

4 1次不定方程式, 最小公倍数, 素因数分解の一意性

4.1 解説編

4.1.1 1次不定方程式

a, b を 0 でない整数, $c \in \mathbb{Z}$ とする. $ax + by = c$ が整数解 (x, y) をもつための必要十分条件は, 講義プリント定理 3.4 により $\gcd(a, b) \mid c$ となることである.¹ Euclid の互除法により 1 つの解 (特殊解) (x_0, y_0) は求まることを問題 3.5 で具体的に見た. 一般解は次の手順で求まる.

定理 4.1. 上の設定の下で, 簡単のために $d := \gcd(a, b)$ とおく. $d \mid c$ を仮定する. このとき 1 次不定方程式

$$ax + by = c \cdots (*)$$

は無数の整数解をもつ. $(x_0, y_0) \in \mathbb{Z}^2$ を 1 つの解とすると, 一般解は,

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t, \quad t \text{ は任意の整数}$$

で与えられる. 対称的に係数 a, b が現れること, 下線部の符号の違いに注意せよ.

[証明] 始めに一般解の形を探す. (*) の別の整数解 (x, y) があつたとすると, $ax + by = c$ をみताす. 一方 (x_0, y_0) は特殊解だから, $ax_0 + by_0 = c$. これらの辺辺を引くと, $a(x - x_0) + b(y - y_0) = 0$, よって, $a(x - x_0) = -b(y - y_0)$ となる. この両辺を d で割ると,

$$\frac{a}{d}(x - x_0) = -\frac{b}{d}(y - y_0). \cdots (**)$$

問題 3.4 により $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ であり, $-(y - y_0)$ は整数だから $\frac{b}{d} \mid \frac{a}{d}(x - x_0)$. ゆえに問題 3.3 により, $\frac{b}{d} \mid (x - x_0)$ となる. したがって, $x - x_0 = \frac{b}{d}t$, すなわち, $x = x_0 + \frac{b}{d}t$ をみたす整数 t が存在する. これを (**) に代入すると, $\frac{a}{d} \frac{b}{d}t = -\frac{b}{d}(y - y_0)$. この両辺を $-\frac{b}{d}$ で割ると, $y - y_0 = -\frac{a}{d}t$, すなわち, $y = y_0 - \frac{a}{d}t$ となる. このように一般解の候補が見つかる. これらがすべての解を与えるかどうかを確かめるために, t を任意の整数として

$$x := x_0 + \frac{b}{d}t, \quad y := y_0 - \frac{a}{d}t$$

とおくと, $\frac{b}{d}$ と $\frac{a}{d}$ は整数だから, $x, y \in \mathbb{Z}$. そして,

$$ax + by = ax_0 + \frac{ab}{d}t + by_0 - \frac{ab}{d}t = ax_0 + by_0 = c.$$

確かに解になることがわかる. □

¹ $f(X_1, \dots, X_n)$ を n 変数 X_1, \dots, X_n の整数係数多項式とする. n 個の整数の組 $(x_1, \dots, x_n) \in \mathbb{Z}^n$ が $f(x_1, \dots, x_n) = 0$ をみたすとき, (x_1, \dots, x_n) は方程式 $f(X_1, \dots, X_n) = 0$ の整数解であるという. (すべての) 整数解を見出すことを「不定方程式 $f(X_1, \dots, X_n) = 0$ を解く」といい, その整数解を「不定方程式 $f(X_1, \dots, X_n) = 0$ の解」という.

4.1.2 最小公倍数

注意 2.4 の続きとして, n 個の整数の「最小公倍数」の再定義について少し解説する. 問題 2.5(1) で見たように, 2 個の整数の最小公倍数の特徴付け「 $a\mathbb{Z} \cap b\mathbb{Z} = \text{lcm}(a, b)\mathbb{Z}$ 」があった. そこで n 個の場合もこれを定義にしてしまう.

定義 4.1. (最小公約数) a_1, \dots, a_n を n 個の整数とする. そのとき集合

$$I := a_1\mathbb{Z} \cap \dots \cap a_n\mathbb{Z}$$

を考える (簡単のために I とおく). I は, 下で見るように講義プリントの命題 3.1 の条件 (ii):

$$\lceil a, b \in I, c \in \mathbb{Z} \implies a + b \in I \text{ かつ } ca \in I \rceil \dots (*)$$

をみます. この条件 (ii) をみます \mathbb{Z} の部分集合は「 \mathbb{Z} のイデアル」と呼ばれる重要なものである. したがって同値な条件 (iii) が成り立つから,

$$I = a_1\mathbb{Z} \cap \dots \cap a_n\mathbb{Z} = m\mathbb{Z}$$

をみます整数 $m \geq 0$ が唯一つ存在する. (一意性は問題 2.4 と問題 2.2(2) からわかる.) そこで m を a_1, \dots, a_n の最小公倍数 (the least common multiple) といい, 記号で $m = \text{lcm}(a_1, \dots, a_n)$ と表わす. \square

この整数 $m \geq 0$ は次の 2 つの性質をもつ:

- (L1) すべての番号 $i, 1 \leq i \leq n$ に対して, $a_i \mid m$. つまり m は a_1, \dots, a_n の公倍数.
- (L2) 整数 c が a_1, \dots, a_n の公倍数ならば, $m \mid c$ となる.

このように m は a_1, \dots, a_n の (正の) 公倍数のうち最小のものとなり, 始めの定義 (定義 2.3) と一致する.

[証明]

「(*) が成り立つこと」 $a, b \in I, c \in \mathbb{Z}$ とする. $a, b \in I$ により, すべての番号 $i, 1 \leq i \leq n$ に対して $a \in a_i\mathbb{Z}$ かつ $b \in a_i\mathbb{Z}$. $1 \leq i \leq n$ とする. よって, $\exists x_i \exists y_i \in \mathbb{Z}$ s.t. $a = a_i x_i$ かつ $b = a_i y_i$.

$$a + b = a_i x_i + a_i y_i = a_i (x_i + y_i)$$

であり $x_i + y_i \in \mathbb{Z}$ だから, $a + b \in a_i\mathbb{Z}$ ($1 \leq i \leq n$) となる. ゆえに,

$$a + b \in a_1\mathbb{Z} \cap \dots \cap a_n\mathbb{Z} = I.$$

また, $ca = c(a_i x_i) = a_i (c x_i)$ であり $c x_i \in \mathbb{Z}$ だから, $ca \in a_i\mathbb{Z}$ ($1 \leq i \leq n$) となる. ゆえに, $ca \in a_1\mathbb{Z} \cap \dots \cap a_n\mathbb{Z} = I$. このように (*) をみます.

(L1) $1 \leq i \leq n$ とする. $m = m \cdot 1 \in m\mathbb{Z} = I \subset a_i\mathbb{Z}$ だから, $\exists x \in \mathbb{Z}$ s.t. $m = a_i x$. したがって, $a_i \mid m$.

(L2) 整数 c が a_1, \dots, a_n の公倍数であるとする. $1 \leq i \leq n$ とする. $a_i \mid c$ により, $\exists x_i \in \mathbb{Z}$ s.t. $c = a_i x_i$. よって, $c = a_i x_i \in a_i\mathbb{Z}$ ($1 \leq i \leq n$). ゆえに, $c \in a_1\mathbb{Z} \cap \dots \cap a_n\mathbb{Z} = I = m\mathbb{Z}$. よって, $\exists y \in \mathbb{Z}$ s.t. $c = my$. したがって, $m \mid c$ となる. \square

a_1, \dots, a_n の最大公約数, 最小公倍数を求める計算は 2 個の場合に帰着する. 簡単のために $n = 3$ の場合を書く:

命題 4.2. $a, b, c \in \mathbb{N}$ とする. このとき次が成り立つ.

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

$$(2) \operatorname{lcm}(a, b, c) = \operatorname{lcm}(a, \operatorname{lcm}(b, c)).$$

[証明]

(1) $\alpha \in \mathbb{Z}$ とする. 最大公約数の定義により,

$$\begin{aligned} \alpha \in \gcd(a, b, c)\mathbb{Z} &\iff \exists x \exists y \exists z \in \mathbb{Z} \text{ s.t. } \alpha = ax + by + cz = ax + (by + cz) \\ &\iff \exists x \exists w \in \mathbb{Z} \text{ s.t. } \alpha = ax + \gcd(b, c)w \\ &\iff \alpha \in \gcd(a, \gcd(b, c))\mathbb{Z} \end{aligned}$$

だから, $\gcd(a, b, c)\mathbb{Z} = \gcd(a, \gcd(b, c))\mathbb{Z}$. 問題 2.4 と問題 2.2(2) により, $\gcd(a, b, c) = \pm \gcd(a, \gcd(b, c))$. 最大公約数は定義により正の整数だから, $\gcd(a, b, c) = \gcd(a, \gcd(b, c))$ となる.

(2) $\alpha \in \mathbb{Z}$ とする. 最小公倍数の定義により,

$$\begin{aligned} \alpha \in \operatorname{lcm}(a, b, c)\mathbb{Z} &\iff \alpha \in a\mathbb{Z} \cap b\mathbb{Z} \cap c\mathbb{Z} = a\mathbb{Z} \cap (b\mathbb{Z} \cap c\mathbb{Z}) \\ &\iff \alpha \in a\mathbb{Z} \cap \operatorname{lcm}(b, c)\mathbb{Z} \\ &\iff \alpha \in \operatorname{lcm}(a, \operatorname{lcm}(b, c))\mathbb{Z} \end{aligned}$$

だから, $\operatorname{lcm}(a, b, c)\mathbb{Z} = \operatorname{lcm}(a, \operatorname{lcm}(b, c))\mathbb{Z}$. 問題 2.4 と問題 2.2(2) により, $\operatorname{lcm}(a, b, c) = \pm \operatorname{lcm}(a, \operatorname{lcm}(b, c))$. 最小公倍数は定義により正の整数だから, $\operatorname{lcm}(a, b, c) = \operatorname{lcm}(a, \operatorname{lcm}(b, c))$ となる. \square

4.2 問題編

問題 4.1. 次の1次不定方程式のすべての(整数)解を求めよ.

$$(1) 10086x + 897y = 322 \quad (2) 1963x + 274y = 2014 \quad (3) 2728x + 1243y = 66$$

問題 4.2.

(1) $121x + 323y = 1$ をみたす整数 x, y を1組求めよ.

(2) 条件

$$121m + 323n = 5, \quad |m| \leq 160, \quad |n| \leq 60$$

をみたす整数 m, n を求めよ.

問題 4.3. (チャレンジ問題) n は自然数とする. 2次不定方程式 $x^2 - y^2 = n$ が(整数)解をもつための n に関する必要十分条件を求めよ.

問題 4.4. a, b を2以上の整数とし, a, b の素因数分解をそれぞれ

$$a = \prod_{i=1}^r p_i^{e_i}, \quad b = \prod_{i=1}^r p_i^{f_i}$$

とする. ここで, p_1, \dots, p_r はどの2つも相異なる素数, e_i, f_i は0以上の整数である. 次を証明せよ.

(1) $a \mid b \iff$ 「任意の番号 $i, 1 \leq i \leq r$ に対して $e_i \leq f_i$ 」.

$$(2) \gcd(a, b) = \prod_{i=1}^r p_i^{\min(e_i, f_i)}.$$

(ヒント: 右辺が最大公約数の性質 (G1), (G2) を満たすことを確かめる.)

$$(3) \operatorname{lcm}(a, b) = \prod_{i=1}^r p_i^{\max(e_i, f_i)}.$$

(ヒント: 右辺が最小公倍数の性質 (L1), (L2) を満たすことを確かめる.)

(4) $ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$. (ヒント: 小問 (2), (3) を使う.)

問題 4.5. Euclid の互除法と問題 4.4 (4) を使って次を求めよ. (積の形のままでよい.)

$$(1) \operatorname{lcm}(470, 105) \quad (2) \operatorname{lcm}(2046, 589)$$

問題 4.6. $\gcd(48, a) = 3, \operatorname{lcm}(48, a) = 240$ をみたす自然数 a を求めよ.

問題 4.7. Euclid の互除法と命題 4.2 を使って次を求めよ.

$$(1) \gcd(3375, 645, 477)$$

$$(2) \operatorname{lcm}(1112, 139, 16)$$

問題 4.8. $189\mathbb{Z} \cap 68\mathbb{Z} = a\mathbb{Z}$ をみたす $a \in \mathbb{N}$ を求めよ.