

9. ユークリッドの互除法

- a, b を整数とし, $a \neq 0$ とする. a が b を割り切るとき, $a \mid b$ と表す.
- a, b を 0 でない整数とする. a と b に共通な正の約数の中で最大のものを a と b の最大公約数 (greatest common divisor) といい, $\gcd(a, b)$ で表す. また, a と b に共通な正の倍数の中で最小のものを a と b の最小公倍数 (least common multiple) といい, $\text{lcm}(a, b)$ で表す.
- a, b を自然数とする. $r_{-1} = a, r_0 = b$ とおく. $j = 1, 2, \dots$ に対して, $r_{j-1} \neq 0$ ならば, 除算

$$r_{j-2} = q_j r_{j-1} + r_j \quad (0 \leq r_j < r_{j-1})$$

によって整数 q_j, r_j を定める. このとき, ある整数 n に対して $r_{n+1} = 0$ となり, $\gcd(a, b) = r_n$ となる. このアルゴリズムをユークリッドの互除法という.

- 自然数 a, b に対して, $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$ が成り立つ (問題 9-3). このことを用いて a と b の最小公倍数 $\text{lcm}(a, b)$ を求めることができる.
- a, b を自然数として, $g = \gcd(a, b)$ とおく. このとき, 変数 X と Y に関する方程式

$$aX + bY = g$$

は整数解を持つ. 以下で説明する拡張ユークリッドの互除法で整数解を求めることができる.

$r_{-1} = a, r_0 = b, x_{-1} = 1, x_0 = 0, y_{-1} = 0, y_0 = 1$ とおく. $j = 1, 2, \dots$ に対して, $r_{j-1} \neq 0$ ならば, 除算

$$\begin{aligned} r_{j-2} &= q_j r_{j-1} + r_j \quad (0 \leq r_j < r_{j-1}), \\ x_j &= x_{j-2} - q_j x_{j-1}, \quad y_j = y_{j-2} - q_j y_{j-1} \end{aligned}$$

によって整数 q_j, r_j, x_j, y_j を定める. このとき, $ax_j + by_j = r_j$ が成り立つ. 特に, $r_{n+1} = 0$ となる整数 n に対して, $ax_n + by_n = r_n = g$ が成り立つ.

問題

解答に際して、その問題より前にある問題の結果を用いてもよい。

- 9-1. ユークリッドの互除法を用いて $\gcd(936, 598)$ を求めよ。
- 9-2. 前ページのユークリッドの互除法について、以下の問いに答えよ。
 - (a) すべての $j = 1, 2, \dots, n$ に対して、 $r_{j+1} < \frac{r_{j-1}}{2}$ となることを示せ。
 - (b) (a) を用いて、ユークリッドの互除法で必要となる除算は高々 $2\lfloor \log_2 b \rfloor + 1$ 回であることを示せ。
- 9-3. 自然数 a, b に対して、 $ab = \gcd(a, b) \cdot \text{lcm}(a, b)$ が成り立つことを示せ。
- 9-4. $\text{lcm}(1288, 462)$ を求めよ。
- 9-5. a, b, c を整数として、 $a, b \neq 0$ とする。このとき、方程式 $aX + bY = c$ が整数解 (X, Y) を持つための必要十分条件は、 $\gcd(a, b)$ が c の約数になることであることを示せ。
- 9-6. 拡張ユークリッドの互除法を用いて、方程式 $71X + 17Y = 1$ の整数解 (X, Y) を 1 組求めよ。
- 9-7. 拡張ユークリッドの互除法を用いて、方程式 $221X + 119Y = 85$ の整数解 (X, Y) を 1 組求めよ。
- 9-8. 方程式 $273X + 112Y = 5$ が整数解を持たないことを示せ。
- 9-9. 方程式 $12X + 15Y + 20Z = 7$ の整数解 (X, Y, Z) を 1 組求めよ。