計算機数学I (2019)
第11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)

有理数の再構成 (§ 4.12) (p. 70)

有理数を剰余環に埋めこんでの計算

有理数を剰余環に埋め込んでの計算:例題

$$\frac{2}{5}+\frac{1}{3}=\frac{6+5}{15}=\frac{11}{15}$$

有理数を剰余環に埋め込んでの計算：例題

- 有理数 r/t (r, t $\in$ Z) を Z/pZ で表現する (p: 十分大きな素数)
  - p は素数より、$a \in$ Z/pZ は乗法の逆元をもつ:

    $\exists\ t^{-1} \in$ Z/pZ s.t $t \times t^{-1} \equiv 1 \pmod{487}$
  - そこで、Z/pZ で r/t を $r \times t^{-1}$ で表す
  - t^{-1}の計算→ pを法とする法逆元 (modular inverse) の計算に帰着される

有理数を剰余環に埋め込んでの計算：例題

- $\frac{2}{5} + \frac{1}{3} = \frac{6+5}{15} = \frac{11}{15}$

- r/t に対し、$|r| < 15$, $|t| < 16$ として、$2\,|r\,t| = 2 \times 240 = 480 < p$ なる素数 p を選ぶ: $p := 487$

有理数を剰余環に埋め込んでの計算:例題

- 2/5 の Z/487Z への埋め込み
  - EEA(487, 5) により、487 を法とする 5 の逆元を計算する
  - $(r_0, s_0, t_0) = (487, 1, 0)$
  - $(r_1, s_1, t_1) = (5, 0, 1)$
  - $(r_2, s_2, t_2) = (487, 1, 0) - 97\,(5, 0, 1) = (2, 1, -97)$
  - $(r_3, s_3, t_3) = (5, 0, 1) - 2\,(2, 1, -97) = (1, -2, 195)$

有理数を剰余環に埋め込んでの計算：例題

- 2/5 の Z/487Z への埋め込み（つづき）
  - $1 = (-2) \times 487 + 195 \times 5$
  - $5^{-1} = 195$
  - 2/5 を $2 \times 195 = 390 \equiv 390 \pmod{487}$ として埋め込む

有理数を剰余環に埋め込んでの計算:例題

- 1/3 の Z/487Z への埋め込み
  - EEA(487, 3) により、487 を法とする 3 の逆元を計算する
  - $(r_0, s_0, t_0) = (487, 1, 0)$
  - $(r_1, s_1, t_1) = (3, 0, 1)$
  - $(r_2, s_2, t_2) = (487, 1, 0) - 162\,(3, 0, 1) = (1, 1, -162)$

有理数を剰余環に埋め込んでの計算：例題

- 1/3 の Z/487Z への埋め込み（つづき）
  - $1 = 1 \times 487 - 162 \times 3$
  - $3^{-1} = -162 \equiv 325 \pmod{487}$
  - 1/3 を $325 \equiv 325 \pmod{487}$ として埋め込む

有理数を剰余環に埋め込んでの計算:例題

- 2/5 + 1/3 の Z/487Z での計算
  - 390 + 325 = 715 ≡ 228 (mod 487)

有理数を剰余環に埋め込んでの計算：例題

- 次に確認すること
  - $r/t = r \times t^{-1} \equiv 228 \pmod{487}$ を満たす r と t が存在するか？
  - もし、上の r と t が存在した場合、それらは $\frac{2}{5} + \frac{1}{3} = \frac{6+5}{15} = \frac{11}{15}$ に対応しているか？

有理数を剰余環に埋め込んでの計算:例題

- そこで、とりあえず EEA で 11/15 を Z/487Z に埋め込んでみる
- 487を法とする15の逆元を計算する
  - $(r_0, s_0, t_0) = (487, 1, 0)$
  - $(r_1, s_1, t_1) = (15, 0, 1)$
  - $(r_2, s_2, t_2) = (487, 1, 0) - 32\,(15, 0, 1) = (7, 1, -32)$
  - $(r_3, s_3, t_3) = (15, 0, 1) - 2\,(7, 1, -32) = (1, -2, 65)$

有理数を剰余環に埋め込んでの計算：例題

- 11/15 の Z/487Z への埋め込み（つづき）
  - $1 = (-2) \times 487 + 65 \times 15$
  - $15^{-1} = 65 \equiv 65 \pmod{487}$
  - よって

    11/15 を $11 \times 65 = 715 \equiv 228 \pmod{487}$

    ということで、計算結果が対応していそう

有理数を剰余環に埋め込んでの計算:例題

- 次に EEA(487, 228) を計算する
  - $(r_0, s_0, t_0) = (487, 1, 0)$
  - $(r_1, s_1, t_1) = (228, 0, 1)$
  - $(r_2, s_2, t_2) = (487, 1, 0) - 2\,(228, 0, 1) = (31, 1, -2)$
  - $(r_3, s_3, t_3) = (228, 0, 1) - 7\,(31, 1, -2) = (11, -7, 15)$
  - 剰余 $r_j \leqq 15$ になった段階で計算を終了

有理数を剰余環に埋め込んでの計算：例題

- EEA(487, 228) の計算（つづき）
  - $11 = (-7) \times 487 + 228 \times 15$
  - $11 \equiv 15 \times 228 \pmod{487}$
  - より,
  - $r = 11, t = 15$ とおくことで r/t を復元可能

定理 4.82 (有理数の再構成)

- $n, b, r^*, t^* \in \mathbb{Z}$
- $0 \leqq b < n, 0 \leqq r^* < n, t^* > 0$
- $\mathrm{EEA}(n, b) = \{(r_i, s_i, t_i)\}, i \in [0..\lambda+1]$
- $j \in \{0, \ldots, \lambda+1\}$: $r_j \leqq r^*$ を満たす最小のindex
  - $r' := r_j, \quad s' := s_j, \quad t' := t_j$
- $\exists\, r, s, t \in \mathbb{Z}$ s.t. $r = n s + b t, |n| \leqq r^*, 0 < |t| \leqq t^*$

定理 4.82 (有理数の再構成)

このとき、次が成り立つ:

1. $0 < |t'| \leqq t^*$
2. $n > 2\, r^*\, t^* \Rightarrow \exists\ q \neq 0 \in \mathbb{Z}$ s.t.

   $r = r'q\,,\ \ s = s'q\,,\ \ t = t'q$

有理数の（循環）小数表記からの復元

有理数の（循環）小数表記からの復元

- $z = \frac{s}{t}, \quad 0 \leq s < t < M$ …(1)
- $10^k > 2M^2$ を満たす k に対し、z の小数表記が

  $b = 0.z_1 z_2 z_3 \ldots z_k \ldots$ (2)

  小数第 k 位まではわかっているものとする
- このとき、次のアルゴリズムにより、z の既約分数表現が得られる

有理数の（循環）小数表記からの復元

Algorithm (Rational reconstruction)

- 入力:
  - $z = s/t$ (1) の (循環) 小数表記 b (2)
  - M
  - $t \leqq M$ を満たす M に対し、$10^k > 2M^2 \geqq t$ を満たす k
- 出力: z の既約分数表現 $z = s' / t'$

有理数の（循環）小数表記からの復元

Algorithm (Rational reconstruction)

1. $n \leftarrow 10^k$; $b' \leftarrow \lfloor n\, b \rfloor$;
2. EEA $(n, b') = \{(r_i, s_i, t_i)\}$を計算し、$r_j < M$ を満たす最小の j を求める;
3. $s' \leftarrow s_j$; $t' \leftarrow -t_j$;
4. return s' / t' ;

定理 4.83

- Algorithm (Rational reconstruction) の出力 s' / t' は、与えられた小数表記 b が表す有理数 z の既約分数表記である

例 4.83: 有理数の（循環）小数表記からの復元

循環小数 $0.\dot{2}85714\dot{}$ を既約分数で表す

- これまでの方法:

$$r = \frac{285714}{999999} = \frac{2}{7}$$

- 分母 t が $0 < t < M$ のとき、循環節の長さ（桁数）は $O(M)$ になるので、計算が大変

例 4.83: 有理数の（循環）小数表記からの復元

- Algorithm (Rational reconstruction) を用いた方法

$$r = 0.\dot{2}85714\dot{} = \frac{s}{t}$$

- アルゴリズムの入力
  - $b \leftarrow 0.285714$
  - $0 \leqq s < t \leqq M = 7$ とすると、
    $2 \times M^2 = 2 \times 49 = 98 < 10^k$ を満たす k の最小値は 2、よって $k \leftarrow 2$ とおく

例 4.83: 有理数の（循環）小数表記からの復元

- $n \leftarrow 10^2 = 100$;
- $b' \leftarrow \lfloor n\,b \rfloor = \lfloor 100 \times 0.285714 \rfloor = \lfloor 28.5714 \rfloor = 28$;
- EEA (100, 28) を $r_j < M = 7$ を満たすまで計算する
  - $(r_0, s_0, t_0) = (100, 1, 0)$
  - $(r_1, s_1, t_1) = (28, 0, 1)$
  - $(r_2, s_2, t_2) = (100, 1, 0) - 3\,(28, 0, 1) = (16, 1, -3)$
  - $(r_3, s_3, t_3) = (28, 0, 1) - 1(16, 1, -3) = (12, -1, 4)$
  - $(r_4, s_4, t_4) = (16, 1, -3) - 1(12, -1, 4) = (4, 2, -7)$

例 4.83: 有理数の（循環）小数表記からの復元

- EEA (100, 28) を $r_j < M = 7$ を満たすまで計算する
  - $(r_4, s_4, t_4) = (16, 1, -3) - 1(12, -1, 4) = (4, 2, -7)$
  - ここで $r_4 = 4 < 7 = M$ を満たすので計算終了
- よって r = $s_4 / (-t_4) = 2/7$

第11回のまとめ

- 有理数を剰余環に埋めこんでの計算
- 有理数の（循環）小数表記からの復元

第12回の内容

- 中国剰余算法の応用
  - モジュラ算法
    - 行列積の法計算 (§ 4.9)