

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. 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

$$aX + bY = g \tag{1}$$

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.

- a, b, c を整数として, $a, b \neq 0$ とする. X と Y に関する方程式

$$aX + bY = c$$

が解を持つための必要十分条件は, $\gcd(a, b)$ が c を割り切ることである. このとき, 両辺を $c/\gcd(a, b)$ で割ることで方程式 (1) に帰着される.

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 $\gcd(4508, 931)$ を求めよ。
- 9-2. ユークリッドの互除法を用いて $\gcd(3337, 1491)$ を求めよ。
- 9-3. $\text{lcm}(1246, 801)$ を求めよ。
- 9-4. 拡張ユークリッドの互除法を用いて、方程式 $68X + 57Y = 1$ の整数解 (X, Y) を 1 組求めよ。
- 9-5. 拡張ユークリッドの互除法を用いて、方程式 $799X + 629Y = 85$ の整数解 (X, Y) を 1 組求めよ。
- 9-6. 方程式 $55X + 33Y + 15Z = 1$ の整数解 (X, Y, Z) を 1 組求めよ。
- 9-7. $\phi = \frac{1 + \sqrt{5}}{2}$ とおく。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 $j = 0, 1, \dots, n$ に対して、 $r_{n-j} \geq \phi^j$ が成り立つことを示せ。
- (b) ユークリッドの互除法で必要となる除算回数は $\log_{\phi} b + 1$ 以下であることを示せ。
- 9-8. 以下の問いに答えよ。
- (a) a, b を自然数として、 $a \geq b$ とする。除算により $a = qb + r$ ($0 \leq r < b$) を満たす整数 q, r を求めるのに必要なビット演算量は高々 $(\lfloor \log_2 b \rfloor + 1)(\lfloor \log_2 q \rfloor + 1)$ であることを示せ。
- (b) a, b を高々 l ビットの自然数とする。前ページのユークリッドの互除法で $\gcd(a, b)$ を計算するときのビット演算量は $O(l^2)$ であることを示せ。
- 9-9. a, b を自然数とする。次のアルゴリズムによって有限回のステップで $\gcd(a, b)$ が計算できることを示せ。
- (i) $a = 2^e x, b = 2^f y$ となる整数 e, f と奇数 x, y を計算する。
- (ii) $x \neq y$ である間、以下を繰り返す。
- (a) $|y - x| = 2^g z$ となる整数 g と奇数 z を計算する。
- (b) $(x, y) \leftarrow (\min\{x, y\}, z)$ とする。
- (iii) $\gcd(a, b)$ として $2^{\min\{e, f\}} x$ を返す。
- (このアルゴリズムは **2進 gcd アルゴリズム** (binary gcd algorithm) と呼ばれる。)
- 9-10. 9-9 のアルゴリズムを用いて $\gcd(5044, 3614)$ を求めよ。