第2章　整除関係

2.1　割り算と余り

整数全体の集合 $\boldsymbol{Z}$ では，足し算と掛け算が定義されていて通常の演算規則，すなわち，**結合法則，交換法則，分配法則**が成り立っている． さらに，$\boldsymbol{Z}$ は 0 と負の数を含むので，引き算もいつでもできる． しかし割り算は必ずしもできない，つまり割り算の値が整数の範囲に納まらないことがある． このような場合でも，小学校で学んだように「余り」付きの割り算はいつでも可能である． すなわち，2 つの整数 a, b に対して，商 q と余り r が定まり，関係式 $a = qb + r$ が成り立つ． この事実を定理として精密に定式化しておこう．

定理 2.1 (割り算の定理) 任意の $a, b \in \boldsymbol{Z}$（ただし $b \neq 0$）に対して，

$$a = qb + r, \quad 0 \leq r < |b|$$

をみたす $q, r \in \boldsymbol{Z}$ が存在し，しかもそれらの組は一意的に定まる．

証明　はじめに，上のような q, r が存在することを示そう． 集合

$$R = \left\{ a - q\,|b| \;\middle|\; q \in \boldsymbol{Z},\, a - q\,|b| \geq 0 \right\}$$

を考える． q として絶対値の大きい負の整数をとれば，$a - q\,|b| \geq 0$ とできるから，$R \neq \phi$ がわかる． そこで R の最小元 r をとる;　$r = \min R$． この $r \in R$ を実現する $q \in \boldsymbol{Z}$ をとれば，$a = q\,|b| + r$ であるが，ここで，もし $|b| \leq r$ とすると，

$$0 \leq r - |b| = (a - q\,|b|) - |b| = a - (q+1)\,|b| \in R$$

となって，$r = \min R$ に矛盾する． したがって $0 \leq r < |b|$ が成り立つ． $b > 0$ のときは $|b| = b$ だから $a = qb + r$ となるが，$b < 0$ のときも，q のかわりに $-q$ を用いれば同じ式が成り立ち，定理の主張が示された．

次に一意性を示すために

$$a = qb + r = q'b + r', \quad 0 \leq r, r' < |b|$$

として，$q = q', r = r'$ を示そう． もし $q \neq q'$ ならば $|q - q'| \geq 1$ であるから，$|r - r'| = |q - q'|\,|b| \geq |b|$ となって $0 \leq r, r' < |b|$ に矛盾する． よって $q = q'$ であり，これから $r = r'$ も得られる． □

2.2　約数・倍数

前節冒頭に述べたように，$\boldsymbol{Z}$ においては加減乗除のうち 3 つの演算，$+, -, \times$ は自由にできて通常の演算規則が成り立つが，除法すなわち割り算 $\div$ は必ずしもできない．そこで,「割り切れる」かどうかが最初の問題として浮上する．

整数 a が整数 b で割り切れるとは，$a = bc$ をみたす整数 c が存在することである．このとき，b は a の**約数**である，または，a は b の**倍数**であるといい，

$$b|a$$

で表す．$b|a$ でないときは $b\nmid a$ と書く．たとえば $2|6,\ 4\nmid 10,\ 17|51$ である．約数や倍数によって表される整数の関係を**整除関係**という．

1 や -1 はすべての $a \in \boldsymbol{Z}$ の約数であり，0 はすべての $a \in \boldsymbol{Z}$ の倍数である．一方，1 の約数は 1 または -1 だけであり，0 の倍数は 0 だけである．記号 $|$ を使って表せば次のようになる;

- すべての $a \in \boldsymbol{Z}$ に対して，$1|a$ かつ $-1|a$ かつ $a|0$.
- $a|1$ ならば $a = \pm 1$.
- $0|a$ ならば $a = 0$.

これらは，1 と 0 にまつわる極端な性質である．とくに 0 との整除関係は小学校では扱わなかったので少し戸惑うこともあるかもしれないが，もうこどもじゃないもん，慣れれば難しくないもん．次の命題の証明もひとりでできるもん．

命題 2.2 $a, b, c \in \boldsymbol{Z}$ とする．

(1) $a|b$ かつ $b|a$ ならば，$|a| = |b|$.

(2) $c|a$ かつ $c|b$ ならば，任意の $x, y \in \boldsymbol{Z}$ に対して $c|(ax + by)$.

整数 a, b のどちらの約数でもある整数を a, b の**公約数**という．また，a, b どちらの倍数でもある整数を a, b の**公倍数**という．a, b どちらかが 0 でないとき，a, b の公約数で最大のものが存在する．それを a, b の**最大公約数**といい $\gcd(a, b)$ で表す．一方，a, b どちらも 0 でないとき，a, b の正の公倍数のうち最小のものが存在する．それを a, b の**最小公倍数**といい $\mathrm{lcm}(a, b)$ で表す．すなわち，$ab \neq 0$ のとき

$$\gcd(a, b) = \max\left\{ c \in \boldsymbol{N} \,\middle|\, c|a,\ c|b \right\}, \quad \mathrm{lcm}(a, b) = \min\left\{ c \in \boldsymbol{N} \,\middle|\, a|c,\ b|c \right\}.$$

$ab = 0$ のとき（つまり $a = 0$ または $b = 0$ のとき）は，

$$\gcd(a, 0) = |a|, \quad \gcd(0, b) = |b|, \quad \mathrm{lcm}(a, 0) = \mathrm{lcm}(0, b) = 0$$

と定めることにする．

ええっと，上の定義はなんだかややこしいし，0 だけ特別視すっるのってイヤだなあ…．“0 はどんな自然数よりも大きい自然数” とすればうまく定義できそうなんだけど…，ここでは，以下のような定義を採用することにしよう．

定義 2.3 (最大公約数・最小公倍数のホントの定義) a, b を整数とする．

(1) 0 以上の整数 d が a, b の公約数であり，かつ a, b の任意の公約数が d の約数であるとき，d を a, b の**最大公約数**といい $\gcd(a, b)$ で表す．

(2) 0 以上の整数 m が a, b の公倍数であり，かつ a, b の任意の公倍数が m の倍数であるとき，m を a, b の**最小公倍数**といい $\mathrm{lcm}(a, b)$ で表す．

この定義が前ページの “定義” と同じであることの確認は，演習としよう．

命題 2.4 $a, b \in \boldsymbol{Z}$ とする． 整数を成分とする 2 次正方行列 A に対して，$c, d \in \boldsymbol{Z}$ を

$$A\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix}$$

によって定めると，次が成り立つ．

(1) $\gcd(a, b) | \gcd(c, d)$.

(2) $\det A = \pm 1$ ならば $\gcd(a, b) = \gcd(c, d)$.

証明 $A = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ とおくと，$c = ax + by$, $d = az + bw$ である． $g = \gcd(a, b)$ ならば $g|a$, $g|b$ だから，命題 2.2 (2) を使って $g|c$, $g|d$. したがって g は c, d の公約数となるから $g | \gcd(c, d)$ であり (1) が示された． (2) を示すために $\det A = \pm 1$ とすると，A の逆行列 $B = A^{-1}$ も整数を成分とする 2 次正方行列で $B\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$ をみたすから，(1) より $\gcd(c, d) | \gcd(a, b)$ であり，これから (2) が成り立つことがわかる． □

2.3 ユークリッドの互除法

割り算の定理の応用として，2 つの整数の最大公約数を効率よく求める方法が，以下に述べる**ユークリッドの互除法**である． 整数 a, b に対して $\gcd(a, b) = \gcd(|a|, |b|)$ かつ $\gcd(a, 0) = |a|$ なので，はじめから $b > 0$ として最大公約数を考えればよい．

定理 2.5 (ユークリッドの互除法) 整数 a, b（ただし $b > 0$）に対して，$a_0 = a$, $a_1 = b$ とおき，数列 $\{a_n\}_{n=0,1,\cdots}$ を，$a_n \neq 0$ である限り

$$a_{n-1} = q_n a_n + a_{n+1}, \quad 0 \leq a_{n+1} < a_n$$

によって定めることができる． さらに，ある $N \geq 1$ に対して $a_{N+1} = 0$ となり，そのとき

$$a_N = \gcd(a, b)$$

が成り立つ．

証明　まず，定理 2.1 を繰り返し適用すれば，数列 $\{a_n\}_{n=0,1,\cdots}$ が定まることはすぐにわかる．また，$0 \leq \cdots < a_2 < a_1 = b$ だから，この操作を（多くとも b 回）繰り返せば $a_{N+1} = 0$ となる $N \geq 1$ が得られることがわかる．一方，

$$\begin{pmatrix} a_{n-1} \\ a_n \end{pmatrix} = \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix}, \qquad \begin{vmatrix} q_n & 1 \\ 1 & 0 \end{vmatrix} = -1$$

なので，命題 2.4 によって $\gcd(a_{n-1}, a_n) = \gcd(a_n, a_{n+1})$ であり，これを繰り返せば，

$$\gcd(a, b) = \gcd(a_0, a_1) = \gcd(a_1, a_2) = \cdots = \gcd(a_N, a_{N+1}) = \gcd(a_N, 0) = a_N$$

となる．□

定理 2.6 $a, b \in \boldsymbol{Z}$ の最大公約数を d とすると，

$$ax + by = d$$

をみたす $x, y \in \boldsymbol{Z}$ が存在する．

証明　$b > 0$ のときにのみ確かめれば十分である．このとき，前定理の証明から，2 次正方行列 A で $\begin{pmatrix} a \\ b \end{pmatrix} = A \begin{pmatrix} d \\ 0 \end{pmatrix}$, $\det A = \pm 1$ をみたすものがとれる．そこで，A^{-1} の第 1 行を (x, y) とすれば，$x, y \in \boldsymbol{Z}$ であり $ax + by = d$ を得る．□

証明中の A^{-1} は，定理 2.5 の証明に現れる行列 $\begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}$ の逆行列 $\begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix}$ の積

$$A^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_N \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{N-1} \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}$$

として計算でき，原理的にはこれから x, y を求めることができる．

例 2.7 ユークリッドの互除法を用いて，201609 と 219294 の最大公約数を求めてみよう．

$$\begin{aligned} 219294 &= 1 \cdot 201609 + 17685, \\ 201609 &= 11 \cdot 17685 + 7074, \\ 17685 &= 2 \cdot 7074 + 3537, \\ 7074 &= 2 \cdot 3537 + 0 \end{aligned}$$

より $\gcd(201609, 219294) = 3537$ を得る．また，

$$201609x + 219294y = 3537$$

をみたす (x, y) を見つけるには，上述のように行列の積を計算すればよいが，ここでは上の計算を逆にたどって求めてみる．

$$\begin{aligned} 3537 &= 17685 - 2 \cdot 7074 = 17685 - 2 \cdot (201609 - 11 \cdot 17685) \\ &= 23 \cdot 17685 - 2 \cdot 201609 = 23 \cdot (219294 - 201609) - 2 \cdot 201609 \\ &= 23 \cdot 219294 - 25 \cdot 201609 \end{aligned}$$

したがって，$(x, y) = (-25, 23)$ が得られる．