数理解析研究所講究録
1199巻 2001年 213-219

Lagrangeによる連分数展開のアルゴリズムの一般化の試み

名古屋大学大学院
人間情報学研究科　橋本　竜太(Ryuuta HASHIMOTO) *

概　要

実2次無理数の連分数展開のアルゴリズムとして, Lagrangeによるものが知られている. そのアルゴリズムは優れた特長をもつものであるが, 如何せん, 2次無理数にしか適用することができない. そこで, Lagrangeのアルゴリズムの優れた点を保持しながらも, より高次の代数的実数に適用できるアルゴリズムの構築が望まれる. 本講演では純3次体の無理数に適用できるアルゴリズムを構築する. 構築の過程において, 代数的数の連分数展開のアルゴリズムを構築するアルゴリズムを, 数式処理を利用して実装することに関する示唆が見出される.

1　実数の連分数展開と近似分数

実数 α に対して,

$$\alpha_0 = \alpha, \quad a_k = \lfloor \alpha_k \rfloor, \quad \alpha_{k+1} = \frac{1}{\alpha_k - a_k} \tag{1}$$

により, α の連分数展開

$$\alpha = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \cdots \tag{2}$$

が得られる. これを途中で打ち切って得られる有理数

$$a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \cdots + \frac{1|}{|a_k} \tag{3}$$

を α の第 k 近似分数と呼ぶ. 第 k 近似分数の分子 p_k および分母 q_k は次のようにして得ることができる.

$$p_{-1} = 1, \quad p_0 = a_0, \quad p_k = a_k p_{k-1} + p_{k-2},$$
$$q_{-1} = 0, \quad q_0 = 1, \quad q_k = a_k q_{k-1} + q_{k-2}.$$

なお, p_k と q_k は互いに素である.

*ryuuta@math.human.nagoya-u.ac.jp

2 実2次無理数の連分数展開

α を実2次無理数とする. このとき, 次を満たす整数 D, P, Q が存在する:

$$\alpha = \frac{P + \sqrt{D}}{Q}, \tag{4}$$

$$Q \mid D - P^2. \tag{5}$$

実際, (4) については問題ないだろう. もしも (5) が成り立っていなければ, 改めて DQ^2, $P|Q|, Q|Q|$ をそれぞれ D, P, Q とすればよい.

$P_0 = P, Q_0 = Q$ とする. だまされたと思って, 次の計算を実行して, 数列 $\{P_k\}_{k\geq 0}$, $\{Q_k\}_{k\geq 0}$, および整数列 $\{a_k\}_{k\geq 0}$ を求めてみよう.

$$a_k = \left\lfloor \frac{P_k + \sqrt{D}}{Q_k} \right\rfloor, \quad P_{k+1} = a_k Q_k - P_k, \quad Q_{k+1} = \frac{D - {P_{k+1}}^2}{Q_k}. \tag{6}$$

実は, これで α の連分数展開が得られるのである. 実際に, 次が成り立っている:

$$\alpha = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \cdots.$$

さらに, $\{P_k\}_{k\geq 0}, \{Q_k\}_{k\geq 0}$ は整数列である. このことは (5) より帰納法で証明することができる.

このようにして実2次無理数の連分数展開を得るアルゴリズムは, Lagrange により考案されたものとして知られている (たとえば [1, 第4章] 参照). 実2次無理数 α を小数で近似して素直に連分数展開を得る場合と比べて, Lagrange のアルゴリズムは次のような利点を持つ.

- 整数演算のみで計算を遂行できる. 誤差の入る余地がない.
- (2次方程式の解であるという) 代数的な性質が失われない.
- 2次無理数の連分数展開の循環性の証明に利用できる.
- 2元2次不定方程式の整数解の存在判定ならびに求解に利用できる. たとえば, 平方数ではない正整数 D について, $X^2 - DY^2 = N$ の整数解に関連して, D の近似分数を p_k/q_k とするとき, 次が成り立つ:

$$ {p_k}^2 - D{q_k}^2 = (-1)^{k+1} Q_{k+1}. \tag{7}$$

このように, Lagrange のアルゴリズムはいろいろと優れた面を持つ. しかしながら, 明らかに実2次無理数にしか適用できない. そこで, より高次の代数的無理数に対して適用できて, しかも Lagrange のアルゴリズムの利点を継承しているような, 連分数展開のアルゴリズムを考えることはできないだろうか.

3 一般化のヒント

Lagrange のアルゴリズムの一般化を考えるにあたって, 2 つのポイントを検討する. それらをここでは標語的に「基底の任意性」「係数の斉次化」ということにしよう.

3.1 基底の任意性

(4) における $\sqrt{D}$ の代わりに $\mathbb{Q}(\alpha)$ の任意の代数的整数を採っても, Lagrange のアルゴリズムと類似のアルゴリズムを構築できる. 実際, 次のようにすればよい.

実 2 次無理数 α に対して,

$$\alpha = \frac{P+\omega}{Q} \tag{8}$$

なる整数 P, Q, および $\mathbb{Q}(\alpha)$ の代数的整数 ω を採る. ここで, (5) に相当する条件は

$$Q \mid \mathcal{N}(P+\omega) \tag{9}$$

とすればよい. ただし, $\mathcal{N}$ は $\mathbb{Q}(\alpha)/\mathbb{Q}$ 上のノルムである. 条件 (9) が満たされないときには, 改めて $PQ, Q^2, Q\omega$ をそれぞれ P, Q, ω とすればよい.

$P_0 := P, Q_0 := Q$ とする. そして, 数列 $\{P_k\}_{k\geq 0}, \{Q_k\}_{k\geq 0}, \{a_k\}_{k\geq 0}$ を次で計算する:

$$a_k = \left\lfloor \frac{P_k+\omega}{Q_k} \right\rfloor, \quad P_{k+1} = a_k Q_k - P_k - \mathrm{Tr}(\omega), \quad Q_{k+1} = -\frac{\mathcal{N}(P_k+\omega)}{Q_k}. \tag{10}$$

ただし, Tr は $\mathbb{Q}(\alpha)/\mathbb{Q}$ 上のトレースである. このとき, $\{P_k\}_{k\geq 0}, \{Q_k\}_{k\geq 0}$ は整数列である. そして, α の連分数展開が次のように得られる:

$$\alpha = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \cdots.$$

このアルゴリズムは Lagrange のアルゴリズムの利点を継承している.

3.2 係数の斉次化

先のアルゴリズムにおいて ω の係数を必ずしも 1 にしなくても, やはり Lagrange のアルゴリズムと類似のアルゴリズムを構築できる. 実際, 次のようにすればよい.

実 2 次無理数 α に対して,

$$\alpha = \frac{P^{(0)} + P^{(1)}\omega}{Q} \tag{11}$$

なる整数 $P^{(0)}, P^{(1)}, Q$, および $\mathbb{Q}(\alpha)$ の代数的整数 ω を採る. ここで, (5) に相当する条件は

$$Q \mid \mathcal{N}(P^{(0)} + P^{(1)}\omega) \tag{12}$$

とすればよい. これが満たされないときには, 改めて $P^{(0)}Q, Q^2, Q\omega$ をそれぞれ $P^{(0)}, Q, \omega$ とすればよい.

$P_0^{(j)} := P^{(j)}, Q_0 := Q$ とする. そして, 数列 $\{P_k^{(j)}\}_{k\geq 0}^{j=0,1}, \{Q_k\}_{k\geq 0}, \{a_k\}_{k\geq 0}$ を次で計算する:

$$a_k = \left\lfloor \frac{P_k^{(0)} + P_k^{(1)}\omega}{Q_k} \right\rfloor, \tag{13}$$

$$P_{k+1}^{(0)} = a_k Q_k - P_k^{(0)} - \mathrm{Tr}(P_k^{(1)}\omega), \quad P_{k+1}^{(1)} = P_k^{(1)}, \quad Q_{k+1} = -\frac{\mathcal{N}(P_k^{(0)} + P_k^{(1)}\omega)}{Q_k}. \tag{14}$$

このとき, $\{P_k^{(j)}\}_{k\geq 0}^{j=0,1}, \{Q_k\}_{k\geq 0}$ は整数列である. そして, α の連分数展開が次のように得られる:

$$\alpha = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \cdots.$$

このアルゴリズムもまた Lagrange のアルゴリズムの利点を継承していることは確認できる.

4 純3次無理数の連分数展開

3次以上の代数的数の中でも簡単な場合として, 純3次体の無理数, すなわち, 整数 D, $P^{(j)}$ $(j = 0, 1, 2)$, Q により

$$\alpha = \frac{P^{(0)} + P^{(1)}\sqrt[3]{D} + P^{(2)}\sqrt[3]{D^2}}{Q} \tag{15}$$

と表わされる数 α の連分数展開について考察してみよう.

$$\frac{P_k^{(0)} + P_k^{(1)}\sqrt[3]{D} + P_k^{(2)}\sqrt[3]{D^2}}{Q_k} = a_k + \frac{1}{\dfrac{P_{k+1}^{(0)} + P_{k+1}^{(1)}\sqrt[3]{D} + P_{k+1}^{(2)}\sqrt[3]{D^2}}{Q_{k+1}}} \tag{16}$$

が成り立つような整数列 $\{P_k^{(j)}\}_{k\geq 0}^{j=0,1,2}, \{Q_k\}_{k\geq 0}$ を得るアルゴリズムが構築できると嬉しい. 実際にそれは可能である. 次のようにすればよい.

整数 $P^{(j)}$ $(j=0,1,2)$, Q は次を満たすとしてよい:

$$\begin{aligned} &Q^2 \mid \mathcal{N}\big(P^{(0)}+P^{(1)}\sqrt[3]{D}+P^{(2)}\sqrt[3]{D^2}\big),\\ &Q \mid ({P^{(0)}}^2 - DP^{(1)}P^{(2)}),\\ &Q \mid (D{P^{(2)}}^2 - P^{(0)}P^{(1)}),\\ &Q \mid ({P^{(1)}}^2 - P^{(0)}P^{(2)}). \end{aligned} \tag{17}$$

ここで $\mathcal{N}$ は $\mathbb{Q}(\sqrt[3]{D})/\mathbb{Q}$ 上のノルムである. もしも (17) が満たされていなければ, 改めて $Q^3D, Q^{3-j}P^{(j)}, Q^4$ をそれぞれ $D, P^{(j)}, Q$ とすればよい.

$P_0^{(j)} := P^{(j)}, Q_0 := Q$ とする. 数列 $\{P_k^{(j)}\}_{k\geq 0}^{j=0,1,2}, \{Q_k\}_{k\geq 0}, \{a_k\}_{k\geq 0}$ は次で計算する.

$$a_k = \left\lfloor \frac{P_k^{(0)}+P_k^{(1)}\sqrt[3]{D}+P_k^{(2)}\sqrt[3]{D^2}}{Q_k} \right\rfloor, \tag{18}$$

$$P_{k+1}^{(0)} = \frac{(P_k^{(0)}-a_kQ_k)^2 - DP_k^{(1)}P_k^{(2)}}{Q_k}, \tag{19}$$

$$P_{k+1}^{(1)} = \frac{D{P_k^{(2)}}^2 - (P_k^{(0)}-a_kQ_k)P_k^{(1)}}{Q_k}, \tag{20}$$

$$P_{k+1}^{(2)} = \frac{{P_k^{(1)}}^2 - (P_k^{(0)}-a_kQ_k)P_k^{(2)}}{Q_k}, \tag{21}$$

$$Q_{k+1} = -\frac{\mathcal{N}\big((P_k^{(0)}-a_kQ_k)+P_k^{(1)}\sqrt[3]{D}+P_k^{(2)}\sqrt[3]{D^2}\big)}{Q_k}. \tag{22}$$

条件 (17) より, $\{P_k^{(j)}\}_{k\geq 0}^{j=0,1,2}, \{Q_k\}_{k\geq 0}$ は整数列であることが証明できる. さらに, α の連分数展開は次のようになっている:

$$\alpha = a_0 + \frac{1|}{|a_1} + \frac{1|}{|a_2} + \cdots.$$

さて, このアルゴリズムは Lagrange のアルゴリズムの利点を継承しているだろうか. それについて, 筆者にはまだ十分な検討ができていない. ここでは, すぐにわかることを二三挙げるにとどめておこう.

- 整数演算のみで計算が遂行できるかということについては, (18) において $\sqrt[3]{D}$ をどのように扱うかによる. (6) において $\sqrt{D}$ をそれに近い整数で置き換えるのは問題なかった. しかし, (18) において $\sqrt[3]{D}$ をそれに近い整数で置き換えるてしまうと, a_k が正しく求まらない. 一方, 数値実験によれば, $\sqrt[3]{D}$ を小数で近似する場合, 同じ精度で素直に連分数展開をするときと比べれば, より長い連分数展開が得られるようである.

- 3 次の無理数であるという代数的な性質が失われないのは明らかである.

- 不定方程式の整数解の存在判定について, たとえば $X^3 - DY^3 = N$ を考えてみよう. ただし D は立方数ではない正整数とする. $\sqrt[3]{D}$ の近似分数を p_k/q_k としたとき, (7) の類似として, 次の式が成り立つ:

$$p_k{}^3 - Dq_k{}^3 = \frac{(-1)^{k+1}Q_{k+1}p_k}{P_{k+1}^{(1)}} = \frac{(-1)^{k+1}Q_{k+1}q_k}{P_{k+1}^{(2)}}. \tag{23}$$

5 アルゴリズムの導出

前節のアルゴリズムは, (16) から導出することができる. 実際, (16) の分母を払って, 1, $\sqrt[3]{D}$, $\sqrt[3]{D^2}$ が $\mathbb{Q}$ 上線型独立であることに注意すると, 次の等式が得られる.

$$\begin{cases} (P_k^{(0)} - a_kQ_k)P_{k+1}^{(0)} + DP_k^{(2)}P_{k+1}^{(1)} + DP_k^{(1)}P_{k+1}^{(2)} = Q_kQ_{k+1}, \\ P_k^{(1)}P_{k+1}^{(0)} + (P_k^{(0)} - a_kQ_k)P_{k+1}^{(1)} + DP_k^{(2)}P_{k+1}^{(2)} = 0, \\ P_k^{(2)}P_{k+1}^{(0)} + P_k^{(1)}P_{k+1}^{(1)} + (P_k^{(0)} - a_kQ_k)P_{k+1}^{(2)} = 0. \end{cases}$$

これを $P_{k+1}^{(0)}, P_{k+1}^{(1)}, P_{k+1}^{(2)}, Q_{k+1}$ に関する連立 1 次方程式と見ると, 次のように, 自由度 1 を込めてその解が求まる.

$$\begin{aligned} P_{k+1}^{(1)} &= T\big(DP_k^{(2)2} - (P_k^{(0)} - a_kQ_k)P_k^{(1)}\big), \\ P_{k+1}^{(2)} &= T\big(P_k^{(1)2} - (P_k^{(0)} - a_kQ_k)P_k^{(2)}\big), \\ P_{k+1}^{(0)} &= T\big((P_k^{(0)} - a_kQ_k)^2 - DP_k^{(1)}P_k^{(2)}\big), \\ Q_{k+1} &= -T\mathcal{N}\big((P_k^{(0)} - a_kQ_k) + P_k^{(1)}\sqrt[3]{D} + P_k^{(2)}\sqrt[3]{D^2}\big)/Q_k. \end{aligned}$$

$T = 1/Q_k$ と採れば, 前節のアルゴリズムが得られる.

6 メタアルゴリズムの構築を目指して

前節の議論を踏まえると, 有限次代数体 $K/\mathbb{Q}$ を固定したとき, K の元 α の連分数展開を得る Lagrange 流のアルゴリズムを, 次のようにして得ることができるのではないかと考えられる.

1. 代数的整数 $\omega \in K$ を固定する.
2. 次の式より, $(P_k^{(j)}, Q_k)$ から $(P_{k+1}^{(j)}, Q_{k+1})$ を求める式を決める.

$$\frac{\sum_{j=0}^{n-1} P_k^{(j)}\omega^j}{Q_k} = a_k + \frac{1}{\dfrac{\sum_{j=0}^{n-1} P_{k+1}^{(j)}\omega^j}{Q_{k+1}}}$$

3. 初期条件を決める

いわば, 連分数展開を得るアルゴリズムを得る, メタアルゴリズムとでもいえよう. 筆者には, このメタアルゴリズムの実装にこそ, 数式処理にさせなければならないのではないかという気がしているのだが, 残念ながらその実現には至っていない. この研究を進展させて, 近いうちに報告できるようにしたいものである.

参 考 文 献

[1] Scharlau, W. and Opolka, H. 志賀 弘典 訳. **フェルマーの系譜**. 日本評論社. 1994.