3　Euclid の互除法, 最大公約数

3.1　解説編

講義プリントの定義 3.3 において「最大公約数」が再定義される. 注意 2.4 の続きとして, これについて少し解説する.

定義 3.1. (**最大公約数**)　$a_1, \ldots, a_n$ を n 個の整数とする. そのとき**講義プリントの定理 3.2(2)** により,

$$\{a_1x_1 + \cdots + a_nx_n \mid x_1, \ldots, x_n \in \mathbb{Z}\} = d\mathbb{Z}$$

をみたす整数 $d \geq 0$ が唯 1 つ存在する. (一意性は問題 2.4 と問題 2.2(2) からわかる.) そこで d を $a_1, \ldots, a_n$ の**最大公約数** (the greatest common divisor) といい, 記号で $d = \gcd(a_1, \ldots, a_n)$ と表わす. □

この整数 $d \geq 0$ は**講義プリントの定義 3.3** の 2 つの性質をもつ:

(G1) すべての番号 i, $1 \leq i \leq n$ に対して, $d \mid a_i$. つまり d は $a_1, \ldots, a_n$ の公約数.
(G2) 0 でない整数 c が $a_1, \ldots, a_n$ の公約数ならば, $c \mid d$ となる.

このように d は $a_1, \ldots, a_n$ の公約数のうち最大のものとなり, 始めの定義 (定義 2.3) と一致する.

[**証明**] 簡単のために, $I := \{a_1x_1 + \cdots + a_nx_n \mid x_1, \ldots, x_n \in \mathbb{Z}\}$ とおく.
(G1) $1 \leq i \leq n$ とする.

$$a_i = 0a_1 + \cdots + 1a_i + \cdots + 0a_n \in I$$

だから, $a_i \in I = d\mathbb{Z}$. よって, $\exists x \in \mathbb{Z}$ s.t. $a_i = dx$. したがって, $d \mid a_i$.
(G2) 0 でない整数 c が $a_1, \ldots, a_n$ の公約数であるとする. $d = d \cdot 1 \in d\mathbb{Z} = I$ だから, $d = a_1x_1 + \cdots + a_nx_n$ をみたす $x_1, \ldots, x_n \in \mathbb{Z}$ が存在する. $c \neq 0$ だから, この右辺を c でくくると,

$$d = c\left(\frac{a_1}{c}x_1 + \cdots + \frac{a_n}{c}x_n\right).$$

$c \mid a_i$ により, $\frac{a_i}{c} \in \mathbb{Z}$ $(1 \leq \forall i \leq n)$. したがって上の右辺の括弧の中身は整数になる. ゆえに, $c \mid d$. □

3.2 問題編

問題 3.1. a, b, c, d, q, $r \in \mathbb{Z}$ とする. **講義プリントの命題 2.3(2):** 「$a \neq 0$ または $b \neq 0$」かつ「$c \neq 0$ または $d \neq 0$」のとき, 整数を成分とする 2 次行列 A が存在して,

$$\begin{pmatrix} c \\ d \end{pmatrix} = A \begin{pmatrix} a \\ b \end{pmatrix} \quad \text{かつ} \quad \det A = \pm 1$$

をみたすならば, $\gcd(a, b) = \gcd(c, d)$ が成り立つ. これを使って次を示せ.

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

(2) $\gcd(bq + r, b) = \gcd(r, b)$. ここで $b \neq 0$ かつ $qb + r \neq 0$ と仮定する.

問題 3.2. a, $b \in \mathbb{N}$ とする. 問題 3.1 を使って次の等式を示せ.

(1) $\gcd(3a + 1, 11a + 4) = 1$. (2) $\gcd(11a + 5b, 2a + b) = \gcd(a, b)$.

問題 3.3. (**重要**) a, b, $c \in \mathbb{Z}$, $c \neq 0$ とする. 次を示せ.

$$\gcd(a, c) = 1 \text{ かつ } c \mid ab \Longrightarrow c \mid b.$$

(ヒント: **講義プリントの定理 2.5(1)** により, $ax + cy = 1$ をみたす整数 x, y が存在する. この命題の主張は「素因数分解の一意性」を既知とすると, すぐ納得できると思う.)

問題 3.4. a, b を共に 0 でない整数とし, $d := \gcd(a, b)$ とおく. このとき, $\gcd\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$ が成り立つことを証明せよ.
(ヒント: 最大公約数の性質 (G1), (G2) を使うと良い.)

問題 3.5. 次の整数 a, b に対して, Euclid の互除法を使って $d := \gcd(a, b)$ の値と $ax + by = d$ をみたす整数の組 (x, y) を 1 つ (特殊解を) 求めよ.

(1) $a = 15450$, $b = 6901$. (2) $a = 16980$, $b = 4380$. (3) $a = 30769$, $b = 9483$.