アルゴリズム B 演習 No. 9　　2014 年 12 月 12 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，$r_i \neq 0$ ならば，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．このとき，ある非負整数 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（問題 9-3）．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 $\dfrac{c}{\gcd(a, b)}$ 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 $\gcd(1976, 1092)$ 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 $i = 1, 2, \ldots, n$ に対して，$r_{i+1} < \dfrac{r_{i-1}}{2}$ 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．

9-3. 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．

9-4. $\mathrm{lcm}(345, 276)$ を求めよ．

9-5. 拡張ユークリッドの互除法を用いて，方程式 $42X + 31Y = 1$ の整数解 (X, Y) を 1 組求めよ．

9-6. 拡張ユークリッドの互除法を用いて，方程式 $187X + 143Y = 121$ の整数解 (X, Y) を 1 組求めよ．

9-7. 方程式 $589X + 209Y = 12$ が整数解を持たないことを示せ．

9-8. 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．）

9-9. 9-8 のアルゴリズムを用いて $\gcd(1976, 1092)$ を求めよ．