# 2　$\mathbb{Z}$ の整除関係

## 2.1　解説編

次の問題を例に取り, 基本的な命題を定義だけを使って証明してみる.

**問題 A.** $a, b, c \in \mathbb{Z}$ に対して「$b \mid a$ かつ $c \mid b \Longrightarrow c \mid a$」を示せ.

定義から直接示そう[1]. 「$b \mid a$ ($b$ は $a$ の約数である; $a$ は $b$ の倍数である; $b$ は $a$ を割り切る)」の定義は次のものである.

**定義 2.1.** $b \mid a \overset{\text{def}}{\Longleftrightarrow} \exists c \in \mathbb{Z}$ s.t. $a = bc$. □

[**問題 A の解**]　$b \mid a$ かつ $c \mid b$ より, $\exists d\ \exists e \in \mathbb{Z}$ s.t. $a = bd$ かつ $b = ce$. このとき

$$a = bd = (ce)d = c(ed)$$

であり $ed \in \mathbb{Z}$ より $c \mid a$ となる. □

**定義 2.2.** 整数 $a$ に対して, $a$ の倍数全体の集合を $a\mathbb{Z}$ と表わすことにする. つまり,

$$a\mathbb{Z} := \{ac \mid c \in \mathbb{Z}\} = \{0, \pm a, \pm 2a, \dots\}.$$

## 2.2　問題編

**問題 2.1.** $a, b, c \in \mathbb{Z}$ について次を示せ.

(1) $c \mid a$ かつ $c \mid b \Longrightarrow c \mid (a + b)$.

(2) $c \mid a$ ならば, 任意の $x \in \mathbb{Z}$ について $c \mid ax$.

**問題 2.2.** $a, b, c \in \mathbb{Z}$ について次を示せ.

(1) $c \mid a$ かつ $c \mid b$ ならば, 任意の $x, y \in \mathbb{Z}$ について $c \mid (ax + by)$.

(2) $b \mid a$ かつ $a \mid b \Longrightarrow a = \pm b$. ただし簡単のために, $a \neq 0$ を仮定する.

**問題 2.3.** 次の (1)~(6) について, 正しい命題には証明を, 正しくない命題には反例を与えよ. ただし $a, b \in \mathbb{N}$ とし, 「$b \nmid a$」は 「$b$ は $a$ の約数でない」を意味する. 必要ならば「素因数分解の一意性」を使って良いことにする.

(1) $b \mid a \Longrightarrow b^2 \mid a^2$.　(2) $b^2 \mid a^2 \Longrightarrow b \mid a$.　(3) $b \nmid a \Longrightarrow b^2 \nmid a$.
(4) $b^2 \nmid a \Longrightarrow b \nmid a$.　(5) $b \nmid a \Longrightarrow b \nmid a^2$.　(6) $b \nmid a^2 \Longrightarrow b \nmid a$.

**問題 2.4.** $a, b$ を自然数とする. 以下の条件のうちで「$b \mid a$」と同値なものはどれか?

(1) $a\mathbb{Z} \cap b\mathbb{Z} = \{0\}$.　(2) $a\mathbb{Z} \cup b\mathbb{Z} = \mathbb{Z}$.　(3) $a\mathbb{Z} \subset b\mathbb{Z}$.　(4) $b\mathbb{Z} \subset a\mathbb{Z}$.

[1] どうみても明らかな簡単な命題を定義だけを使って一見回りくどく証明する, という習慣をつけておくと, ややこしそうな証明も意外にすんなりできるようになります.

**定義 2.3.** $a, b$ を共に 0 でない整数とし,

$$\gcd(a,b) := \max\{c \in \mathbb{N} \mid c \mid a \text{ かつ } c \mid b\},$$
$$\mathrm{lcm}(a,b) := \min\{c \in \mathbb{N} \mid a \mid c \text{ かつ } b \mid c\}$$

とおく. $\gcd(a,b)$ を $a$ **と** $b$ **の最大公約数**, $\mathrm{lcm}(a,b)$ を $a$ **と** $b$ **の最小公倍数**という. □

**いまから「割り算の定理 (原理)」を使って良いことにする.**

**問題 2.5.** $a, b$ を共に 0 でない整数, $m, d \in \mathbb{N}$ とする. 次を示せ.

(1) $m = \mathrm{lcm}(a,b)$ ならば $m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$.

(2) $d = \gcd(a,b)$ ならば $d\mathbb{Z} \supset a\mathbb{Z} \cup b\mathbb{Z}$.

(3) $I := \{ax + by \mid x, y \in \mathbb{Z}\}$ とおく. $d = \gcd(a,b)$ ならば $d\mathbb{Z} \supset I$.

**注意 2.4.** 問題 2.5 (1) は $a$ と $b$ の最小公倍数の特徴付けを与えている.

$$m := \min\{c \in \mathbb{N} \mid a \mid c \text{ かつ } b \mid c\}$$

とおく. $m\mathbb{Z} \subset a\mathbb{Z} \cap b\mathbb{Z}$ が成り立つことから (問題 2.4 により),

(1) $a \mid m$ かつ $b \mid m$. (つまり, $m$ は $a$ と $b$ の公倍数.)

$m\mathbb{Z} \supset a\mathbb{Z} \cap b\mathbb{Z}$ が成り立つことから,

(2) $c \in \mathbb{N}$, $a \mid c$ かつ $b \mid c \implies m \mid c$.

$m' \in \mathbb{N}$ が「条件 (1) かつ (2)」をみたすなら問題 2.2 (2) により, $m = m'$ となる. このように最小公倍数 $m$ は「条件 (1) かつ (2)」により唯 1 つに定まる.

同様に, $a$ と $b$ の最大公約数の特徴付けが存在する. しかしながら, いまそれを証明することはできない. もっと知識を深めてからわかる. □