計算機数学I (2019)
第8回

照井 章（筑波大学 数理物質系 数学域）
Akira Terui (Institute of Mathematics, University of Tsukuba)

第7回のまとめ

- 可換環の基本的定義の復習
- Euclid互除法
- 拡張Euclid互除法

第8回の内容

- 拡張Euclid互除法の性質
- 拡張Euclid互除法の応用
  - 法逆元 (modular inverse) の計算

拡張Euclid互除法 (The Extended Eucliean Algorithm; EEA) の性質 (§ 4.3) (p. 53)

定理 4.25

- $f, g \in \mathrm{R}$
- 剰余つき除算により，$\lambda \geqq 0$ に対し，

  $r_1, \ldots, r_\lambda, r_{\lambda+1}$ および $q_1, \ldots, q_\lambda$ をEA, EEAと同様に定める
- $s_0, \ldots, s_\lambda, s_{\lambda+1}$ および $t_0, \ldots, t_\lambda, t_{\lambda+1}$ をEEAと同様に定める

定理 4.25: r_i, q_i の定義

$$
\begin{aligned}
f &= r_0, g = r_1, \\
r_0 &= r_1 q_1 + r_2 \quad (0 < r_2 < r_1), \\
&\vdots \\
r_{i-1} &= r_i q_i + r_{i+1} \quad (0 < r_{i+1} < r_i), \\
&\vdots \\
r_{\lambda-2} &= r_{\lambda-1} q_{\lambda-1} + r_\lambda \quad (0 < r_\lambda < r_{\lambda-1}), \\
r_{\lambda-1} &= r_\lambda q_\lambda \quad (r_{\lambda+1} = 0).
\end{aligned}
$$

($g = 0$ のとき $\lambda = 0$, $g \neq 0$ のとき $\lambda > 0$)

定理 4.25: s_i, t_i の定義

- $s_0 = 1, t_0 = 0$
- $s_1 = 0, t_1 = 1$
- $s_{i+1} = s_{i-1} - s_i q_i, \quad t_{i+1} = t_{i-1} - t_i q_i \quad (i = 1, \ldots, \lambda)$

  $(r_{i+1}, s_{i+1}, t_{i+1}) = (r_{i-1}, s_{i-1}, t_{i-1}) - q_i (r_i, s_i, t_i)$
- アルゴリズム EEA の出力:

  $(d, s, t) = (r_{i-1}, s_{i-1}, t_{i-1})$

定理 4.25 $T_i = \begin{pmatrix} s_i & s_{i+1} \\ t_i & t_{i+1} \end{pmatrix}, \quad Q_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$

- このとき、次が成り立つ:

a. $(f\ g)^{\mathrm{t}}(s_i\ t_i) = r_i$, $(f\ g)\ T_i = (r_i\ r_{i+1})$

b. $T_i = T_0 Q_1 Q_2 \cdots Q_i = Q_1 Q_2 \cdots Q_i$

c. 任意の i に対し $d = \gcd(r_i, r_{i+1}) = \gcd(f, g)$

d. $\det T_i = s_i t_{i+1} - s_{i+1} t_i = (-1)^i$, 従って $s_i \perp t_i$

e. $f = (-1)^i (r_i t_{i+1} - r_{i+1} t_i)$, $g = (-1)^i (s_i r_{i+1} - s_{i+1} r_i)$

定理 4.25 $T_i = \begin{pmatrix} s_i & s_{i+1} \\ t_i & t_{i+1} \end{pmatrix}, \quad Q_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$

- 証明
  a. $(f\ g)\ {}^{t}(s_i\ t_i) = r_i$, $(f\ g)\ T_i = (r_i\ r_{i+1})$

     前回の定理 (EEA) 1. の通り

  b. $T_i = T_0 Q_1 Q_2 \cdots Q_i = Q_1 Q_2 \cdots Q_i$

     (帰納法) $i = 0$ のときは明らか

     $0, \ldots, i$ までで成り立つとき

     $T_i = Q_1 Q_2 \cdots Q_i$

定理 4.25 $T_i = \begin{pmatrix} s_i & s_{i+1} \\ t_i & t_{i+1} \end{pmatrix}, \quad Q_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$

- 証明

b. (続き) このとき

$$
\begin{aligned}
T_i Q_{i+1} &= \begin{pmatrix} s_i & s_{i+1} \\ t_i & t_{i+1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{pmatrix} \\
&= \begin{pmatrix} s_{i+1} & s_i - q_{i+1} s_{i+1} \\ t_{i+1} & t_i - q_{i+1} t_{i+1} \end{pmatrix} \\
&= \begin{pmatrix} s_{i+1} & s_{i+2} \\ t_{i+1} & t_{i+2} \end{pmatrix} = T_{i+1}
\end{aligned}
$$

定理 4.25 $T_i = \begin{pmatrix} s_i & s_{i+1} \\ t_i & t_{i+1} \end{pmatrix}, \quad Q_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$

- 証明

  c. 任意の i に対し

  $d = \gcd(r_i, r_{i+1}) = \gcd(f, g)$

  前回の定理 (EA) a. の通り

定理 4.25 $T_i = \begin{pmatrix} s_i & s_{i+1} \\ t_i & t_{i+1} \end{pmatrix}, \quad Q_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$

- 証明

  d. $\det T_i = s_i t_{i+1} - s_{i+1} t_i = (-1)^i$, 従って $s_i \perp t_i$

  $\det(T_0) = 1$, $\det(Q_i) = -1$

  b. より $T_i = Q_1 Q_2 \cdots Q_i$

  ゆえに $\det(T_i) = \det(Q_1 Q_2 \cdots Q_i) = (-1)^i$

定理 4.25 $T_i = \begin{pmatrix} s_i & s_{i+1} \\ t_i & t_{i+1} \end{pmatrix}, \quad Q_i = \begin{pmatrix} 0 & 1 \\ 1 & -q_i \end{pmatrix}$

- 証明

  e. $f = (-1)^i (r_i t_{i+1} - r_{i+1} t_i), g = (-1)^i (s_i r_{i+1} - s_{i+1} r_i)$

  a. より $(f\ g)\ T_i = (r_i\ r_{i+1})$

  これを f, g に関する連立1次方程式と見て、クラメルの公式などで解くことで結論を得る

4.7 法逆元 (modular inverse) の計算 (p. 60)

法逆元 (modular inverse) の計算

- R: 可換環 (commutative ring)
- $I \subset R$: イデアル (ideal)
- R/I: 剰余環 (residue class ring)
- $a \in R/I$ が単元のとき（⇔ 乗法の逆元をもつ）、その逆元を計算する
- この計算に拡張Euclid互除法が有効

定理 4.48（法逆元の計算）

- (R, d): Euclid整域, d: Euclid関数
- $a, m \in R$
- このとき $a \bmod m$ が R/mR の単元

  $\Leftrightarrow \gcd(a, m) = 1$
- さらに、このとき、EEAを用いて R/mR における $a \bmod m$ の乗法の逆元 b を計算可能

定理 4.48 の証明

$a \bmod m$ が R/mR の単元

$\Leftrightarrow \exists\ s \in R \text{ s.t. } \quad s\,a \equiv 1 \pmod{m}$

$\Leftrightarrow \exists\ t \in R \text{ s.t. } \quad s\,a - 1 = t\,m$

$\Leftrightarrow s\,a + t\,m = 1$ (s, t はEEAにより計算可能）

$\Leftrightarrow \gcd(a, m) = 1$

定理 4.48 の備考

EEA (a, m) の出力を (r, s, t) とするとき

- $r = 1$ ⇒ $s \bmod m$ は R/mR における $a \bmod m$ の乗法の逆元
- $r \neq 1$ ⇒ $a \bmod m$ は R/mR において単元ではなく、$a \bmod m$ の乗法の逆元は存在しない

例 4.49（法逆元の計算）

- R = Z, $m = 29$, $a = 12$
- $m = 29$ を法として $a = 12$ の逆元が存在すれば求める

例 4.49（法逆元の計算）

- $(r, s, t) = \mathrm{EEA}(\, m = 29, a = 12\,)$ を計算する
- $(r_0, s_0, t_0) = (29, 1, 0)$
- $(r_1, s_1, t_1) = (12, 0, 1)$
- $(r_2, s_2, t_2) = (r_0, s_0, t_0) - q_1 (r_1, s_1, t_1)$

  $= (29, 1, 0) - 2 \times (12, 0, 1)$

  $= (29, 1, 0) - (24, 0, 2) = (5, 1, -2)$

例 4.49（法逆元の計算）

- $(r_3, s_3, t_3) = (r_1, s_1, t_1) - q_2 (r_2, s_2, t_2)$

  $= (12, 0, 1) - 2 \times (5, 1, -2)$

  $= (12, 0, 1) - (10, 2, -4) = (2, -2, 5)$

- $(r_4, s_4, t_4) = (r_2, s_2, t_2) - q_3 (r_3, s_3, t_3)$

  $= (5, 1, -2) - 2 \times (2, -2, 5)$

  $= (5, 1, -2) - (4, -4, 10) = (1, 5, -12)$

例 4.49（法逆元の計算）

- $(r_5, s_5, t_5) = (r_3, s_3, t_3) - q_4 (r_4, s_4, t_4)$

  $= (2, -2, 5) - 2 \times (1, 5, -12)$

  $= (2, -2, 5) - (2, 10, -24) = (0, -12, 29)$

- よって $i = 4$ のとき $5 \times 29 + (-12) \times 12 = 1$
  $a = 12$ に対し $(-12)\, a \equiv 1 \pmod{29}$
  $17 \equiv -12 \pmod{29}$ より、17が29を法とする12の逆元

問題 4.55（代数的数の逆数の計算）

- 方程式 $x^3 - x^2 - x - 1 = 0$ の根の一つを α とする
- $\alpha^2 + \alpha$ の逆数を $A\alpha^2 + B\alpha + C$ の形で表せ

  $(A, B, C \in \mathbb{Q})$

問題 4.55（代数的数の逆数の計算）

- $f(x) = x^3 - x^2 - x - 1 = 0$ の根の一つを α とする
- Q(α): 有理数体 Q のαによる拡大体
- $\mathbb{Q}[x]/\langle f(x)\rangle$: 剰余環

問題 4.55（代数的数の逆数の計算）

$$\begin{array}{ccc} \mathbb{Q}(\alpha) & \longrightarrow & \mathbb{Q}[x]/\langle f(x)\rangle \\ \cup & & \cup \\ A\alpha^2 + B\alpha + C & \mapsto & Ax^2 + Bx + C \end{array}$$

- $f(x)$ は Q 上既約より、$\mathbb{Q}(\alpha)$ と $\mathbb{Q}[x]/\langle f(x)\rangle$ は同型
- $g(x) = x^2 + x$ の $\mathbb{Q}[x]/\langle f(x)\rangle$ 上の逆元を求める

  ⇔ $g(x)$ の $f(x)$ を法とする逆元を求める

問題 4.55（代数的数の逆数の計算）

- $(r, s, t) = \mathrm{EEA}(\, f(x), g(x)\,)$ を計算する
- $(r_0, s_0, t_0) = (f(x), 1, 0)$
- $(r_1, s_1, t_1) = (g(x), 0, 1)$
- $(r_2, s_2, t_2) = (r_0, s_0, t_0) - q_1 (r_1, s_1, t_1)$

  $= (f(x), 1, 0) - (x - 2) \times (g(x), 0, 1)$

  $= (x - 1, 1, -x + 2)$

問題 4.55（代数的数の逆数の計算）

- $(r_3, s_3, t_3) = (r_1, s_1, t_1) - q_2 (r_2, s_2, t_2)$

  $= (g(x), 0, 1) - (x + 2) \times (x - 1, 1, -x + 2)$

  $= (2, -x - 2, x^2 - 3)$

- ゆえに $(-x - 2)\, f(x) + (x^2 - 3)\, g(x) = 2$

問題 4.55（代数的数の逆数の計算）

- 両辺を2で割って

$$\left(\frac{-x-2}{2}\right) f(x) + \left(\frac{x^2-3}{2}\right) g(x) = 1$$

- ゆえに

$$\left(\frac{x^2-3}{2}\right) g(x) \equiv 1 \pmod{f(x)}$$

$$(g(\alpha))^{-1} = \frac{1}{2}(\alpha^2 - 3)$$

問題 4.55（代数的数の逆数の計算）

- 検算

  $(1/2)\,(\alpha^2 - 3)\,(\alpha^2 + \alpha) = (1/2)(\alpha^4 + \alpha^3 - 3\alpha^2 - 3\alpha)$

  $(1/2)(\alpha^4 + \alpha^3 - 3\alpha^2 - 3\alpha)$

  $= (1 + \alpha/2)\, f(\alpha) + 1$

第8回のまとめ

- 拡張Euclid互除法の性質
- 拡張Euclid互除法の応用
  - 法逆元 (modular inverse) の計算

第9回の内容

- 拡張Euclid互除法の性質（つづき）
- 拡張Euclid互除法の応用
  - 実数の連分数展開 (§ 4.13)