NO. 28

DATE 5 · 23 · 2016

6/20

⑩ Euclid 互除法.

Theorem (EA) $a, b \in \mathbb{Z}$ with $a \geq b \geq 0$.
剰余つき除算により, $\lambda \geq 0$ が存在し,
$r_0, r_1, \dots, r_{\lambda+1}$ および $q_1, \dots, q_\lambda$ を次のように定める:

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

(このとき, $\begin{cases} \lambda = 0 & (b = 0) \\ \lambda > 0 & (b \neq 0) \end{cases}$.)

このとき, ① $r_\lambda = \gcd(a, b)$.

② $b > 0 \Rightarrow \lambda \leq \dfrac{\log b}{\log \varphi} + 1$.

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

(φ は $\varphi^2 - \varphi - 1 = 0$ をみたす.)

Proof ① (テキスト, p.51) Thm 4.15 を参照.

② $b > 0$ と仮定. $\therefore \lambda > 0$.

$\lambda = 1$ のときは自明.

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

(★) $r_{\lambda-i} \geq \varphi^i$ をみたせば十分.

(実際, $i = \lambda - 1$ のとき, $b = r_1 \geq \varphi^{\lambda-1}$.
両辺の対数をとると $\log b \geq (\lambda - 1) \log \varphi$.
$\therefore \lambda - 1 \leq \dfrac{\log b}{\log \varphi}$ $\therefore \lambda \leq \dfrac{\log b}{\log \varphi} + 1$.)

そこで, (★) を示す. (帰納法)

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

$i=2, \cdots, \lambda-1$ 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. □

Note 上の証明は, $r_{\lambda-i}$ を構成するのに, q_i がどんな値をとると λ が最も大きくなるか (= 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, $q_i = 1$, すなわち $r_{\lambda-i}$ が「フィボナッチの数列」になることがわかる.

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)

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; □

§3 拡張 Euclid 互除法 (The Extended Euclidean Algorithm)

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

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) $i = 0, \dots, \lambda+1$ に対し, $s_i a + t_i b = r_i$. とくに $s_\lambda a + t_\lambda b = \gcd(a, b)$.
(ii) $i = 0, \dots, \lambda$ に対し, $s_i t_{i+1} - t_i s_{i+1} = (-1)^i$.
(iii) $i = 0, \dots, \lambda+1$ に対し, $\gcd(s_i, t_i) = 1$.
(iv) $i = 0, \dots, \lambda$ に対し, $t_i t_{i+1} \le 0$ かつ $|t_i| \le |t_{i+1}|$
$i = 1, \dots, \lambda$ に対し, $s_i s_{i+1} \le 0$ かつ $|s_i| \le |s_{i+1}|$.
(v) $i = 1, \dots, \lambda+1$ に対し, $r_{i-1}|t_i| \le a$ かつ $r_{i-1}|s_i| \le b$.
(vi) $a > 0 \Rightarrow i = 1, \dots, \lambda+1$ に対し $|t_i| \le a$ かつ $|s_i| \le b$.
$a > 1$ かつ $b > 0 \Rightarrow |t_\lambda| \le \frac{a}{2}$ かつ $|s_\lambda| \le \frac{b}{2}$.

Proof

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

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

(帰納法の仮定)

より 成り立つ.