計算機数学I (2019)
第7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6回のまとめ

- 1変数多項式の乗算
- 多倍長整数と単精度整数の乗算
- 多倍長整数どうしの乗算
- 整数の剰余つき除算
- 多項式の剰余つき除算

第7回の内容

- 第4章: ユークリッド互除法

  (The Euclidean Algorithm)

4 ユークリッド互除法
(The Euclidean Algorithm) (p. 49)

4.1 イデアル，剰余環，最大公約子 (GCD)，最小公倍子 (LCM)

復習（主に2年次の「代数入門」から）

- R: 可換環 (commutative ring)
- Rのイデアル (ideal)
  - 生成元 (generator(s))
  - 有限生成 (finitely generated)
  - 単項イデアル (principal ideal)
- 剰余類 (residue class)
- 剰余環 (residue class ring)

定義 4.3

- 約元 (divisor)
- 倍元 (multiple)
- 最小公倍子 (The Least Common Multiple, LCM)
- 最大公約子 (The Greatest Common Divisor, GCD)
- 単元 (unit)
- 逆元 (inverse)
- 既約 (irreducible)

注意

- GCDとLCMは一般に一意ではないが、整数環 Z においては、正数にとれば一意に定まる

4.2 Euclid整域と互除法

定義 4.11（Euclid整域）

- R: 整域,　d: $R \to N \cup \{-\infty\}$
- このときRがEuclid整域 ⇔

  $\forall\ a, b \in R$

  $(b \neq 0 \Rightarrow \exists\ q, r \in R \text{ s.t. } a = b\,q + r,\ d(r) < d(b))$
- d: Euclid関数 (Euclidean function)
- q: 商 (quotient)
- r : 剰余 (remainder)

注意

- 一般に，与えられた a と b に対し，q と r が一意に定まるとは限らない

定義 4.14（互いに素）

- $a_1, \ldots, a_n \in \mathrm{R}$ が互いに素 (mutually prime) ⇔ $a_1, \ldots, a_n$ のgcdが単元
- 特に $a, b \in \mathrm{R}$ が互いに素のとき，$a \perp b$ で表す

定理 (EA) (← The Euclidean Algorithm)
(cf. 定理 4.15)

- $a, b \in \mathbb{Z}$ with $a \geqq b \geqq 0$
- 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 $q_1, \ldots, q_\lambda$ を次のように定める:

定理 (EA) (← The Euclidean Algorithm)

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

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

定理 (EA) (← The Euclidean Algorithm)

- このとき，以下が成り立つ:

  a. $r_\lambda = \gcd(a, b)$

  b. $b > 0 \Rightarrow \lambda \leq \dfrac{\log b}{\log \varphi} + 1$

  ただし $\varphi = \dfrac{1+\sqrt{5}}{2} \simeq 1.62$ 黄金比

  （φは $\phi^2 - \phi - 1 = 0$ を満たす）

定理 (EA) (← The Euclidean Algorithm)

- 証明
  a. 定理 4.15 を参照
  b. $b > 0$ と仮定する. このとき $\lambda > 0$.
     - λ に関する帰納法で示す.
     - $\lambda = 1$ のときは明らか.

定理 (EA) (← The Euclidean Algorithm)

- 証明

  b. （続き）

  - $\lambda > 1$ とおく. このとき, $i = 0, \ldots, \lambda - 1$ に対し

    $(*)\ r_{\lambda - i} \geqq \Phi^i$

    を示せば十分.

定理 (EA) (← The Euclidean Algorithm)

- 証明

  b. （続き）

  - 実際, $i = \lambda - 1$ のとき $b = r_1 \geqq \phi^{\lambda-1}$.
  - 両辺の対数をとると

    $\log(b) \geqq (\lambda-1)\log(\phi)$.
  - ゆえに $\lambda - 1 \leq \dfrac{\log b}{\log \varphi}, \quad \lambda \leq \dfrac{\log b}{\log \varphi} + 1.$
  - よって、$(*)$ $r_{\lambda-i} \geqq \phi^i$ を帰納法で示す.

定理 (EA) (← The Euclidean Algorithm)

- 証明

  b. （続き）

  - $i = 0$ のとき: $r_\lambda \geqq 1 = \phi^0$
  - $i = 1$ のとき: $r_{\lambda-1} \geqq r_\lambda + 1 \geqq 2 \geqq \phi^1$
  - $i = 2, \ldots, \lambda - 1$ のとき, $\phi^2 = \phi + 1$ を用いると

定理 (EA) (← The Euclidean Algorithm)

- 証明 b.（続き）
  - $i = 0$ のとき: $r_{\lambda} \geqq 1 = \phi^0$
  - $i = 1$ のとき: $r_{\lambda-1} \geqq r_{\lambda} + 1 \geqq 2 \geqq \phi^1$
  - $i = 2, \ldots, \lambda - 1$ のとき, $(\phi^2 = \phi + 1)$
  - $$r_{\lambda-i} = q_{\lambda-(i-1)}\, r_{\lambda-(i-1)} + r_{\lambda-(i-2)} \geqq r_{\lambda-(i-1)} + r_{\lambda-(i-2)}$$
    $$\geqq \phi^{i-1} + \phi^{i-2} = \phi^{i-2}(1 + \phi) = \phi^{i-2}(\phi^2)$$
    $$= \phi^i .$$

定理 (EA) (← The Euclidean Algorithm)

- 備考

Kを体とするとき，K[x] は，Euclid関数dをd(f) = deg(f) で定めれば Euclid 整域となり，Euclidの互除法が Z と同様に成り立つ.

The Euclidean Algorithm

Algorithm (The Euclidean Algorithm; EA)

入力: $f, g \in \mathrm{R}$
出力: $d \in \mathrm{R}$ s.t. d = gcd(f,g)

1. $r_0 \leftarrow f$; $r_1 \leftarrow g$; $i \leftarrow 1$;
2. while $r_i \neq 0$ do
   a. $(q_i, r_{i+1}) \leftarrow r_{i-1} \div r_i$;
   b. $i \leftarrow i + 1$;
3. d $\leftarrow r_{i-1}$; return d;

4.3 拡張Euclid互除法
(The Extended Euclidean Algorithm)

どこが「拡張」？

- $a, b \in \mathbb{Z},\ d = \gcd(a, b)$ のとき

  $\exists\ s, t \in \mathbb{Z}\quad \text{s.t.}\quad d = s\,a + t\,b$

- このとき，s と t を効率的に計算する

定理 (The Extended Euclidean Algorithm; EEA)

- $a, b \in \mathbb{Z}$ with $a \geqq b \geqq 0$
- 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 $t_0, \ldots, t_\lambda, t_{\lambda+1}$ を次のように定める

定理 (The Extended Euclidean Algorithm; EEA)

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

  $(r_{i+1}, s_{i+1}, t_{i+1}) = (r_{i-1}, s_{i-1}, t_{i-1}) - q_i (r_i, s_i, t_i)$
- このとき，次が成り立つ:

定理 (The Extended Euclidean Algorithm; EEA)

1. $i = 0, \ldots, \lambda+1$ に対し $s_i a + t_i b = r_i$, 特に

   $s_\lambda a + t_\lambda b = \gcd(a, b)$.
2. $a > 0 \Rightarrow i = 0, \ldots, \lambda+1$ に対し $|t_i| \leqq a$ かつ $|s_i| \leqq b$.

   $a > 1$ かつ $b > 0 \Rightarrow |t_\lambda| \leqq a/2$ かつ $|s_\lambda| \leqq b/2$.

定理 (The Extended Euclidean Algorithm; EEA)

証明

1. 帰納法. $i = 0,\ 1$ のときOK.
   $i = 2, \ldots, \lambda+1$のとき

$$\begin{aligned} r_i &= r_{i-2} - q_{i-1} r_{i-1} \\ &= (s_{i-2}a + t_{i-2}b) - q_{i-1}(s_{i-1}a + t_{i-1}b) \\ &= (s_{i-2} - s_{i-1}q_{i-1})a + (t_{i-2} - t_{i-1}q_{i-1})b \\ &= s_i a + t_i b. \end{aligned}$$

2. はここでは省略(後で少し触れるかも)

The Extended Euclidean Algorithm

Algorithm (EEA)

入力: $f, g \in \mathrm{R}$
出力: $(d, s, t) \in \mathrm{R}^3$, s.t. $d = \gcd(f, g), s\,f + t\,g = d$

1. $r_0 \leftarrow f$; $s_0 \leftarrow 1$; $t_0 \leftarrow 0$;
   $r_1 \leftarrow g$; $s_1 \leftarrow 0$; $t_1 \leftarrow 1$; $i \leftarrow 1$;
2. while $r_i \neq 0$ do
   a. $(q_i, r_{i+1}) \leftarrow r_{i-1} \div r_i$;
   b. $(s_{i+1}, t_{i+1}) \leftarrow (s_{i-1}, t_{i-1}) - q_i (s_i, t_i)$;
   c. $i \leftarrow i + 1$;

The Extended Euclidean Algorithm

Algorithm (EEA)

3. $d \leftarrow r_{i-1}$; $s \leftarrow s_{i-1}$; $t \leftarrow t_{i-1}$;
   return (d, s, t);

例題（例 4.23）

- $f = r_0 = 119, g = r_1 = 35$
- $(r_2, s_2, t_2) = (r_0, s_0, t_0) - q_1 (r_1, s_1, t_1)$

  $= (119, 1, 0) - 3 (35, 0, 1) = (14, 1, -3)$
- $(r_3, s_3, t_3) = (r_1, s_1, t_1) - q_2 (r_2, s_2, t_2)$

  $= (35, 0, 1) - 2 (14, 1, -3) = (7, -2, 7)$
- $(r_4, s_4, t_4) = (r_2, s_2, t_2) - q_3 (r_3, s_3, t_3)$

  $= (14, 1, -3) - 2 (7, -2, 7) = (0, 5, -17)$

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