アルゴリズム B 演習 No. 8 2012 年 12 月 7 日配布

8. ユークリッドの互除法

- 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．
- K を体，$K[X]$ を K 上の一変数多項式環とする．$f, g \in K[X]$ を 0 でない多項式とする．f と g をともに割り切る多項式の中で次数が最大のものを f と g の**最大公約元** (greatest common divisor) といい，$\gcd(f, g)$ と表す．$\gcd(f, g)$ は定数倍を除いて定まることに注意する．

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．

8-1. 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，$\gcd(a, b) = r_n$ となることを示せ．（このアルゴリズムを**ユークリッドの互除法**という．）

8-2. ユークリッドの互除法を用いて $\gcd(391, 153)$ を求めよ．

8-3. 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．

8-4. a, b を自然数として，$a > b$ とする．フィボナッチ数列 $\{F_n\}$ を

$$F_1 = 1, \quad F_2 = 1, \quad F_{n+2} = F_{n+1} + F_n$$

で定義する．

(a) 8-1 のようにユークリッドの互除法で $\gcd(a, b)$ を計算するとき，$0 \leq k \leq n + 1$ に対し，$r_{n-k} \geq F_{k+2}$ であることを示せ．

(b) ユークリッドの互除法で $\gcd(a, b)$ を計算する際に必要な除算回数は高々 $\lfloor \log_\phi (3 - \phi)(b + 1) \rfloor$ であることを示せ．ただし，$\phi = (1 + \sqrt{5})/2$ とする．

8-5. 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．

8-6. ユークリッドの互除法の手続きを逆にたどることで，方程式 $29X + 23Y = 1$ の整数解 (X, Y) を一組求めよ．（この方法を**拡張ユークリッドの互除法**という．）

8-7. 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．

8-8. 次の問いに答えよ．

（a）ユークリッドの互除法を用いて $\gcd(899, 713)$ を求めよ．

（b）8-7 の等式を用いて $\mathrm{lcm}(899, 713)$ を求めよ．

- K を体，$f, g \in K[X]$ を 0 でない多項式とする．$r_{-1} = f$, $r_0 = g$ とおく．$i = 0, 1, 2, \ldots$ に対して，除算

$$r_{i-1} = q_i r_i + r_{i+1} \quad (\deg r_{i+1} < \deg r_i \text{ または } r_{i+1} = 0)$$

によって $q_i, r_{i+1} \in K[X]$ を定める操作を繰り返し，$r_{n+1} = 0$ となったら終了する．このとき，$\gcd(f, g) = r_n$ となる．（これもユークリッドの互除法と呼ばれる．$\gcd(f, g) = r_n$ となることの証明は 8-1 と同様である．）

8-9. ユークリッドの互除法を用いて，$\mathbb{Q}[X]$ において

$$\gcd(X^4 - 2X^3 + 3X^2 - 6X + 9, X^3 - X^2 + X - 6)$$

を求めよ．

8-10. ユークリッドの互除法の手続きを逆にたどることで，

$$(X^2 + X + 1)p(X) + (X^2 - X - 3)q(X) = 1$$

を満たす $p(X), q(X) \in \mathbb{Q}[X]$ を一組求めよ．