計算機数学I (2019)
第10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)

中国剰余算法 (§ 4.8) (p. 63)

中国剰余定理 (Chinese Remainder Theorem)

- R: Euclid整域
- 線形合同式: $n, a, b \in \mathrm{R}$

  $a\,x \equiv b \pmod{n}$ を x について解く

中国剰余定理 (Chinese Remainder Theorem)

- 連立線形合同式

  $n_1, \ldots, n_k \in \mathrm{R}$: 互いに素　$\forall\, i \neq j\, (n_i \perp n_j)$

  $a_1, \ldots, a_k \in \mathrm{R}$

  のとき

  $a \equiv a_i \pmod{n_i} \quad (i = 1, \ldots, k)$

  を満たす$a \in \mathrm{R}$を求める

定理 4.62 (Chinese Remainder Theorem)

- $n_1, \ldots, n_k \in \mathrm{R}$: 互いに素
- $a_1, \ldots, a_k \in \mathrm{R}$

のとき

1. $\exists\, a \in \mathrm{R} \quad \text{s.t. } a \equiv a_i \pmod{n_i} \quad (i = 1, \ldots, k) \quad (*)$
2. さらに、$a' \in \mathrm{R}$ も合同式 (*) の解
   $\Leftrightarrow a' \equiv a \pmod{n}, \quad n = n_1 \times \ldots \times n_k$
   （解は n を法として一意的に存在）

定理 4.62: 証明

- 次の性質を満たす $e_1, \ldots, e_k \in R$ の存在を示す:
  - $i, j \in [1..k]$ に対し

$$e_j \equiv \begin{cases} 1 \pmod{n_i} & j = i, \\ 0 \pmod{n_i} & j \neq i \end{cases} \qquad (**)$$

定理 4.62: 証明

- (**) を満たす e_j が得られれば

$$a := \sum_{i=1}^{k} a_i e_i$$

とおくことにより

$$a \equiv \sum_{i=1}^{k} a_i e_i \equiv a_j \pmod{n_j}$$

が成り立つ

定理 4.62: 証明

- (**) を満たす e_j の存在:

$$n := n_1 \cdots n_k,$$

$$n_i^* := \frac{n}{n_i} = n_1 \cdots n_{i-1} n_{i+1} \cdots n_k$$

とおくと、$n_1, \ldots, n_k$ は互いに素であるから、

n_i と n_i^* も互いに素

定理 4.62: 証明

- ゆえに、n_iを法とする n_i^* の逆元が存在し、EEAで計算可能。これを t_iとおく。t_i は次式を満たす:
- そこで、$e_i := t_i n_i^*$ とおくと、e_i は $(**)$を満たす

$$e_j \equiv \begin{cases} 1 \pmod{n_i} & j = i, \\ 0 \pmod{n_i} & j \neq i \end{cases} \qquad (**)$$

定理 4.62: 証明

- nを法とする解の一意性:
  - a'を別の解とすると、$i = 1, \ldots, k$に対して次が成り立つ:

$$
\begin{aligned}
& a \equiv a_i \equiv a' \pmod{n_i} && (i = 1, \ldots, k) \\
\Leftrightarrow\ & n_i \mid a - a' && (i = 1, \ldots, k) \\
\Leftrightarrow\ & n_1 \times \ldots \times n_k \mid a - a' && (n_1, \ldots, n_k \text{ は互いに素}) \\
\Leftrightarrow\ & a \equiv a' \pmod{n}
\end{aligned}
$$

問題 3.59（一部改題）

- $a \equiv 2 \pmod 5$, $a \equiv 3 \pmod 6$, $a \equiv 5 \pmod 7$ をみたす整数 a で、非負かつ最小のものを求めよ。
- 定理 4.62 において

  $n_1 = 5, n_2 = 6, n_3 = 7$

  $a_1 = 2, a_2 = 3, a_3 = 5$

  に対し、e_1, e_2, e_3 を求め、

  $0 \leqq a < n_1 n_2 n_3 = 5 \cdot 6 \cdot 7 = 210$

  を満たす a を求める

問題 3.59

- e_1 の計算
  - $n_1^* = \mathrm{n} / n_1 = 210/5 = 42$
  - $n_1 = 5$ を法とする $n_1^* = 42$ の逆元を EEA(42, 5) により求める
  - $(r_0, s_0, t_0) = (42, 1, 0)$
  - $(r_1, s_1, t_1) = (5, 0, 1)$

問題 3.59

- e_1 の計算（つづき）
  - $(r_2, s_2, t_2) = (r_0, s_0, t_0) - q_1 (r_1, s_1, t_1)$
    $= (42, 1, 0) - 8 \times (5, 0, 1)$
    $= (42, 1, 0) - (40, 0, 8) = (2, 1, -8)$
  - $(r_3, s_3, t_3) = (r_1, s_1, t_1) - q_2 (r_2, s_2, t_2)$
    $= (5, 0, 1) - 2 \times (2, 1, -8)$
    $= (5, 0, 1) - (4, 2, -16) = (1, -2, 17)$

問題 3.59

- e_1 の計算（つづき）
  - よって $(-2) \times 42 + 17 \times 5 = 1$

    $(-2) \times 42 \equiv 1 \pmod 5$
  - $-2 \equiv 3 \pmod 5$ より $e_1 = 3 \times 42 = 126$

問題 3.59

- e_2 の計算
  - $n_2^* = \mathrm{n} / n_2 = 210/6 = 35$
  - $n_2 = 6$ を法とする $n_2^* = 35$ の逆元を EEA(35, 6) により求める
  - $(r_0, s_0, t_0) = (35, 1, 0)$
  - $(r_1, s_1, t_1) = (6, 0, 1)$

問題 3.59

- e_2 の計算（つづき）
  - $(r_2, s_2, t_2) = (r_0, s_0, t_0) - q_1 (r_1, s_1, t_1)$
    $= (35, 1, 0) - 5 \times (6, 0, 1)$
    $= (35, 1, 0) - (30, 0, 5) = (5, 1, -5)$
  - $(r_3, s_3, t_3) = (r_1, s_1, t_1) - q_2 (r_2, s_2, t_2)$
    $= (6, 0, 1) - 1 \times (5, 1, -5)$
    $= (6, 0, 1) - (5, 1, -5) = (1, -1, 6)$

問題 3.59

- e_2 の計算（つづき）
  - よって $(-1) \times 35 + 6 \times 6 = 1$

    $(-1) \times 35 \equiv 1 \pmod 6$
  - $-1 \equiv 5 \pmod 6$ より $e_2 = 5 \times 35 = 175$

問題 3.59

- e_3 の計算
  - $n_3^* = \mathrm{n} / n_3 = 210/7 = 30$
  - $n_3 = 7$ を法とする $n_3^* = 30$ の逆元を EEA(30, 7) により求める
  - $(r_0, s_0, t_0) = (30, 1, 0)$
  - $(r_1, s_1, t_1) = (7, 0, 1)$

問題 3.59

- e_3 の計算（つづき）
  - $(r_2, s_2, t_2) = (r_0, s_0, t_0) - q_1 (r_1, s_1, t_1)$
    $= (30, 1, 0) - 4 \times (7, 0, 1)$
    $= (30, 1, 0) - (28, 0, 4) = (2, 1, -4)$
  - $(r_3, s_3, t_3) = (r_1, s_1, t_1) - q_2 (r_2, s_2, t_2)$
    $= (7, 0, 1) - 3 \times (2, 1, -4)$
    $= (7, 0, 1) - (6, 3, -12) = (1, -3, 13)$

問題 3.59

- e_3 の計算（つづき）
  - よって $(-3) \times 30 + 13 \times 7 = 1$

    $(-3) \times 30 \equiv 1 \pmod 7$
  - $-3 \equiv 4 \pmod 7$ より $e_3 = 4 \times 30 = 120$

問題 3.59

- a の計算

$$
\begin{aligned}
a &= a_1 e_1 + a_2 e_2 + a_3 e_3 \\
&= 2 \cdot 126 + 3 \cdot 175 + 5 \cdot 120 \\
&= 252 + 525 + 600 \\
&= 1377 \\
a &\equiv 117 \pmod{210}
\end{aligned}
$$

問題 3.59

- a の検算

$$\begin{aligned} 117 &\equiv -3 \pmod 5 \\ &\equiv 2 \pmod 5, \\ 117 &\equiv 3 \pmod 6, \\ 117 &\equiv 5 \pmod 7 \end{aligned}$$

- ゆえに、求める a は 117.

第10回のまとめ

- 拡張Euclid互除法の応用
  - 中国剰余算法 (§ 4.8):

    拡張Euclid互除法を用いた中国剰余定理の計算法

第11回の内容

- 拡張Euclid互除法の応用
  - 有理数の再構成 (§ 4.12)