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　絶対値の大きい負の整数 x をとれば，$a - x\,|b| \geq 0$ とできるから，集合

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

は空集合ではない． 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 $x \in \boldsymbol{Z}$ をあらためて p と書けば，$a = p\,|b| + r$ であるが，ここで，もし $|b| \leq r$ とすると，

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

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． さらに，b の正負にしたがって $q = \pm p$ とおけば，$a = qb + r$ が成り立つ．

次に一意性を示すために，整数 q, r, q', r' が

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

をみたすとして，$q = q', r = r'$ 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 $\boldsymbol{Z}$ における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 $2|6,\ 4\nmid 10,\ (-3)|12$ 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 や負の整数との整除関係は，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けれど，もうこどもじゃないもん，慣れれば難しくないもん． 次の命題もひとりで証明できるもん．

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**公約数**とは a, b のどちらの約数でもある整数のことであり，**公倍数**とはどちらの倍数でもある整数のことである． さて，次に述べる最大公約数と最小公倍数の定義は，小学校で学んだものとちょっと違っているが，これがおとなの定義である．

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.

なぜ，このような定義を採用するのか？ 小学校では，正の整数つまり自然数のペアについてだけこれらを定義したのだが，ここでは，0 や負の整数も含めて例外なしに一般の整数のペアを扱うため，というのが理由のひとつである． ここで，$ab \neq 0$ のとき（つまり

a も b も 0 でないとき）は，確かに，公約数である “最大の自然数” が最大公約数，公倍数である “最小の自然数” が最小公倍数になっている;

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

一方，$ab = 0$ のとき（つまり $a = 0$ または $b = 0$ のとき）は，

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

となっている．

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，命題 2.2 (1) より，(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，整数列 $\{a_n\}_{n=0,1,\cdots}$ を，$a_n \neq 0$ である限り

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

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，$b = a_1 > a_2 > \cdots \geq 0$ 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．　□

例 2.7　ユークリッドの互除法を用いて，220426 と 196373 の最大公約数を求めてみよう．

$$\begin{aligned} 220426 &= 1 \cdot 196373 + 24053, \\ 196373 &= 8 \cdot 24053 + 3949, \\ 24053 &= 6 \cdot 3949 + 359, \\ 3949 &= 11 \cdot 359 + 0 \end{aligned}$$

より $\gcd(220426, 196373) = 359$ を得る．　また，

$$220426x + 196373y = 359$$

をみたす整数の組 (x, y) を見つけるには，上の計算を逆にたどって，

$$\begin{aligned} 359 &= 24053 - 6 \cdot 3949 = 24053 - 6 \cdot (196373 - 8 \cdot 24053) = 49 \cdot 24053 - 6 \cdot 196373 \\ &= 49 \cdot (220426 - 196373) - 6 \cdot 196373 = 49 \cdot 220426 - 55 \cdot 196373 \end{aligned}$$

よって，$(x, y) = (49, -55)$ が得られる．　別の方法として，定理 2.6 の証明に現れる行列 A の逆行列 A^{-1} の第 1 行を計算する方法がある．　$\begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix}$ に注意して，今の場合に適用すれば，

$$A^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -11 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -6 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -8 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 49 & -55 \\ * & * \end{pmatrix}$$

となって $(x, y) = (49, -55)$ が求まる（A^{-1} の第 2 行は計算しなくてよいので，ほんのちょっとトクした気分になる）．