倍数となるが，$l - k < b$より矛盾。よって，bで割った余りはすべて異なることになり，余りは$0 \leqq r < b$より，0から$b-1$までのすべてがでそろう。

補題の例(1)

$a=7$，$b=5$とすると，aとbは互いに素である。

$$1\times 7,\ 2\times 7,\ 3\times 7,\ 4\times 7,\ 5\times 7$$

すなわち，

$$7,\ 14,\ 21,\ 28,\ 35$$

のそれぞれを5で割った余りは，

$$2,\ 4,\ 1,\ 3,\ 0$$

となり，余りは0から4のすべてでそろう。

補題の例(2)

$a = 6$, $b = 4$とすると，aとbは互いに素ではない。

$$1 \times 6,\ 2 \times 6,\ 3 \times 6,\ 4 \times 6$$

すなわち,

$$6,\ 12,\ 18,\ 24$$

のそれぞれを4で割った余りは,

$$2,\ 0,\ 2,\ 0$$

となり，余りは0から3のすべてはでそろわない。

定理1

aとbを互いに素な自然数とするとき$ax + by = 1$を満たす整数x，yが存在する。

定理1の証明

補題より，$a,\ 2a,\ 3a,\ \cdots,\ ba$を$b$で割ると，余りが$1$となるものが存在する。これを$xa$とする。$xa$を$b$で割ったときの商を$-y$とすれば,

$$ax = b(-y) + 1$$

$$\therefore ax + by = 1$$

定理1の例

- $7x + 5y = 1$を満たす整数x，yは$x = -2,\ y = 3$などがある。
- $4x + 2y = 1$を満たす整数x，yは存在しない。（4と2は互いに素ではない）

定理2

$ax + by = 1$を満たす整数x，y，自然数a，bが存在すれば，aとbは互いに素である。

定理2の証明

aとbは互いに素ではないと仮定すると,

$$a = pk,\ b = pl$$

$$(p\text{は}2\text{以上の自然数},\ l\text{と}k\text{は互いに素})$$

とおける。$ax + by = 1$より,

$$p(kx + ly) = 1$$

$p > 0$より，$p = 1$となるが，$p \geqq 2$に矛盾する。よって，aとbは互いに素である。

定理3

$a < b$とする。aとbが互いに素な自然数であれば，$b - a$とbも互いに素である。

定理3の証明

aとbは互いに素なので，$ax + by = 1$を満たす整数x，yが存在する。（定理1より）

$$\therefore ax + b(x - x + y) = 1$$

$$\therefore (b - a)(-x) + b(x + y) = 1$$

$-x$，$x + y$は整数，$b - a$，bは自然数なので定理2より，$b - a$とbは互いに素である。

定理3の例

120と7は互いに素である。$120 - 7 = 113$より，120と113は互いに素となる。