⑩ 有理数の再構成 (rational reconstruction) (p.69)

- 有理数を剰余環に埋め込んで計算する.

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

↑ ↗

$\mathbb{Z}/p\mathbb{Z}$ に埋め込む. $\frac{r}{t}$ に対し

$|r| < 15$, $|t| < 16$ として $2|rt| = 2 \cdot 240$
$= 480 < p$ なる素数 p を選ぶ: $p := 487$.

- $\frac{r}{t}$ を $\mathbb{Z}/487\mathbb{Z}$ で表現する.

p: prime より $a \in \mathbb{Z}/487\mathbb{Z}$ は乗法の逆元をもつ.

$\therefore \exists t^{-1} \in \mathbb{Z}/487\mathbb{Z}$ s.t. $t \cdot t^{-1} \equiv 1 \bmod 487$.

そこで, $\frac{r}{t}$ を $r \cdot t^{-1}$ として $\mathbb{Z}/487\mathbb{Z}$ で表す.

t^{-1} の計算 → 法逆元 (modular inverse) の計算.

① $\frac{2}{5}$ より 5^{-1} の計算.

$\mathrm{EEA}(487, 5) = \{(r_i, s_i, t_i)\}_{i=0}^{\lambda+1}$

を計算する.

$(r_0, s_0, t_0) = (487, 1, 0)$
$(r_1, s_1, t_1) = (5, 0, 1)$
$(r_2, s_2, t_2) = (487, 1, 0) - 97(5, 0, 1) = (2, 1, -97)$.
$(r_3, s_3, t_3) = (5, 0, 1) - 2(2, 1, -97) = (1, -2, 195)$.
$\therefore 1 = (-2) \cdot 487 + 195 \cdot 5$.
$\therefore 5^{-1} = 195$.

よって $\frac{2}{5} \longrightarrow 2 \cdot 195 = 390 \bmod 487$
$\equiv \underline{390}$ を割り当てる.

② $\frac{1}{3}$ より 3^{-1} の計算.

EEA (487, 3) を計算する.

$(r_0, s_0, t_0) = (487, 1, 0)$
$(r_1, s_1, t_1) = (3, 0, 1)$
$(r_2, s_2, t_2) = (487, 1, 0) - 162(3, 0, 1) = (1, 1, -162)$
$\therefore 1 = 1 \cdot 487 - 162 \cdot 3$
$\therefore 3^{-1} = -162 \equiv 325 \mod 487.$
$\therefore \frac{1}{3} \longrightarrow 325$ を割り当てる.

③ ①, ② より
$\frac{2}{5} + \frac{1}{3} \longrightarrow 390 + 325 = 715 \equiv \underline{\underline{228}} \mod 487.$

④ 次の必要なのは
(i) $\frac{r}{t} = r \cdot t^{-1} \equiv 228 \mod 487$
をみたす r と t が存在するか?
(ii) もし (i) をみたす r, t が存在するならば, $\frac{r}{t}$ は $\frac{2}{5} + \frac{1}{3}$ の分母 n 対応しているか?

⑤ そこで, とりあえず, $\frac{2}{5} + \frac{1}{3} = \frac{6+5}{15} = \frac{11}{15}$ を
$\mathbb{Z}/487\mathbb{Z}$ の中に埋め込んでみる.

$15^{-1} \in \mathbb{Z}/487\mathbb{Z}$ を EEA (487, 15) で計算.

$(r_0, s_0, t_0) = (487, 1, 0)$
$(r_1, s_1, t_1) = (15, 0, 1)$
$(r_2, s_2, t_2) = (487, 1, 0) - 32(15, 0, 1) = (7, 1, -32)$
$(r_3, s_3, t_3) = (15, 0, 1) - 2(7, 1, -32) = (1, -2, 65)$
$\therefore 1 = -2 \cdot 487 + 65 \cdot 15$
$\therefore 15^{-1} = 65.$
よって $\frac{11}{15} \longrightarrow 11 \cdot 65 = 715 \equiv \underline{\underline{228}}$

計算分母が対応してそう!

⑥ 次の EEA (487, 228) を計算してみる.

$(r_0, s_0, t_0) = (487, 1, 0)$
$(r_1, s_1, t_1) = (228, 0, 1)$
$(r_2, s_2, t_2) = (487, 1, 0) - 2(228, 0, 1) = (31, 1, -2)$
$(r_3, s_3, t_3) = (228, 0, 1) - 7(31, 1, -2) = (11, -7, 15)$

$\uparrow$ 15 になった時点で計算終了.

$\therefore 11 = -7 \cdot 487 + 15 \cdot 8$
$\therefore \underbrace{11}_{\| \\ r} \equiv \underbrace{15}_{\| \\ t} \cdot 228 \mod 487$

とおくと. $\frac{r}{t} = \frac{11}{15}$ が復元できた! ☑

次の定理で, その理論的拡張を与える.

Theorem 4.80 (有理数の再構成)

$n, b, r^*, t^* \in \mathbb{Z}$.
$0 \le b < n$, $0 \le r^* < n$, $t^* > 0$.
$EEA(n, b) = \{(r_i, s_i, t_i)\}_{i=0}^{\lambda+1}$,

$j \in \{0, \dots, \lambda+1\}$: $r_j \le r^*$ をみたす最小の index.

$r' := r_j$, $s' := s_j$, $t' := t_j$.

このとき, $\exists r, s, t \in \mathbb{Z}$ s.t. $r = ns + bt$, $|n| \le r^*$, $0 < |t| \le t^*$.

このとき, 次が成り立つ.

(i) $0 < |t'| \le t^*$.
(ii) $n > 2r^* t^* \Rightarrow \exists q \ne 0 \in \mathbb{Z}$ s.t.

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

<Proof> $r_0 = n > r^* \geq 0 = r_{\lambda+1}$ より，j の定め well-defined かつ $j \geq 1$．このとき，以下の不等式が成り立つ．

$$0 \leq r_j < r^* < r_{j-1}, \quad 0 < |t_j|, \quad |r| < r^*, \quad 0 < |t| \leq t^*.$$

ついでに次の等式が成り立つ．

$$\begin{aligned} r_{j-1} &= n s_{j-1} + b t_{j-1}, \\ r_j &= n s_j + b t_j, \quad \cdots (1) \\ r &= n s + b t \quad \cdots (2) \end{aligned}$$

(i) $|t_j| < t^* \cdots (3)$ を示す（これが一番難しい）．そのために，以下の定義を行う．

$$\begin{aligned} \varepsilon &:= s_j t_{j-1} - s_{j-1} t_j, \\ \mu &:= (t_{j-1} s - s_{j-1} t) / \varepsilon, \\ \nu &:= (s_j t - t_j s) / \varepsilon. \end{aligned}$$

Theorem EEA (p. 30)，(ii) より，$\varepsilon = \pm 1$．かつ μ, ν とも整数．すると次式が成り立つ．

$$\begin{aligned} s_j \mu + s_{j-1} \nu &= s_j (t_{j-1} s - s_{j-1} t)/\varepsilon \\ &\quad + s_{j-1} (s_j t + t_j s)/\varepsilon \\ &= (s_j t_{j-1} s - s_{j-1} s_j t)/\varepsilon + (s_{j-1} s_j t - s_{j-1} t_j s)/\varepsilon \end{aligned}$$

（$s_j t_{j-1} s$ と $s_{j-1} s_j t$，$s_{j-1} s_j t$ と $s_{j-1} t_j s$ が cancelled）

$$= s \underbrace{(s_j t_{j-1} - s_{j-1} t_j)}_{=\varepsilon} / \varepsilon = s. \quad \cdots (4)$$

$$\begin{aligned} t_j \mu + t_{j-1} \nu &= t_j (t_{j-1} s - s_{j-1} t)/\varepsilon \\ &\quad + t_{j-1} (s_j t - t_j s)/\varepsilon \\ &= (t_j t_{j-1} s - s_{j-1} t t_j)/\varepsilon + (t_{j-1} t s_j - s t_{j-1} t_j)/\varepsilon \end{aligned}$$

（$t_j t_{j-1} s$ と $t_{j-1} t s_j$，$s_{j-1} t t_j$ と $s t_{j-1} t_j$ が cancelled）

$$= t \underbrace{(s_j t_{j-1} - s_{j-1} t_j)}_{=\varepsilon} / \varepsilon = t. \quad \cdots (5)$$

(4), (5) より (3) を示す．証明は以下の通り，3つの場合に分けて行う．

a) $\nu = 0$ のとき： (5) $t_j \mu + t_{j-1} \nu = t$
に $\nu = 0$ を代入すると $t_j \mu = t$．
$\therefore t_j \mid t$．かつ $t \neq 0$ より $|t_j| \leq |t| \leq t^*$．

b) $\mu\nu < 0$ のとき．t_j と t_{j-1} の符号は逆である (Thm. EEA, (iv)) ことから，(5) の $t_j \mu$ と $t_{j-1}\nu$ の符号は等しい (∵仮定より $t > 0$)．
ゆえに
$$|t| = |t_j \mu + t_{j-1} \nu| = |t_j \mu| + |t_{j-1} \nu| \geq |t_j|.$$
$$\therefore |t_j| \leq |t| < t^*.$$

c) $\nu \neq 0$ かつ $\mu\nu \geq 0$ の場合はない．

$r = ms + bt$ に (4) および (5) を代入すると

$$r = m(s_j \mu + s_{j-1} \nu) + b(t_j \mu + t_{j-1} \nu)$$
$$= \mu \underbrace{(ms_j + bt_j)}_{\| \; r_j} + \nu \underbrace{(ms_{j-1} + bt_{j-1})}_{\| \; r_{j-1}}$$
$$\therefore r = \mu r_j + \nu r_{j-1}.$$

$\nu \neq 0$ かつ μ と ν が同符号のとき，
$0 \leq b < n$ より $r_{j-1} > r_j \geq 0$ (同符号)．
ゆえに $|r| = |r_j \mu + r_{j-1} \nu| = |r_j \mu| + |r_{j-1} \nu| \geq r_{j-1}$ より
$r_{j-1} < |r| \leq r^*$．ゆえに $r_{j-1} > r^*$ の矛盾．

(iii) if $n > 2r^*t^* \Rightarrow \exists g \neq 0 \in \mathbb{Z}$
s.t. $r = r'g$, $s = s'g$, $t = t'g$ をみたす．

$n > 2r^*t^*$ を仮定する．(1), (2) より

$$r_j \equiv b t_j \pmod{n} \quad \cdots (6)$$
$$r \equiv bt \pmod{n} \quad \cdots (7)$$

が成りたつ．
(7) $\times t_j$ − (6) $\times t$ より

$$\begin{array}{rl} & rt_j \equiv bt t_j \pmod n \\ - & \underline{r_j t \equiv b t_j t \pmod n} \end{array}$$

$$rt_j - r_j t \equiv 0 \pmod n .$$

よって、$rt_j - r_j t$ は n の定数倍であるから、

$$|rt_j - r_j t| \leq \underset{\wedge\!\wedge}{|r|}\,|t_j| + |r_j|\,\underset{\wedge\!\wedge}{|t|} \leq 2r^*t^* < n ,$$

r^* (仮定)　t^* ((i)より)　r^* (仮定)　t^* (仮定)　n (仮定)

よって $rt_j - r_j t = 0$. ⋯ (§)

次に、(2) × t_j − (1) × t を計算すると、

$$\begin{array}{rl} & t_j r = t_j n s + bt t_j \quad \cdots (2)\times t_j \\ - & \underline{r_j t = n s_j t + b t_j t \quad \cdots (1)\times t} \end{array}$$

cancelled

$$\underline{rt_j - r_j t} = n(st_j - s_j t)$$
$$\parallel$$
$$0$$

$$\therefore \quad st_j - s_j t = 0 \quad \cdots (9)$$

(9) より $t_j \mid s_j t$. かつ $\underline{\gcd(s_j, t_j) = 1}$ より
$t_j \mid t$. ゆえに $\exists g \in \mathbb{Z}$ s.t. $t = t_j g$,
かつ $t \neq 0$ より $g \neq 0$.

Thm. EEA (iii)

(§) $rt_j - r_j t = 0$ に $t = t_j g$ を代入すると
$rt_j - r_j t_j g = 0$
$\therefore t_j(r - r_j g) = 0 \quad \therefore r = r_j g$.

(9) $st_j - s_j t = 0$ に $t = t_j g$ を代入すると
$st_j - s_j t_j g = 0$
$\therefore t_j(s - s_j g) = 0 \quad \therefore s = s_j g$.

以上より (ii) が示された。 □

⑧ 有理数の（循環）小数表現からの復元．

$x := \frac{s}{t}$，　$0 \leq s < t \leq M$ … (1)，

$10^k > 2M^2$ なる k に対し，その小数表示が…

$$b = 0.\underbrace{z_1 z_2 z_3 \cdots z_k}\cdots \quad \cdots (2)$$

小数点以下 k 桁より十分上まかっているものとする．

このとき，以下のアルゴリズムにより，その既約分数表現が得られる．

Algorithm（有理数の（循環）小数表現からの復元）

Input ・ $x = \frac{s}{t}$ $(0 \leq s < t)$ … (1) の小数表現 b … (2)

・ $10^k > 2M^2 \geq t$ をみたす k．

Output その既約分数表現 $x = s'/t'$．

1) $b' \leftarrow \lfloor 10^k b \rfloor$；

2) $\mathrm{EEA}(M, b') = \{(r_i, s_i, t_i)\}_{i=0}^{\lambda+1}$

を計算し，$r_j < M$ をみたす最小の j を求める；

3) $s' \leftarrow s_j$；　$t' \leftarrow -t_j$；

4) return $\frac{s'}{t'}$；　□

Theorem 4.81　上記アルゴリズムの出力 s'/t' は，

与えられた有理数 x の既約分数表現である．

(Proof) x の既約分数表記 s/t と，x の無限小数表記 $b = 0.z_1z_2z_3\cdots$ に対し．

Step 1), 2) より，$2M^2 < 10^k = n$ をみたす n と $b' = z_1z_2\cdots z_k$ が得られ，$0 \le b' < n$ が成り立つ．また．$n\cdot\frac{s}{t} = 10^k x$ の小数表示は

$z_1z_2\cdots z_k . z_{k+1}\cdots$ より，

$$b' = z_1z_2\cdots z_k \le n\cdot\frac{s}{t} < b'+1 . \quad \text{よって}$$

$$0 \le \frac{ns}{t} - b' < 1$$

$$\therefore\ ns - b't < t \qquad \text{(アルゴリズムの出力から)}$$

より，$r' = ms' + b't'$，$r^* = t^* = M$ とおけば，(r', s', t') は，Thm 4.80 の r, s, t に関する条件をみたす．n は $2r^*t^* = 2M^2 < n$ をみたすので，Thm. 4.80 (ii) より，$\exists q \neq 0 \in \mathbb{Z}$ s.t. $r = r'q$，$s = s'q$，$t = t'q$ だが，

s'/t' は既約分数より $q = 1$．従って $s = s'$，$t = t'$．

EEA より s', t' は互いに素 (Thm. EEA (iii))．よって ∎

例 4.82 循環小数 0.285714 を既約分数で表す．

① これまでの方法．

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

しかし．分母 t が $0 < t < M$ のとき．循環部の長さ (桁数) は $O(M)$ になるので．計算が大変．

(Shoup, §4.6.1)

③ Rational reconstruction による方法．

$r = 0.285714 = \frac{t}{s}$，$0 \le s < t \le M = 7$ とすると

$2\cdot M^2 = 2\cdot 7^2 = 98 < 10^e$ をみたす e の最小値として．よって $n = 10^2 = 100$ とおく．

まず、 $b = 10^2 \cdot r = 28.571428571428\ldots$ だから、
$b' = \lfloor b \rfloor = 28$ とおく。 (Alg. Step 1)

(Alg. Step 2) より $\mathrm{EEA}(100, 28) = \{(r_i, s_i, t_i)\}_{i=0}^{\lambda+1}$ を計算すると、 $r_i < M = 7$ をみたすまで

$(r_0, s_0, t_0) = (100, 1, 0)$,
$(r_1, s_1, t_1) = (28, 0, 1)$,
$(r_2, s_2, t_2) = (100, 1, 0) - 3(28, 0, 1)$
$= (16, 1, -3)$.
$(r_3, s_3, t_3) = (28, 0, 1) - 1(16, 1, -3)$
$= (12, -1, 4)$,
$(r_4, s_4, t_4) = (16, 1, -3) - 1(12, -1, 4)$
$= (4, 2, -7)$.
↑
ここで $r_4 < M$ をみたすので計算終了。
$r_4 = 4$, $M = 7$

よって、 $r = \dfrac{s_4}{-t_4} = \dfrac{2}{7}$.

□