**アルゴリズム B 演習 No. 9** 2013 年 12 月 13 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．$i = 0, 1, 2, \ldots$ に対して，除算

$$r_{i-1} = q_i r_i + r_{i+1} \quad (0 \leq r_{i+1} < r_i)$$

によって整数 $q_i$, $r_{i+1}$ を定める操作を繰り返す．このとき，ある自然数 $n$ 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．
- $a, b, c$ を整数として，変数 $X$ と $Y$ に関する方程式

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

を考える．$\gcd(a, b) = c$ のとき，$a$ と $b$ にユークリッドの互除法を行い，その手順を逆にたどることで方程式 (1) の整数解が 1 つ得られる．このアルゴリズムを**拡張ユークリッドの互除法**という．また，$\gcd(a, b) \mid c$ のとき，方程式

$$aX + bY = \gcd(a, b)$$

の解をそれぞれ $c/\gcd(a, b)$ 倍すれば方程式 (1) の整数解が得られる．また，$\gcd(a, b) \nmid c$ のとき方程式 (1) は整数解を持たない．

**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 $\gcd(377, 156)$ を求めよ.

9-2. ユークリッドの互除法により最大公約数を計算するアルゴリズムを再帰を用いて書け.

9-3. (a) 前ページのユークリッドの互除法において，$r_{i+1} \leq \dfrac{r_{i-1}}{2}$ となることを示せ.
(b) (a) を用いて，ユークリッドの互除法が $O(\log b)$ 回の除算でできることを示せ.

9-4. $\mathrm{lcm}(744, 527)$ を求めよ.

9-5. $a, b$ を自然数，$r_{-1} = a$, $r_0 = b$ として，整数 $r_{-1}, r_0, \ldots, r_n$ が

$$r_{i-1} = q_i r_i + r_{i+1} \quad (i = 0, 1, \ldots, n-1), \quad r_{n-1} = q_n r_n$$

を満たすとする．行列 $Q_0, Q_1, \ldots, Q_n$ を

$$Q_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix} \quad (i = 0, 1, \ldots, n)$$

で定める．このとき，

$$(x, y) = (1, 0) Q_n \cdots Q_1 Q_0$$

で整数 $x, y$ を定めれば，$ax + by = r_n$ となることを示せ.

9-6. 拡張ユークリッドの互除法を用いて，方程式 $81X + 19Y = 1$ 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 $161X + 133Y = 21$ の整数解 $(X, Y)$ を 1 組求めよ.