計算機数学I (2019)
第9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)

拡張Euclid互除法 (The Extended Eucliean Algorithm; EEA) の性質 (つづき)

定理 (6/17)

- $f, g \in \mathbb{Z}, f \geqq g \geqq 0$
- 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 (6/17) 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 (6/17) s_i, t_i の定義

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

$$(r_{i+1}, s_{i+1}, t_{i+1}) = (r_{i-1}, s_{i-1}, t_{i-1}) - q_i (r_i, s_i, t_i)$$

定理 (6/17)

- このとき、次が成り立つ:

  a. $i = 0, \ldots, \lambda+1$ に対し $t_i t_{i+1} \leqq 0$ かつ $|t_i| \leqq |t_{i+1}|$,

  $i = 0, \ldots, \lambda$ に対し $s_i s_{i+1} \leqq 0$ かつ $|s_i| \leqq |s_{i+1}|$.

  b. $i = 0, \ldots, \lambda+1$ に対し $r_{i-1}|t_i| \leqq a$ かつ

  $r_{i-1}|s_i| \leqq b$.

定理 (6/17)

- 証明

  a. （帰納法）

  t_i : $i = 0$ のときは明らか.

  $0, \ldots, i$ に対し主張が成り立つと仮定

  $t_{i+1} = t_{i-1} - t_i q_i$ に対し、帰納法の仮定より

  t_{i-1} と t_i は異なる符号を持ち、$|t_i| \geqq |t_{i-1}|$.

定理 (6/17)

- 証明

  a. （つづき）ゆえに

  $|t_{i+1}| = |t_{i-1}| + |t_i|\, q_i \geqq |t_i|$

  かつ t_{i+1} の符号は t_i の符号と逆.

  s_i の場合も同様、ただし帰納法は $i = 1$ から始める.

定理 (6/17)

- 証明

  b. $a\,s_{i-1} + b\,t_{i-1} = r_{i-1}$ の両辺を t_i 倍 … (1)
  $a\,s_i + b\,t_i = r_i$ の両辺を t_{i-1} 倍 … (2)
  (1) の両辺から (2) の両辺をそれぞれ引くと
  $a\,(s_{i-1}\,t_i - s_i\,t_{i-1}) = t_i\,r_{i-1} - t_{i-1}\,r_i$
  $a\,(-1)^{i-1} = t_i\,r_{i-1} - t_{i-1}\,r_i$ (定理 4.25, d. より)
  $\pm a = t_i\,r_{i-1} - t_{i-1}\,r_i$

定理 (6/17)

- 証明

  b. $\pm a = t_i r_{i-1} - t_{i-1} r_i$

  ここで, a. より t_i と t_{i-1} が異なる符号を持つことを用いると

  $a = |t_i r_{i-1} - t_{i-1} r_i| = |t_i| r_{i-1} + |t_{i-1}| r_i \geqq |t_i| r_{i-1}$

  s_i に対しても同様に示される

実数の連分数展開（§ 4.13 ）（p. 74）

連分数 (Continued fraction)

- R: Euclid整域、K: Rの商体 R/R
  - 例: R=Z, K=Q
- $\frac{r_0}{r_1} \in K$ ($r_0, r_1 \in$ R) に対し、次の計算による分数の列を考える:

連分数 (Continued fraction)

$$
\begin{aligned}
\frac{r_0}{r_1} &= q_1 + \frac{r_2}{r_1} \\
&= q_1 + \frac{1}{\frac{r_1}{r_2}} = q_1 + \frac{1}{q_2 + \frac{r_3}{r_2}} \\
&= q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_2}{r_3}}} = q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{r_4}{r_3}}} \\
&\ \ \vdots \\
&= q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots \cfrac{1}{q_k + \cfrac{r_{k+1}}{r_k}}}}} \\
&=: \left[q_1, q_2, \ldots, q_k, \frac{r_{k+1}}{r_k} \right]
\end{aligned}
$$

$$r_0 = q_1 r_1 + r_2$$

$$r_1 = q_2 r_2 + r_3$$

$$r_2 = q_3 r_3 + r_4$$

$$r_{k-1} = q_k r_k + r_{k+1}$$

連分数 (Continued fraction)

- r_1/r_0 の（正則）連分数展開
- 「正則」の条件
  - 分子が r_{k+1} を除いてすべて1
  - $q_1 \in Z$
  - $q_2, \ldots, q_k$ は正整数

連分数 (Continued fraction)

- $r_{k+1} = 0$ のとき $[q_1, q_2, \ldots, q_k]$
- 一般に $[q_1] = q_1$,

$$[q_1, q_2, \ldots, q_k] = q_1 + \frac{1}{[q_2, \ldots, q_k]}$$

- 連分数展開は $(q_i, r_{i+1}) \leftarrow r_{i-1} \div r_i$ $(i = 1, \ldots, \mathrm{k})$ を求めるEuclid互除法によって求まる

例 4.89（126/35の連分数展開）

- 126 ÷ 35 → (3, 21) より

$$\frac{126}{35} = 3 + \frac{21}{35} = 3 + \frac{1}{\frac{35}{21}}$$

- 35 ÷ 21 → (1, 14) より

$$\frac{35}{21} = 1 + \frac{14}{21} = 1 + \frac{1}{\frac{21}{14}}$$

例 4.89（126/35の連分数展開）

- 21 ÷ 14 → (1, 7) より

$$\frac{21}{14} = 1 + \frac{7}{14} = 1 + \frac{1}{\frac{14}{7}}$$

- 14 ÷ 7 → (2, 0) より

$$\frac{14}{7} = 2$$

例 4.89（126/35の連分数展開）

- よって、求める連分数展開は

$$\frac{126}{35} = 3 + \frac{21}{35} = 3 + \frac{1}{\frac{35}{21}}$$

$$= 3 + \frac{1}{1 + \frac{1}{\frac{21}{14}}} = 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\frac{14}{7}}}}$$

$$= 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{2}}} = [3, 1, 1, 2]$$

例 4.92（無理数の連分数近似）

$\alpha \in \mathbb{R}$ の連分数近似を考える:

$\alpha_1 = \alpha$ とおいて

$$q_i = \lfloor \alpha_i \rfloor, \alpha_{i+1} = \frac{1}{\alpha_i - q_i}$$

$$(i = 1, 2, 3, \ldots)$$

例 4.92（無理数の連分数近似）

分子を1にする

分母を有理化

整数部分と小数部分に分離

$$\sqrt{3} = 1 + (\sqrt{3} - 1) = 1 + \cfrac{1}{\cfrac{1}{\sqrt{3}-1}}$$

$$\frac{1}{\sqrt{3}-1} = \left(\frac{1}{\sqrt{3}-1}\right)\left(\frac{\sqrt{3}+1}{\sqrt{3}+1}\right) = \frac{\sqrt{3}+1}{2}$$

$$= 1 + \left(\frac{\sqrt{3}+1}{2} - 1\right) = 1 + \left(\frac{\sqrt{3}+1-2}{2}\right)$$

$$= 1 + \frac{\sqrt{3}-1}{2} = 1 + \cfrac{1}{\cfrac{2}{\sqrt{3}-1}}$$

整数部分と小数部分に分離

分子を1にする

例 4.92（無理数の連分数近似）

分母を有理化

$$\frac{2}{\sqrt{3}-1} = \left(\frac{2}{\sqrt{3}-1}\right)\left(\frac{\sqrt{3}+1}{\sqrt{3}+1}\right) = \frac{2(\sqrt{3}+1)}{2}$$

$$= \sqrt{3}+1 = 2+(\sqrt{3}+1-2) = 2+(\sqrt{3}-1)$$

$$= 2+\frac{1}{\frac{1}{\sqrt{3}-1}}$$

整数部分と小数部分に分離

分子を1にする

循環節が現れた！

$$\sqrt{3} = [1,1,2,1,2,1,\ldots] = [1,\overline{1,2}]$$

例 4.92（無理数の連分数近似）

- 実数（無理数）α を循環連分数で表せる

$\Leftrightarrow \quad \alpha = \dfrac{m \pm \sqrt{n}}{q} \quad (m, n, q \in \mathbb{Z})$

(2次無理数：整係数2次方程式の根)

第9回のまとめ

- 拡張Euclid互除法の性質（つづき）
- （拡張）Euclid互除法の応用
  - 有理数の連分数展開の計算
  - 無理数の連分数近似の計算

第10回の内容

- 拡張Euclid互除法の応用
  - 中国剰余算法 (§ 4.8)