② $b>0$ と仮定. $\therefore \lambda > 0$.
$\lambda = 1$ のとき自明.
$\lambda > 1$ とおく. このとき, $i = 0, \dots, \lambda-1$ のとき.

(☆) $\boxed{r_{\lambda-i} \geq \varphi^i}$ $\Rightarrow$ $i = \lambda - 1$ とおいて log をとると

$$r_1 \geq \varphi^{\lambda-1}$$
$$\| \quad b$$

$$\therefore \log b \geq (\lambda-1)\log\varphi.$$
$$\therefore \lambda - 1 \leq \frac{\log b}{\log \varphi} \qquad \therefore \lambda \leq \frac{\log b}{\log \varphi} + 1.$$

そこで, (☆) を示す. (帰納法)

$i = 0$ のとき $r_\lambda \geq 1 = \varphi^0$.
$i = 1$ 〃 $r_{\lambda-1} \geq r_\lambda + 1 \geq 2 \geq \varphi^1$.

$i = 2, \dots, \lambda - 1$ のとき. $\varphi^2 = \varphi + 1$ を用いると

$$r_{\lambda-i} \geq r_{\lambda-(i-1)} + r_{\lambda-(i-2)}$$
$$\geq \varphi^{i-1} + \varphi^{i-2} = \varphi^{i-2}\underbrace{(1+\varphi)}_{\| \ \varphi^2} = \varphi^i$$

により成りたつ. ▨

6/29 ↓

Note 上の証明は, $r_{\lambda-i}$ を構成するのに, g_i がどんな値をとると, 最も λ が大きくなるか (= 剰余をとる計算の回数が大きくなるか) という考察である. すると, $r_i = 1$, すなわち $r_{\lambda-i}$ がフィボナッチの数列 u_n になることがわかる. 7/6 ↓

Note K を体とするとき, $K[x]$ は, . Euclid 関数 d を $d(f) = \deg f$ で定義すれば Euclid 整域となり. Euclid の互除法が $\mathbb{Z}$ と同様に成りたつ.

Algorithm (Euclidean Algorithm)

EA (f, g)
入力 $f, g \in R$.

出力 $d \in R$: f と g の gcd.

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

4.3 拡張 Euclid 互除法

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

$\exists s, t \in \mathbb{Z}$ s.t. $sa + tb = d$.

このとき, s と t を効率的に計算する → 拡張 Euclid 互除法.

まず, その拡張となる定理を示す.

Theorem (EEA)

a, b, $r_0, \dots, r_{\lambda+1}$, $q_1, \dots, q_\lambda$: Thm. (EA) と同じ.
$s_0, \dots, s_{\lambda+1}$, $t_0, \dots, t_{\lambda+1} \in \mathbb{Z}$ を以下で定める:

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

このとき, 以下が成り立つ:

(i) $i = 0, \dots, \lambda+1$ について, $s_i a + t_i b = r_i$, とくに
$s_\lambda a + t_\lambda b = \gcd(a, b)$.

(ii) $i=0,\dots,\lambda$ において $s_i t_{i+1} - t_i s_{i+1} = (-1)^i$.
(iii) $i=0,\dots,\lambda+1$ において $\gcd(s_i, t_i) = 1$.
(iv) $i=0,\dots,\lambda$ において $t_i t_{i+1} \leq 0$ かつ $|t_i| \leq |t_{i+1}|$.
$i=1,\dots,\lambda$ において $s_i s_{i+1} \leq 0$ かつ $|s_i| \leq |s_{i+1}|$.
(v) $i=2,\dots,\lambda+1$ において $r_{i-1}|t_i| \leq a$ かつ $r_{i-1}|s_i| \leq b$.
(vi) $a>0 \Rightarrow$ $i=1,\dots,\lambda+1$ において $|t_i| \leq a$ かつ $|s_i| \leq b$.
$a>1$ かつ $b>0 \Rightarrow |t_\lambda| \leq \frac{a}{2}$ かつ $|s_\lambda| \leq \frac{b}{2}$.

Proof

(i) 帰納法. $i=0, 1$ のとき ok.
$i=2,\dots,\lambda+1$ のとき,

$$\begin{aligned} r_i &= r_{i-2} - r_{i-1} q_{i-1} \\ &= (s_{i-2}a + t_{i-2}b) - (s_{i-1}a + t_{i-1}b) q_{i-1} \\ &\qquad (\text{帰納法の仮定による}) \\ &= (s_{i-2} - s_{i-1}q_{i-1})a + (t_{i-2} - t_{i-1}q_{i-1})b \\ &= s_i a + t_i b \end{aligned}$$

により 成りたつ.

(ii) 帰納法. $i=0$ のとき ok.
$i=1,\dots,\lambda$ のとき,

$$\begin{aligned} s_i t_{i+1} - t_i s_{i+1} &= s_i(t_{i-1} - t_i q_i) - t_i(s_{i-1} - s_i q_i) \\ &= -(s_{i-1}t_i - t_{i-1}s_i) \quad (\text{展開して整理}) \\ &= -(-1)^{i-1} \quad (\text{帰納法の仮定より}) \\ &= (-1)^i \end{aligned}$$

により 成りたつ.

(iii) (ii) より ただちに 成りたつ.

(iv) 帰納法.
(t_i) $i=0$ のとき 明らか.
$i=1,\dots,\lambda$ のとき, $t_{i+1} = t_{i-1} - t_i q_i$.
このとき, 帰納法の仮定より t_{i-1} と t_i は異なる符号をもち,

$|t_i| \geq |t_{i-1}|$. これより $|t_{i+1}| = |t_{i-1}| + |t_i| \geq |t_i|$ かつ t_{i+1} の符号は t_i のそれと異なる.

(s_i) s_i の場合も同様. 但し $i \geq 1$.

(v) $$\begin{cases} a s_{i-1} + b t_{i-1} = r_{i-1} & \cdots ① \\ a s_i + b t_i = r_i & \cdots ② \end{cases}$$

ゆえに. $-② \times t_{i-1}$ $①\times t_i$ をみたして

$$\begin{aligned} a s_{i-1} t_i + b t_i t_{i-1} &= r_{i-1} t_i \\ - \quad a s_i t_{i-1} + b t_i t_{i-1} &= r_i t_i \end{aligned}$$

$$a(\underbrace{s_{i-1} t_i - s_i t_{i-1}}_{= (-1)^i \quad (\text{(iii) より})}) = t_i r_{i-1} - t_{i-1} r_i$$

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

ここで, (iv) より t_i と t_{i-1} が異なる符号をもつことを用いると

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

s_i についても同様にして示される (s_i のほうは, $① \times s_i - ② \times s_{i-1}$ から計算する).

(vi) $a > 0 \Rightarrow$ $i = 1, \dots, \lambda+1$ に対し $r_{i-1} > 0$.
ゆえに (v) より $|t_i| \leq a$, $|s_i| \leq b$.

$a > 1$ かつ $b > 0 \Rightarrow$ $\lambda > 0$, $r_{\lambda-1} \geq 2$
(等号成立は $a = 2$, $b = 1$ の場合)

ゆえに (v) より $r_{\lambda-1}|t_\lambda| \leq a$, $r_{\lambda-1}|s_\lambda| \leq b$
≥ 2 ≥ 2

$\therefore |t_\lambda| \leq \frac{a}{2}$, $|s_\lambda| \leq \frac{b}{2}$.

□

Algorithm (The Extended Euclidean Algorithm)

EEA (f, g)
入力 $f, g \in R$: Euclid 整域.
出力 $d = \gcd(f, g) \in R$, $fs + gt = d$ をみたす $s, t \in R$.

(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
$(q_i, r_{i+1}) \leftarrow r_{i-1} \div r_i$;
$s_{i+1} \leftarrow s_{i-1} - q_i s_i$;
$t_{i+1} \leftarrow t_{i-1} - q_i t_i$;
$i \leftarrow i + 1$;

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

(拡張) Euclid 互除法の応用

◎ 実数の連分数展開 (§4.13, p.73)

R: Euclid 整域 (例: $\mathbb{Z}$)
K: その商体 R/R (例: $\mathbb{Q}$)

$\frac{r_0}{r_1} \in K$ $(r_0, r_1 \in R)$ に対し, 以下の計算による分数の列を考える:

$$\frac{r_0}{r_1} = q_1 + \frac{r_2}{r_1} \qquad r_0 = q_1 r_1 + r_2$$

$$= q_1 + \frac{1}{\frac{r_1}{r_2}} = q_1 + \frac{1}{q_2 + \frac{r_3}{r_2}} = q_1 + \frac{1}{q_2 + \frac{1}{\frac{r_2}{r_3}}} \qquad r_1 = q_2 r_2 + r_3$$

$$= q_1 + \frac{1}{q_2 + \frac{1}{q_3 + \frac{r_4}{r_3}}} \qquad r_2 = q_3 r_3 + r_4$$

$$\vdots$$

$$= q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots + \cfrac{1}{q_k + \frac{r_{k+1}}{r_k}}}}} =: [q_1, q_2, \cdots, q_k, \frac{r_{k+1}}{r_k}]$$

$\frac{r_1}{r_0}$ の (正則) 連分数 (continued fraction) 展開

- 分子が r_{k+1} を除いてすべて 1
- $q_1 \in \mathbb{Z}$.
- $q_2, \cdots, q_k \in \mathbb{Z}$ かつ 正.

$r_{k+1} = 0$ のとき $[q_1, q_2, \cdots, q_k]$.

一般に $[q_1] = q_1$, $[q_1, q_2, \dots, q_k] = q_1 + \dfrac{1}{[q_2, \dots, q_k]}$.

☆ 連分数展開は, $(q_i, r_{i+1}) \longleftarrow r_{i-1} \div r_i$ $(i = 1, \dots, k)$ に対し Euclid の互除法を用いて求まる.

例 4.87 $\dfrac{126}{35}$ の連分数展開.

$$\frac{126}{35} = 3 + \frac{1}{\frac{35}{21}} = 3 + \frac{1}{1 + \frac{1}{\frac{21}{14}}} = 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\frac{14}{7} = 2}}}$$

$$= [3, 1, 1, 2]$$

• 無理数の (循環) 連分数表示.

$\alpha \in \mathbb{R}$ の連分数表示を考える.

$\alpha = \alpha_1$.

$$q_i = [\alpha_i], \quad \alpha_{i+1} = \frac{1}{\alpha_i - q_i} \quad (i = 1, 2, 3, \dots)$$

例 4.90 $\alpha = \sqrt{3}$.

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

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

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

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

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

NO. 44

DATE 7 · 5 · 2013

循環節

$$\text{よって} \quad \sqrt{3} = [1, 1, 2, 1, \overset{2}{\cancel{1}}, \overset{1}{\cancel{2}}, \dots] = [1, \overline{1, 2}]$$

☆ 実数(無理数) α を循環連分数で表す

$\Leftrightarrow$ $\alpha = \dfrac{m \pm \sqrt{n}}{\ell}$ $(m, n, \ell \in \mathbb{Z})$ と表される.

(2次無理数: 整係数の2次方程式の根)

7/6