アルゴリズム B 演習 No. 9　　2017 年 12 月 15 日配布

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，$\mathrm{lcm}(a,b)$ で表す．
- a, b を自然数とする．$r_{-1} = a$, $r_0 = b$ とおく．$j = 1, 2, \ldots$ 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，$ab = \gcd(a,b) \cdot \mathrm{lcm}(a,b)$ が成り立つ．このことを用いて a と b の最小公倍数 $\mathrm{lcm}(a,b)$ 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．$j = 1, 2, \ldots$ に対して，$r_{j-1} \neq 0$ ならば，除算
$$\begin{gathered} r_{j-2} = q_j r_{j-1} + r_j \quad (0 \leq r_j < r_{j-1}), \\ x_j = x_{j-2} - q_j x_{j-1}, \quad y_j = y_{j-2} - q_j y_{j-1} \end{gathered}$$
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 $\gcd(1271, 697)$ を求めよ．

9-2. $\phi = \dfrac{1+\sqrt{5}}{2}$ 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 $j = 0, 1, \ldots, n$ 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．

9-3. 自然数 a, b が

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

と素因数分解されているとする．ただし，$p_1, p_2, \ldots, p_r$ は相異なる素数であり，すべての $i = 1, 2, \ldots, r$ に対して $e_i \geq 0$, $f_i \geq 0$ であるとする．このとき，次の式が成り立つことを示せ．

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

9-4. 自然数 a, b に対して，$ab = \gcd(a, b) \cdot \mathrm{lcm}(a, b)$ が成り立つことを示せ．

9-5. $\mathrm{lcm}(696, 551)$ を求めよ．

9-6. 拡張ユークリッドの互除法を用いて，方程式 $42X + 19Y = 1$ 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 $312X + 143Y = 39$ の整数解 (X, Y) を 1 組求めよ．

9-8. 方程式 $35X + 30Y + 21Z = 1$ の整数解 (X, Y, Z) を 1 組求めよ．