ユークリッドの互除法

定義 1. $a \in \mathbb{Z}$ に対し，

$$(a) = \{ax \,|x \in \mathbb{Z}\} \tag{1}$$

と定義する．つまり，これは a の倍数全体の集合をあらわす．
さらに，$a, b \in \mathbb{Z}$ に対し，

$$(a, b) = \{ax + by \,|x, y \in \mathbb{Z}\} \tag{2}$$

と定義する．
これらは，環論においてイデアルと呼ばれるものの一例である．

定理 1. $a, b \in \mathbb{Z}$ に対し，$a, b > 0$ とすると，

$$(a) \cap (b) = (c) \tag{3}$$
$$(a, b) = (d) \tag{4}$$

となる正整数 c, d が存在する．
このとき，c は a, b の最小公倍数であり，d は a, b の最大公約数である．

Proof. c, d の存在は補題 1,2 から証明される．
a, b の最小公倍数を j とすると，j は a の倍数だから $j \in (a)$, 同じく $j \in (b)$, よって，

$$j \in (a) \cap (b) = (c) \tag{5}$$

$c, j > 0$ であり，j は c の倍数だから，$c \leq j$. さらに，

$$(a) \cap (b) = (c) \ni c \tag{6}$$

だから，$c \in (a)$ より，c は a の倍数であり，同じく b の倍数でもある．よって c は a, b の正の公倍数であるが，最小公倍数の最小性から $j \leq c$. したがって，$c = j$.
a, b の最大公約数を k とする. $a = ka', b = kb'$ となる $a', b' \in \mathbb{Z}$ が存在する．

$$(a, b) = (d) \ni d \tag{7}$$

だから, $d = ax+by$ を満たす $x, y \in \mathbb{Z}$ が存在する．よって，$d = ka'x+kb'y = k(a'x+b'y)$ となり, $(a'x+b'y) \in \mathbb{Z}$.
$k, d > 0$ だから，$k \leq d$. さらに，$(a, b) = \{ax + by \,|x, y \in \mathbb{Z}\}$ で $x = 1, y = 0$ と $x = 0, y = 1$ の時を考えれば,

$$a, b \in (a, b) = (d) \tag{8}$$

a, b は d の倍数である．よって d は a, b の公約数であるが，最大公約数の最大性から $d \leq k$. したがって，$d = k$ □

正整数 a, b に対し最大公約数を見つける，つまり $(a, b) = (d)$ となる正整数 d を見つけるアルゴリズムがユークリッドの互除法である．

定理 2. 正整数 a, b について $a = qb + r$ $(q, r \in \mathbb{Z})$ となるとき，$(a, b) = (b, r)$ である．

Proof. 任意の $z \in (a, b)$ に対して, ある $x, y \in \mathbb{Z}$ が存在して $z = ax + by$ とかける．$a = qb + r$ だから，

$$\begin{aligned} z &= ax + by && (9)\\ &= (qb + r)x + by && (10)\\ &= b(qx + y) + rx && (11)\\ &= bx' + ry' \in (b, r) && (12) \end{aligned}$$

$x' = qx + y, y' = x$ とおいた．したがって $(a, b) \subset (b, r)$. さらに，任意の $z' \in (b, r)$ は，ある $x', y' \in \mathbb{Z}$ が存在して $z' = bx' + ry'$ とかける．$r = a - qb$ だから，

$$\begin{aligned} z' &= bx' + ry' && (13)\\ &= bx' + (a - qb)y' && (14)\\ &= ay' + b(x' - qy') && (15)\\ &= ax + by \in (a, b) && (16) \end{aligned}$$

$x = y', y = x' - qy'$ とおいた．したがって $(b, r) \subset (a, b)$.
よって，$(a, b) = (b, r)$. □

任意の正整数 $a > b$ に対し整数の割り算を考えると，$a = bq + r$ $(0 \leq r < b)$ となる整数 q, r がとれる．
正整数 $a_0 > a_1$ に対して整数の割り算 $a_0 \div a_1$ をして，商を q_0，余りを a_2 とおく．すると $a_1 > a_2 \geq 0$ である．$a_2 \neq 0$ ならば，$a_1 \div a_2$ の整数の割り算をして商を q_1，余りを a_3 とおく．以下これを繰り返して，

$$a_j = q_j a_{j+1} + a_{j+2} \tag{17}$$

としていく．a_j が正整数であれば，非負整数 $a_{j+1} < a_j$ が求まり，a_j の列を作ることができる．不等号に注意すれば，$a_j \leq a_0 - j$ がわかる．したがって，ある自然数 $m \leq a_0$ が存在して $a_m = 0$ をみたす．まとめると，

$$a_0 > a_1 > a_2 > \cdots > a_{m-1} > a_m = 0 \tag{18}$$

$$(a_0, a_1) = (a_1, a_2) = (a_2, a_3) = \cdots = (a_{m-1}, 0) \tag{19}$$

$d = a_{m-1}$ とおけば，$(a_0, a_1) = (d, 0)$ である．

$$\begin{aligned} (d, 0) &= \{dx + 0y \,|x, y \in \mathbb{Z}\} && (20)\\ &= \{dx \,|x \in \mathbb{Z}\} && (21)\\ &= (d) && (22) \end{aligned}$$

このようにして，a_0, a_1 の最大公約数 d が求まる．
$a_j = q_j a_{j+1} + a_{j+2}$ だから，$a_{j+2} = a_j - q_j a_{j+1}$ である．行列を用いて整理すると，

$$\begin{pmatrix} a_{j+1} \\ a_{j+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_j \end{pmatrix} \begin{pmatrix} a_j \\ a_{j+1} \end{pmatrix} \tag{23}$$

$$\begin{pmatrix} d \\ 0 \end{pmatrix} = \begin{pmatrix} a_{m-1} \\ a_m \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{m-2} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \end{pmatrix} \tag{24}$$

つまり，$\begin{pmatrix} 0 & 1 \\ 1 & -q_{m-2} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix}$ を計算することで，$d = a_0 x + a_1 y$ となる整数 x, y を求めることができる．

[(参考) イデアル]

ここでは整数環しか扱わないので，環の定義は書かないが，足し算引き算掛け算ができるような集合と思えばよい．一般に掛け算は可換とは限らない．たとえば同じサイズの正方行列全体は非可換な環となる．整数環は可換環なので，ここでは可換な環を考え，環 R は可換環であるとする．

定義 2 (イデアル)**.** 環 R に対して部分集合 $I \subset R$ が以下を満たすときイデアルという．

$$0 \in I \tag{25}$$

$$\forall a, b \in I,\ a + b \in I \tag{26}$$

$$\forall a \in I, \forall x \in R,\ ax \in I \tag{27}$$

補題 1. 整数環 $\mathbb{Z}$ において，$a, b \in \mathbb{Z}$ とすると，$(a), (a, b), (a) \cap (b)$ はイデアルである．

Proof. イデアルの定義を満たすことは容易に確認できる． □

補題 2. 整数環 $\mathbb{Z}$ の任意のイデアル I に対して，ある非負整数 a が存在して，$I = (a)$ である．

このように環 R の任意のイデアル I に対して，ある $a \in R$ が存在して，$I = \{ax \,|x \in R\}$ とかけるとき，R は単項イデアル環であるという．整数環 $\mathbb{Z}$ は単項イデアル環である．

Proof. 整数環 $\mathbb{Z}$ の任意のイデアル I について，$I = (0)$ であれば，これは定理を満たす．以下 $I \neq (0)$ とする．

イデアル I は 0 以外の元を持つ．その元を b し，もし $b < 0$ ならば $-1 \times b$ を b として取り直す．$b > 0$ だから，I に正整数が含まれることがわかる．I の中で最小の正整数を a とおき，$I = (a)$ を示す．$a \in I \Leftrightarrow (a) \subset I$ であることはすぐにわかる．

任意の $z \in I$ に対して，$z \in I \Leftrightarrow -z \in I$ であることから，もし $z < 0$ ならば，$-z$ を z と取り直して議論して良い．また，$z, a \in I$ より，$(z, a) \subset I$ である．

$z \notin (a)$ と仮定する．a の最小性から $z > a$. z は a の倍数ではないから，$z = qa + r$ となる正整数 q, r がとれて，$0 < r < a$ である．定理 2 より，

$$I \supset (z, a) = (a, r) \ni r \tag{28}$$

しかし，$0 < r < a$ であるから，これは a の最小性に反する．よって，仮定は誤りであり，$z \in (a)$. ゆえに，$I \subset (a)$. したがって，$I = (a)$ である． □