1　整数

整数全体の集合 $\mathbb{Z}$ を考える．$\mathbb{Z}$ においては，足し算，引き算，掛け算が自由にできる．すなわち，任意の $a, b \in \mathbb{Z}$ に対し，

$$a + b \in \mathbb{Z} \quad \text{かつ} \quad ab \in \mathbb{Z} \tag{1.1}$$

である．

1.1　約数，倍数

定義 1.1. 2 つの整数 a, b（$a \neq 0$ とする）について，$b = qa$ を満たす $q \in \mathbb{Z}$ が存在するとき，

b は a で割り切れる．
a は b を割り切る．
a は b の約数である．
b は a の倍数である．

といい，

$$a \mid b \tag{1.2}$$

と記す．$a \mid b$ の否定，すなわち，a は b の約数でないことを，$a \nmid b$ と記す．

命題 1.1. 整数 a, b, c について，以下が成り立つ．

(1) $a \mid b$ かつ $a \mid c$ ならば $a \mid (b \pm c)$

(2) $a \mid b$ ならば $a \mid (bc)$

(3) $a \mid b$ かつ $b \mid c$ ならば $a \mid c$

(4) $a \mid b \iff (-a) \mid b$

(5) $a \mid b$ かつ $b \mid a \iff a = \pm b$

証明　ここでは，(1),(5) のみ示す．

(1) $a \mid b$ かつ $a \mid c$ とする．定義より，$b = qa$, $c = q'a$ を満たす $q, q' \in \mathbb{Z}$ が存在する．よって，$b \pm c = (q \pm q')a$ である．$q \pm q' \in \mathbb{Z}$ だから，$a \mid (b \pm c)$ が成り立つ．

(5) $a \mid b$ かつ $b \mid a$ とする．定義より，$b = qa$, $a = q'b$ を満たす $q, q' \in \mathbb{Z}$ が存在する．このとき，$a = q'qa$ より $q'q = 1$ である．$q, q' \in \mathbb{Z}$ だから $q = q' = \pm 1$ である．従って，$a = \pm b$ が成り立つ．　□

命題 1.1 の (4) より，$b \in \mathbb{Z}$ を割り切る整数は，正のものと負のものとが対になっている．このため，b の約数という場合，正のもの（すなわち自然数）だけを指すのが習慣になっている．以下では，この習慣に従うことにする．

定義 1.2. $a, b \in \mathbb{Z}$ について，2 つに共通の約数 d を a と b の公約数という．（正の）公約数 g であって，

$$d \text{ は } a \text{ と } b \text{ の公約数} \iff d \text{ は } g \text{ の約数} \tag{1.3}$$

を満たすものを最大公約数といい，$\gcd(a, b)$ で表す．$\gcd(a, b) = 1$ のとき，a と b は互いに素であるという．

命題 1.2. $a, b, c \in \mathbb{Z}$ とする．

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

(2) $\gcd(a, b + ac) = \gcd(a, b)$

(3) d が a と b の公約数ならば，

$$\gcd(a/d, b/d) = \gcd(a, b)/d \tag{1.4}$$

である．特に，$g = \gcd(a, b)$ とすると，$\gcd(a/g, b/g) = 1$ である．

証明

(1) 定義より明らか.

(2) ここでは省略．応用初等代数演習（第 1 回）に譲る.

(3) 自然数 d' について，

$$\begin{aligned} & d' \mid \frac{a}{d} \quad \text{かつ} \quad d' \mid \frac{b}{d} \\ \overset{\text{定義 1.1}}{\Longleftrightarrow} \quad & dd' \mid a \quad \text{かつ} \quad dd' \mid b \\ \overset{\text{定義 1.2}}{\Longleftrightarrow} \quad & dd' \mid \gcd(a,b) \\ \overset{\text{定義 1.1}}{\Longleftrightarrow} \quad & d' \mid \frac{\gcd(a,b)}{d} \end{aligned}$$

が成り立つから，最大公約数の定義より (3) がわかる． □

定義 1.3. $a, b \in \mathbb{Z}$ について，2 つに共通の倍数 m を a と b の公倍数という．正の公倍数のうちで最小のものを最小公倍数といい，$\mathrm{lcm}\,(a,b)$ で表す.

命題 1.3. 正の整数 a, b に対し，$\ell = \mathrm{lcm}\,(a,b)$ とする.

(1) m は a と b の公倍数である $\iff$ m は ℓ の倍数である.

(2) $g = \gcd(a,b)$ とすると，$\ell g = ab$ である.

証明

(1) $\Leftarrow$ は（公倍数と最小公倍数の）定義より明らか．$\Rightarrow$ を示す．m が a, b の公倍数であるとする.

$$m = q\ell + r \quad (0 \leq r < \ell) \tag{1.5}$$

であるとしよう．このとき，m と ℓ は a, b の公倍数だから，r も a, b の公倍数である．しかも，r は $0 \leq r < \ell$ を満たすので，ℓ の最小性より $r = 0$ である．よって，$\ell \mid m$ である.

(2) (1) より ab は ℓ の倍数だから，

$$ab = \ell d \quad (d \in \mathbb{N}) \tag{1.6}$$

と表せる．このとき，

$$a = \frac{\ell}{b}\, d, \quad b = \frac{\ell}{a}\, d \tag{1.7}$$

から，d は a, b の公約数である．よって，$d \mid g$ である．

一方，

$$\frac{ab}{g} = a\,\frac{b}{g} = b\,\frac{a}{g} \tag{1.8}$$

から，$\dfrac{ab}{g}$ は a, b の公倍数である．よって，(1) より $\ell \mid \dfrac{ab}{g}$ である．これと $ab = \ell d$ より，$g \mid d$ を得る．

以上より，$d \mid g$ かつ $g \mid d$ だから，$d = g$ である． □

3 つ以上の整数 $a, b, c, \ldots$ に対しても，最大公約数や最小公倍数を同様に定義できる．

1.2　1 次不定方程式

$a, b \in \mathbb{Z}$ に対し，$g = \gcd(a, b)$ とする．このとき，$x, y \in \mathbb{Z}$ ならば，$ax + by$ が g の倍数であることは明らかである．では逆に，g の倍数を任意に選んだとき，それは

$$ax + by \quad (x, y \in \mathbb{Z}) \tag{1.9}$$

という形で表されるだろうか？

定理 1.4. $a, b \in \mathbb{Z}$ に対し，$g = \gcd(a, b)$ とする．このとき，

$$ax + by = g \tag{1.10}$$

を満たす $x, y \in \mathbb{Z}$ が存在する．

証明　$a, b > 0$ としても一般性は失われない．集合 I を

$$I = \{ax + by \,|\, x, y \in \mathbb{Z}\} \tag{1.11}$$

で定める．I に属する正の整数のうち，最小のものを d とする（$a, b \in I$ だから，I に正の整数が属することは保証されている）．このとき，$x_0, y_0 \in \mathbb{Z}$ が存在して，

$$d = ax_0 + by_0 \tag{1.12}$$

と表せる．このことと，$g \mid a$ かつ $g \mid b$ であることより，$g \mid d$ であることがわかる．

さて，

$$a = qd + r \quad (0 \leq r < d) \tag{1.13}$$

であるとする．このとき，

$$r = a - qd = a(1 - qx_0) + b(-qy_0) \tag{1.14}$$

より，$r \in I$ である．$0 \leq r < d$ であるから，d の最小性より $r = 0$ である．よって，$d \mid a$ である．同様に，$d \mid b$ もわかる．すなわち，d は a と b の公約数であるから，$d \mid g$ である．

以上で，$g \mid d$ かつ $d \mid g$ がわかったので，$d = g$ である．従って，$g = ax_0 + by_0$ が成り立つ．　□

定理 1.4 から，以下がわかる．

命題 1.5. $a, b \in \mathbb{Z}$ に対し，$g = \gcd(a, b)$ とする．集合 I を

$$I = \{ax + by \,|\, x, y \in \mathbb{Z}\} \tag{1.15}$$

で定めると，I は g の倍数の集合に一致する．すなわち，$J = \{gk \,|\, k \in \mathbb{Z}\}$ として，$I = J$ である．

証明　**定理 1.4** より，g の倍数 $gk\,(k \in \mathbb{Z})$ は

$$gk = a(kx) + b(ky) \tag{1.16}$$

と書けるから，集合 I に属することがわかる．すなわち，$J \subset I$ である．次に，$I \subset J$ を示そう．a, b は $g = \gcd(a, b)$ の倍数だから，集合 I の任意の元 $ax + by$ は

$$ax + by = g(a'x + b'y) \tag{1.17}$$

と書け，従って g の倍数である．すなわち，$I \subset J$ である．　□

$m \in \mathbb{N}$ を固定し，m の倍数全体の集合を $m\mathbb{Z}$ と書く．すなわち，

$$m\mathbb{Z} := \{mk \,|\, k \in \mathbb{Z}\} \tag{1.18}$$

である．

命題 1.6. 集合 $m\mathbb{Z}$ に対し，以下が成り立つ．

(1) $m\mathbb{Z}$ は空集合でない．

(2) $a, b \in m\mathbb{Z}$ ならば $a + b \in m\mathbb{Z}$ である．

(3) $a \in m\mathbb{Z}$ かつ $r \in \mathbb{Z}$ ならば $ra \in m\mathbb{Z}$ である．

注釈 1.1. 加法と乗法が適切に定義された集合を環という（**第 3 節** を参照）．環の部分集合であって，上の命題の性質を満たすものをイデアルという．詳細は，代数学 II で学ぶ．

定理 1.4 は，$ax + by = g$ の解が（少なくともひとつ）存在することを保証しているが,「解がどれくらいあるか」という問に対しては何も答えていない．$ax + by = g$ の両辺を g で割ると，$a'x + b'y = 1$ を得る．ここで，$a' = \dfrac{a}{g}$, $b' = \dfrac{b}{g}$ だから，**命題 1.2** (3) より，$\gcd(a', b') = 1$ である．従って，$\gcd(a, b) = 1$ の場合を考えれば十分である．

命題 1.7. $a, b \in \mathbb{Z}$ および $\gcd(a, b) = 1$ とする．$x, y \in \mathbb{Z}$ に関する方程式

$$ax + by = 1 \tag{1.19}$$

の解のひとつを $(x, y) = (x_0, y_0)$ とする．このとき，任意の解は，

$$x = x_0 + bt, \quad y = y_0 - at \qquad (t \in \mathbb{Z}) \tag{1.20}$$

と表せる．

証明　$ax + by = 1$ および $ax_0 + by_0 = 1$ より，

$$a(x - x_0) + b(y - y_0) = 0 \tag{1.21}$$

すなわち，$b(y - y_0) = -a(x - x_0)$ である．$\gcd(a, b) = 1$ より，$x - x_0$ は b の倍数である[1]．よって，

$$x = x_0 + bt \quad (t \in \mathbb{Z}) \tag{1.22}$$

と表される．これより，$y = y_0 - at$ を得る．こうして，解が (1.20) と表されることが示された．逆に，(1.20) が (1.19) の解を与えることは明らかである．　□

[1] 応用初等代数演習（第 1 回）を参照

例 1.1. $\gcd(35, 109) = 1$ である．$35x + 109y = 1$ を満たす $x, y \in \mathbb{Z}$ をすべて求めよう．ユークリッドの互除法を適用すると，

$$\begin{aligned} 109 &= 3 \times 35 + 4 \\ 35 &= 8 \times 4 + 3 \\ 4 &= 1 \times 3 + 1 \end{aligned} \tag{1.23}$$

である．これを逆に辿ると，

$$\begin{aligned} 1 &= 4 - 3 = 4 - (35 - 8 \times 4) = -35 + 9 \times 4 \\ &= -35 + 9 \times (109 - 3 \times 35) = -28 \times 35 + 9 \times 109 \end{aligned}$$

である．従って，$x = -28, y = 9$ が条件を満たすことがわかる．従って，一般解は

$$x = -28 + 109t, \quad y = 9 - 35t \qquad (t \in \mathbb{Z}) \tag{1.24}$$

で与えられる．