数理解析研究所講究録 第2092巻 2018年 63-74

Multidimensional p-adic continued fraction algorithms

東邦大学　安冨　真一 (Yasutomi Shin-ichi)[1]
Toho University
公立はこだて未来大学　斉藤　朝輝 (Saito Asaki)
Future University Hakodate
津田塾大学　田村　純一 (Tamura Jun-ichi)
Tsuda College

1　緒言

[8] の内容を中心に紹介する．p を素数とする．$\mathbb{Q}_p$ を p 進数体とし $\mathbb{Z}_p$ を p 進整数の集合とし $\mathbb{Z}_p^\times$ をその単数群とする．また $q \in \mathbb{Q}$ に対して $|q|_p := p^{-m}$, $ord_p(q) := m$ とする．ここで $q = p^m r$ および r は p と互いに素であるとする．$\alpha \in \mathbb{Q}_p$ は p 進展開 $\alpha = \sum_{n\in\mathbb{Z}} c_n p^n \in \mathbb{Q}_p \backslash \{0\}$ $(c_n \in \{0, 1, \ldots, p-1\})$ を持つが $\omega_p(\alpha)$, $\lfloor\alpha\rfloor_p$, $\langle\alpha\rangle_p$ を次のように定義する．

$$\begin{aligned}\omega_p(\alpha) &:= c_0,\\ \lfloor\alpha\rfloor_p &:= \Sigma_{n\in\mathbb{Z}_{\leq 0}} c_n p^n,\\ \langle\alpha\rangle_p &:= \Sigma_{n\in\mathbb{Z}_{>0}} c_n p^n.\end{aligned}$$

Schneider [10] は次の p 進連分数展開およびそのアルゴリズムを与えた．$\xi \in \mathbb{Z}_p$ に対して $a_0 \in \{0, 1, \ldots, p-1\}$ を　$\xi - a_0 \in p\mathbb{Z}_p$ となるように選び $\xi_1 := \xi - a_0$ とする．$\xi_n (n \geq 2)$ を次の漸化式で帰納的に決めていく．

$$\xi_n = \frac{p^{ord_p(\xi_{n-1})}}{\xi_{n-1}} - a_{n-1},$$

ここで $a_{n-1} \in \{1, \ldots, p-1\}$ は $\xi_n \in p\mathbb{Z}_p$ となるようにする．すると ξ は次の連分数展開を持つ．

$$\xi = a_0 + \cfrac{p^{ord_p(\xi_1)}}{a_1 + \cfrac{p^{ord_p(\xi_2)}}{a_2 + \cfrac{p^{ord_p(\xi_3)}}{a_3 + \ldots}}}.$$

この Schneider の連分数展開は残念ながら通常の連分数展開の Lagrange の定理にあたるものが成立しないことが知られている．Weger [13] は $\mathbb{Q}_p$ のある 2 次の元が周期的となら

[1] shinichi.yasutomi@sci.toho-u.ac.jp

ないことを示した. 一方で Weger [14] は Lattice に関する周期性を用いて Lagrange の定理にあたるものを述べた. Ruban [6] は Schneider とは異なる連分数展開およびそのアルゴリズムを与えた. しかし大音 (Ooto)[5] は $\mathbb{Q}_p$ のある 2 次の元が Ruban のアルゴリズムで周期的とならないことを示した. Ruban のアルゴリズムに関しては最近 $\mathbb{Q}_p$ の 2 次の元および有理数が周期的となる条件が [4] によって与えられた. Browkin[2] は Lagrange の定理が成立するようなアルゴリズムの探求を行っているが十分には成功していない. 戸次 (Bekki)[1] は geodesic 連分数展開を新たに定義しそれを用いてある条件の下で p 進連分数展開の Lagrange の定理にあたるものを述べた. 我々は [7] において新しい p 進連分数展開およびそのアルゴリズムを与えそれに対して Lagrange の定理が成立することを述べた.

一方高次元の p 進連分数展開の研究は田村 (Tamura)[11] を除いてほとんどないようである. 田村 (Tamura)[11] は特別な $(x_1, \ldots, x_n)$ に対してそれに収束するような高次元 p 進連分数展開を与えているが一般的なアルゴリズムを与えてはいない. ここでは Schneider の連分数展開を高次元化する枠組みを与えその中から具体的にいくつかのアルゴリズムを提案しそれらの性質を述べたい.

2 p 進高次元連分数展開の枠組み

通常の連分数展開も多くの種類があるが高次元連分数展開の世界も多種多様ある. p 進高次元連分数展開およびそのアルゴリズムを考えるときにも様々なアルゴリズムを考えることができる. ここではそれらのあるクラスを考え収束性の性質などは統一的に議論可能である. 実数の有理数による近似ではその数に整数をかけてそれが整数に近いようにするのが一般的である. ここでは整数にあたるものを $\mathbb{Q} \cap \mathbb{Z}_p$ として考えていきたい. また Schneider の連分数展開では $\mathbb{Q}_p$ の任意の元が連分数展開され得るが、我々の連分数展開の対象は $\mathbb{Q}_p$ の中の代数的な元に限定していきたい. これは一見大きな制限に見える. [12] において Jacobi-Perron アルゴリズム（厳密にいうとその近縁のアルゴリズム）では Lagrange の定理がほとんど期待できないことを数値計算で示した. また代数的な元の特性を使う新たに提案した連分数展開アルゴリズムでは Lagrange の定理が期待できることを述べている. 今回アルゴリズムの対象を代数的な元に限定するのはこの経験を踏まえている. $K \subset \mathbb{Q}_p$ を $\mathbb{Q}$ 上の $d(= s+1)$ 次数の拡大体とする. ただし $K = \mathbb{Q}$ のときは $s = 1$ とする.

次の写像:$\Phi : K^s \to \{1, 2, \ldots, s\} \times L(K^s) \times GL(s, \mathbb{Z}_p \cap \mathbb{Q}) \times (p\mathbb{Z}_p \cap Q)^s$. を考える. ここで、$L(K^s)$ は K^s 上の 1 次分数変換の集合とし $\overline{\alpha} = (\alpha_1, \ldots, \alpha_s) \in K^s$ および $F_{\overline{\alpha}} = (f_1, \ldots, f_s)^T$ に対して $\Phi(\overline{\alpha}) := (\phi(\overline{\alpha}), F_{\overline{\alpha}}, A_{\overline{\alpha}}, \gamma(\overline{\alpha}))$ とする. さらに $F_{\overline{\alpha}} = (f_1, \ldots, f_s)^T$ は次の性質を持つとする.

$$f_i(x_1, \ldots, x_s) := \begin{cases} \dfrac{u_{\phi(\overline{\alpha})} p^{ord_p(\alpha_{\phi(\overline{\alpha})})}}{x_{\phi(\overline{\alpha})}} - v_{\phi(\overline{\alpha})} & i = \phi(\overline{\alpha}), \\ \dfrac{u_i' p^k x_i}{x_{\phi(\overline{\alpha})}} - v_i' & i \neq \phi(\overline{\alpha}), \end{cases}$$

ここで $u_i, v_i, u_i' \in \mathbb{Z}_p^{\times} \cap \mathbb{Q}$, $v_i' \in \mathbb{Z}_p \cap \mathbb{Q}$, および $k = \max\{ord_p(\alpha_{\phi(\overline{\alpha})}) - ord_p(\alpha_i), 0\}$. さらに $f_i(\overline{\alpha}) \in p\mathbb{Z}_p$ $(1 \leq i \leq s)$ および $\gamma(\overline{0}) = \overline{0}$. また $\alpha_{\phi(\overline{\alpha})} = 0$ のときは

$$f_i(x_1, \ldots, x_s) := x_i.$$

このような Φ を c-map と呼ぶことにする. u_i, v_i, u_i' などをいろいろ選ぶことによりいろいろなアルゴリズムが定義できる. c-map とは通常の連分数における Gauss map のようなものと考えていただいてよい. c-map Φ に対して K^s 上の変換 $T_{\Phi(\overline{\alpha})}$ を次のように定義する. $\overline{x} \in K^s$ に対して

$$T_{\Phi(\overline{\alpha})}(\overline{x}) := A_{\overline{\alpha}} F_{\overline{\alpha}}(\overline{x}) + \gamma(\overline{\alpha}).$$

$\overline{\alpha} = (\alpha_1, \ldots, \alpha_s)^T \in K^s$ として $\overline{\alpha}^{(0)} := \overline{\alpha}$ とする. $\overline{\alpha}^{(1)}, \overline{\alpha}^{(2)}, \ldots$ を $\overline{\alpha}^{(n+1)} := T_{\Phi(\overline{\alpha}^{(n)})}(\overline{\alpha}^{(n)})$ で定義していく. このとき $\overline{\alpha}$ は Φ 連分数展開 $\{\Phi(\overline{\alpha}^{(0)}), \Phi(\overline{\alpha}^{(1)}), \ldots\}$ を持つということにする. また $T_{\Phi(\overline{\alpha})}$ を Φ 連分数変換と呼ぶことにする. この定義の中で $GL(s, \mathbb{Z}_p \cap \mathbb{Q})$ の要素が登場するが格子の簡約化を行うことを加味している. 後で具体的な例で提示したい.

n-th convergent $\pi(\overline{\alpha}; n)$ を次で定義する.

$$\pi(\overline{\alpha}; n) := T^{-1}_{\Phi(\overline{\alpha}^{(0)})} \cdots T^{-1}_{\Phi(\overline{\alpha}^{(n-1)})}(\overline{0}).$$

収束性に関して次の定理が成立する.

定理 1[8] $\Phi(\overline{\alpha}) = (\phi(\overline{\alpha}), F_{\overline{\alpha}}, A_{\overline{\alpha}}, \gamma(\overline{\alpha}))$ $(\overline{\alpha} = (\alpha_1, \ldots, \alpha_s)^T \in K^s)$ は c-map とする. $\alpha^{(n)}_{\phi(\overline{\alpha}^{(n)})}$ が無限に多くの n に対して 0 でないなら, $\lim_{n \to \infty} \pi(\overline{\alpha}; n) = \overline{\alpha}$.

3 アルゴリズムの例

3.1 $\Phi_0^{[\epsilon]}$ 連分数展開アルゴリズム

記号は前章と同様とする. $Ind := \{1, 2, \ldots, s\}$ とする. K を $\mathbb{Q}_p$ に含まれる $\mathbb{Q}$ 上の有限次拡大体とする. $\epsilon \in \{-1, 1\}$ とする. $\overline{\alpha} = (\alpha_1, \ldots, \alpha_s)^T \in K^s$ および $j \in Ind$ に対して $G_j^{[\overline{\alpha}, \epsilon]} = (g_1^{[\overline{\alpha}, \epsilon]; (j)}, \ldots, g_s^{[\overline{\alpha}, \epsilon]; (j)})$ を次のように定義する. $\alpha_j \neq 0$ とすると $\overline{x} := (x_1, \ldots, x_s)^T \in K^s$ および $i \in Ind$ に対して

$$g_i^{[\overline{\alpha}, \epsilon]; (j)}(\overline{x}) := \begin{cases} \dfrac{\epsilon p^{ord_p(\alpha_j)}}{x_j} - \omega_p \left(\dfrac{\epsilon p^{ord_p(\alpha_j)}}{\alpha_j} \right) & i = j, \\ \dfrac{\epsilon p^k x_i}{x_j} - \omega_p \left(\dfrac{\epsilon p^k \alpha_i}{\alpha_j} \right) & i \neq j, \end{cases}$$

ここで $k = \max\{ord_p(\alpha_j) - ord_p(\alpha_i), 0\}$.
$\alpha_j = 0$ のときは

$$G_j^{[\overline{\alpha}, \epsilon]}(\overline{x}) := \overline{x}.$$

$S=(s_{ij})\in GL(s,\mathbb{Z}_p\cap\mathbb{Q})$ は次の行列とする.

$$s_{ij}:=\begin{cases}\delta_{(i+1)j} & 1\le i\le s-1,\ 1\le j\le s,\\ \delta_{1j} & i=s,\ 1\le j\le s,\end{cases}$$

ここで $i\neq j$ $(i,j\in Ind)$ に対して　$\delta_{ii}:=1$ および $i\neq j$ のときは $\delta_{ij}:=0$. c-map $\Phi_0^{[\epsilon]}$ を以下で定義する. $\overline{\alpha}\in K^s$ に対して

$$\Phi_0^{[\epsilon]}(\overline{\alpha}):=(1,G_1^{[\overline{\alpha},\epsilon]},S,\bar{0}).$$

$s=1$ のとき $\Phi_0^{[1]}$ 連分数展開アルゴリズムは Schneider のアルゴリズムと一致する（K の元という限定付きであるが）.

3.2　$\Phi_1^{[\epsilon]}$ 連分数展開アルゴリズム

Hensel の補題ではある条件を満たす方程式について $\mathbb{Q}_p$ 内に解を持つことを述べるが条件 (H) はこのような最小多項式を持つ元の条件である. すなわち、

代数的な元 $\alpha\in p\mathbb{Z}_p$ が条件 (H) を有するとは α の $\mathbb{Q}$ 上の最小多項式 $x^n+a_1x^{n-1}+\ldots+a_n$ についてすべての $i\in\{1,\ldots,n\}$ について $a_i\in\mathbb{Z}_p$ であり $ord_p(a_{n-1})=0$ かつ $ord_p(a_n)>0$ とする.

これに関して次の補題が成立する.

補題 2[8] $K\subset\mathbb{Q}_p$ を $\mathbb{Q}$ 上の有限次拡大体とする. このときある $z\in K$ が存在し条件 (H) を持ちかつ $K=\mathbb{Q}(z)$ となる.

z を上記のような元とする. K^s 上の 1 次分数変換 $H_j^{[\overline{\alpha},\epsilon,z]}=(h_1^{[\overline{\alpha},\epsilon,z];(j)},\ldots,h_s^{[\overline{\alpha},\epsilon,z];(j)})$ $(1\le j\le s)$ を次のように定義する.

$\overline{\alpha}=(\alpha_1,\ldots,\alpha_s)^T\in K^s$ に対して $g_i^{[\overline{\alpha},\epsilon];(j)}(\overline{\alpha})$ は一次意的に $g_i^{[\overline{\alpha},\epsilon];(j)}(\overline{\alpha})=a_0+a_1z+\ldots+a_sz^s$ と書くことができる. ここで $a_i\in\mathbb{Q}$ $(0\le i\le s)$ である. $a'>0$ を $a_i(1\le i\le s)$ の分子の最大公約数とする. $\overline{x}=(x_1,\ldots,x_s)\in K^s$ に対して $h_i^{[\overline{\alpha},\epsilon,z];(j)}(\overline{x})$ $(0\le i,j\le s)$ を次のように定義する.

$$h_i^{[\overline{\alpha},\epsilon,z];(j)}(\overline{x}):=\frac{g_i^{[\overline{\alpha},\epsilon];(j)}(\overline{x})}{a'}-\left\langle\frac{a_0}{a'}\right\rangle_p.$$

c-map $\Phi_1^{[\epsilon,z]}$ を次のように定義する.

$$\Phi_1^{[\epsilon,z]}(\overline{\alpha}):=(1,H_1^{[\overline{\alpha},\epsilon,z]},S,\bar{0}),\ \overline{\alpha}\in K^s$$

$H_j^{[\overline{\alpha},\epsilon,z]}$ の定義で $a'>0$ で割るところは奇妙に感じる向きもあるかもしれないが、これらを更に洗練化させたものが後で述べる p-簡約と考えることができる. また $-\left\langle\frac{a_0}{a'}\right\rangle_p$ の部分は Ruban が与えた p 進連分数アルゴリズムの要素を入れていると考えることもできる.

3.3 $\Phi_2^{[\epsilon]}$ 連分数展開アルゴリズム

$\alpha \in K$ に対して $\alpha = a_0 + a_1 z + \ldots + a_s z^s$ とするとき $denom_z(\alpha)$ を次のように定義する.

$$denom_z(\alpha) := \min\{|d| \ |d \in \mathbb{Z}, d(a_0 + a_1 x + \ldots + a_s x^s) \in \mathbb{Z}[x]\},$$

$\overline{\alpha} = (\alpha_1, \ldots, \alpha_s)^T \in K^s$ に対して

$$denom_z(\overline{\alpha}) := \max\{denom_z(\alpha_i) | 1 \leq i \leq s\}$$

と定義する. さらに $v_{[\epsilon,z]}^{(1)} : K^s \to \mathbb{Z}$ を次のように定義する. $\overline{\alpha} = (\alpha_1, \ldots, \alpha_s)^T \in K^s$ に対して

$$v_{[\epsilon,z]}^{(1)}(\overline{\alpha}) := \min\{denom_z(H_i^{[\overline{\alpha},\epsilon,z]}(\overline{\alpha})) | 1 \leq i \leq s\}.$$

$(n = 2, 3, \ldots)$ に対して機能的に $v_{[\epsilon,z]}^{(n)} : K^s \to \mathbb{Z}$ を次のように決めていく.

$$v_{[\epsilon,z]}^{(n)}(\overline{\alpha}) := \min\{denom_z(H_i^{[\overline{\alpha},\epsilon.z]}(\overline{\alpha})) v_{[\epsilon,z]}^{(n-1)}(H_i^{[\overline{\alpha},\epsilon,z]}(\overline{\alpha})) | 1 \leq i \leq s\}.$$

$n \in \mathbb{Z}_{\geq 1}$ に対して $\phi_{[\epsilon,z]}^{(n)} : K^s \to \{1, \ldots, s\} (:= Ind)$ を

$$\phi_{[\epsilon,z]}^{(n)}(\overline{\alpha}) := \min\{i \in Ind | v_{[\epsilon,z]}^{(n+1)}(\overline{\alpha}) = denom_z(H_i^{[\overline{\alpha},\epsilon,z]}(\overline{\alpha})) v_{[\epsilon,z]}^{(n)}(H_i^{[\overline{\alpha},\epsilon,z]}(\overline{\alpha}))\}$$

ここで $\overline{\alpha} = (\alpha_1, \ldots, \alpha_s)^T \in K^s$. $\Phi_2^{[\epsilon,z],(n)}$ $(n \in \mathbb{Z}_{\geq 1})$ を以下のように定義する.

$$\Phi_2^{[\epsilon,z],(n)}(\overline{\alpha}) := (\phi_{[\epsilon,z]}^{(n)}(\overline{\alpha}), H_{\phi_{[\epsilon,z]}^{(n)}(\overline{\alpha})}^{[\overline{\alpha},\epsilon,z]}, id, \bar{0}),$$

ここで $\overline{\alpha} \in K^s$ および id は s 次元の単位行列である. この $\Phi_2^{[\epsilon,z],(n)}$ の定義は 1 次分数変換 $H_i^{[\overline{\alpha},\epsilon,z]}$ を n 回繰り返したときにもっとも height が小さくなる i を選らんでいくことを意味している. $\Phi_1^{[\epsilon,z]}(\overline{\alpha})$ ではつねに $i = 1$ となっている. $\Phi_2^{[\epsilon,z],(n)}$ では計算コストが高くなるという意味では良いアルゴリズムとは言えない. 本来は計算コストが低くなる適切な i の見つけ方が望まれるのであるが現時点では見つかっていない. このアルゴリズムの解析は難しく数値計算を行ったに過ぎないが、後で見るように $s = 2, n = 2$ で周期に落ちる例が多いので、周期性が期待できる計算コストが低くなるアルゴリズムの存在を予想させる.

3.4 $\Phi_3^{[\epsilon,z]}$ 連分数展開アルゴリズム

$$\alpha = \sum_{n \in \mathbb{Z}} c_n p^n \in \mathbb{Q}_p \backslash \{0\} \ (c_n \in \{0, 1, \ldots, p-1\}),$$

に対して $\lfloor \alpha : m \rfloor_p$ および $\langle \alpha : m \rangle_p$ を次のように定義する.

$$\lfloor \alpha : m \rfloor_p := \sum_{n \leq m} c_n p^n,$$
$$\langle \alpha : m \rangle_p := \sum_{n > m} c_n p^n.$$

$M(n;\mathbb{Q})$ を $\mathbb{Q}$ 係数 n 次正方行列の集合とする. $M = (m_{ij}) \in M(n;\mathbb{Q})$ が p-既約とは各 $i(1 \leq i \leq n)$ に対してある整数 $u(i)(0 \leq u(i) \leq n)$ が存在して次の (1)-(4) が成立することである.
(1) 任意の整数 $k(1 \leq k \leq u(i))$ に対して $\quad m_{ik} = 0$,
(2) $u(i) \neq n$ の場合, $m_{iu(i)+1} \in \{p^l | l \in \mathbb{Z}\}$, および 任意の整数 $k(i < k \leq n)$ に対して $m_{ku(i)+1} = 0$,
(3) $i > 1$ のとき, $u(i) \geq u(i-1)$,
(4) $u(i) \neq n$ の場合, 任意の整数 $j1 \leq j < i)$ に対して

$$\langle m_{ju(i)+1} : ord_p(m_{iu(i)+1}) - 1 \rangle_p = 0.$$

任意の $M(n;\mathbb{Q})$ の元は次の行基本変形で p-既約に変換される.
(a) 行の入れ替え,
(b) $Z_p^{\times} \cap \mathbb{Q}$ の元を行にかける,
(c) $\mathbb{Z}_p \cap \mathbb{Q}$ の元をある行にかけて他の行に加える.

$$\begin{pmatrix} p^2 & p+p^2 & \frac{1}{p^3} \\ 0 & p^3 & \frac{1}{p^2} \\ 0 & 0 & \frac{1}{p} \end{pmatrix}$$

p-既約な行列の例

$$\begin{pmatrix} 4 & 16 \\ 2 & 4 \end{pmatrix} \to \begin{pmatrix} 2 & 4 \\ 4 & 16 \end{pmatrix} \to \begin{pmatrix} 2 & 4 \\ 0 & 8 \end{pmatrix}$$

p-既約行列への変形の例 $(p = 2)$

次のように p-既約への変形は一意的である.

補題 3[8] $M \in M(n;\mathbb{Q})$ に対してある $N_1, N_2 \in GL(n, \mathbb{Z}_p \cap \mathbb{Q})$ に対して $N_1 M$ および $N_2 M$ が p-既約ならば $N_1 M = N_2 M$ が成立する.

したがって $M \in M(n;\mathbb{Q})$ に対して $N \in GL(n, \mathbb{Z}_p \cap \mathbb{Q})$ が一意的に決まり NM は p-既約となる. 我々はこの N を $pr(M)$ とする. また p-既約にすることを p-簡約と呼ぶ.

$z \in K$ は条件 (H) および $K = \mathbb{Q}(z)$ を満たすとする. $\overline{\alpha} = (\alpha_1, \ldots, \alpha_s)^T \in K^s$ に対して $\overline{\alpha} = M_{\overline{\alpha}}(z^s, \ldots, z, 1)^T$ とする. ただし $M_{\overline{\alpha}} = (m_{ij}) \in M(s \times (s+1); \mathbb{Q})$. $M'_{\overline{\alpha}} \in M_s(\mathbb{Q})$ を $M'_{\overline{\alpha}} := (m_{ij})_{1 \le i \le s, 1 \le j \le s}$ で定義する.

$\tau_z : K^s \to M_s(\mathbb{Z}_p \cap \mathbb{Q})$ を以下のように定義する.

$$\tau_z(\overline{\alpha}) := pr(M'_{\overline{\alpha}}), \ (\overline{\alpha} \in K^s).$$

$\gamma'(\overline{\alpha}) \in (p\mathbb{Z}_p \cap Q)^s$ を次で定義する.

$$\gamma'(\overline{\alpha}) := (-\langle l_{1s+1} \rangle_p, \ldots, -\langle l_{ss+1} \rangle_p)^T,$$

ここで $(l_{ij})_{1 \le i \le s, 1 \le j \le s+1} = pr(M'_{\overline{\alpha}}) M_{\overline{\alpha}}$.

c-map $\Phi_3^{[z]}$ を次で定義する.

$$\Phi_3^{[z]}(\overline{\alpha}) := (s, G_s^{[\overline{\alpha}, \epsilon, z]}, \tau_z(G_s^{[\overline{\alpha}, 1, z]}(\overline{\alpha})), \gamma'(\overline{\alpha})), \ (\overline{\alpha} \in K^s).$$

4 周期性について

この章では最初に有理数体ないしは2次数体における前章で定義したアルゴリズムによる周期性を述べる. さらに高次体に関する結果および予想を述べる.

命題 4[8] K を $\mathbb{Q}$ とする. 任意の有理数 α に対して α は有限の $\Phi_0^{[-1]}$ 連分数展開を持つ.

以下では $\epsilon \in \{-1, 1\}$ とする.

定理 5[8] $K \subset \mathbb{Q}_p$ は $\mathbb{Q}$ の2次拡大体であるとする. $z \in K$ は条件 (H) および $K = \mathbb{Q}(z)$ を満たすとする. このとき任意の $u \in K/\mathbb{Q}$ は周期的な $\Phi_1^{[\epsilon, z]}$ 連分数展開を持ち、$u \in \mathbb{Q}$ は有限の $\Phi_1^{[\epsilon, z]}$ 連分数展開を持つ.

$\Phi_3^{[z]}$ 連分数展開についても同様に、

定理 6[8] $K \subset \mathbb{Q}_p$ は $\mathbb{Q}$ の2次拡大体であるとする. $z \in K$ は条件 (H) および $K = \mathbb{Q}(z)$ を満たすとする. このとき任意の $u \in K/\mathbb{Q}$ は周期的な $\Phi_3^{[z]}$ 連分数展開を持ち、$u \in \mathbb{Q}$ は有限の $\Phi_3^{[z]}$ 連分数展開を持つ.

K が3次体以上については次の結果がある.

定理 7[15] $K \subset \mathbb{Q}_p$ は $\mathbb{Q}$ の3次拡大体であるとする. $z \in K$ は条件 (H) および $K = \mathbb{Q}(z)$ を満たすとする. さらに $x^3 + ax^2 + bx + cp^q$ を $\mathbb{Q}$ 上の z の最小多項式とする ($c \notin p\mathbb{Z}_p$). $a \in p\mathbb{Z}_p$ または $a + c \in p\mathbb{Z}_p$ とする. $(\alpha, \beta) \in K^2$ に対して $\{1, \alpha, \beta\}$ が $\mathbb{Q}$ 上線形独立ならば (α, β) は周期的な $\Phi_3^{[z]}$ 連分数展開を持つ.

K を与えたときの定理 7 の条件を満たす z の存在については次の命題がある.

命題 8[15] $K \subset \mathbb{Q}_p$ は $\mathbb{Q}$ の 3 次拡大体であるとする. ある $z \in K$ が存在し、条件 (H) および $K = \mathbb{Q}(z)$ を満たし $x^3 + ax^2 + bx + cp^q$ を $\mathbb{Q}$ 上の z の最小多項式とする ($c \notin p\mathbb{Z}_p$) とき $a \in p\mathbb{Z}_p$ または $a + c \in p\mathbb{Z}_p$ である.

数値実験 [8] により次を予想している. $s \geq 1$ とする.

予想 [8] $K \subset \mathbb{Q}_p$ は $\mathbb{Q}$ の $s+1$ 次拡大体であるとする. $z \in K$ は条件 (H) および $K = \mathbb{Q}(z)$ を満たすとする. $(\alpha_1, \ldots, \alpha_s) \in K^s$ に対して $\{1, \alpha, \ldots, \alpha_s\}$ が $\mathbb{Q}$ 上線形独立ならば $(\alpha_1, \ldots, \alpha_s)$ は周期的な $\Phi_3^{[z]}$ 連分数展開を持つ.

定理 6 より $s = 1$ で予想は成立し、定理 7 より $s = 2$ で部分的に予想は成立している. 次の定理で周期的になる無数の例を与えている.

定理 9[8] $K \subset \mathbb{Q}_p$ は $\mathbb{Q}$ の $s+1$ 次拡大体であるとする. $z \in K$ は条件 (H) および $K = \mathbb{Q}(z)$ を満たすとする. $1 \leq i \leq s-1$ に対して $u_i := \sum_{i \leq j \leq s} a_{ij} z^{s-j+1}$ とし、 また $u_s := z$ とする. ここで $a_{ij} \in \mathbb{Q} \cap \mathbb{Z}_p$ $(1 \leq i \leq s-1, i \leq j \leq s)$ および $a_{ii} \in \mathbb{Z}_p^{\times}$ $(1 \leq i \leq s-1)$. このとき, $\overline{\alpha} := (u_1, \ldots, u_s)^T$ は周期的な $\Phi_3^{[z]}$ 連分数展開を持つ.

5 数値実験

この章では [8] にあるいくつかの数値実験を示したい. 表 1 では素数 $2 \leq p \leq 100$ に対し最小多項式が $x^3 + ax + bp, (0 < a \leqq 10, -10 \leq b \leq 10, ord_p(a) = 0)$ である $z \in p\mathbb{Z}_p$ に対して、擬似乱数 [9] を用いて $\mathbb{Q}(z)$ 内にいくつかのデータ $\mathbb{Q}$ 上 $1, \alpha_1, \alpha_2$ が線形独立な (α_1, α_2) を生成しアルゴリズム $\Phi_1^{[\epsilon,z]}$ を適用したものである. 表 1 で 1^* は $\Phi_1^{[1,z]}$ 連分数変換を繰り返したところ height が 10^{300} 未満で周期的になったものの個数である. 2^* は $\Phi_1^{[1,z]}$ 連分数変換を繰り返したところ周期性を確認する前にその height が 10^{300} を越えてその変換の適用を停止させたものの個数. 3^*、4^* はそれぞれ $\Phi_1^{[-1,z]}$ 連分数変換に関する同種の個数とする.

表1

素数	1^*	2^*	3^*	4^*	素数	1^*	2^*	3^*	4^*
2	7514	886	7533	867	43	19183	617	19179	621
3	11052	1548	11706	1524	47	18972	1028	18982	1018
5	12534	2266	12576	2224	53	18593	1207	18599	1201
7	14872	2328	14843	2357	59	19164	636	19160	640
11	16424	2776	16441	2759	61	19776	224	19766	224
13	17388	1812	17383	1817	67	19577	223	19569	231
17	18063	1337	18083	1317	71	19598	202	19601	199
19	17956	1644	17934	1666	73	18965	835	18961	839
23	18099	1701	18115	1685	79	19203	797	19203	797
29	17493	2307	17496	2304	83	19774	26	19780	20
31	18627	1173	18636	1164	89	19573	227	19576	224
37	19331	469	19325	475	97	19335	665	19336	664
41	18395	1405	18395	1405					

以上のように $\Phi_1^{[\epsilon,z]}$ 連分数展開では Lagrange の定理が成立しない可能性がある.

表2では素数 $2 \leq p \leq 100$ に対し最小多項式が $x^3 + ax + bp, (0 < a \leqq 10, -10 \leq b \leq 10, ord_p(a) = 0)$ である $z \in p\mathbb{Z}_p$ に対して、擬似乱数 [9] を用いて $\mathbb{Q}(z)$ 内にいくつかのデータ $\mathbb{Q}$ 上 $1, \alpha_1, \alpha_2$ が線形独立な (α_1, α_2) を生成しアルゴリズム $\Phi_2^{[\epsilon,z],(2)}$ を適用したものである. 表1で 1^* は $\Phi_2^{[1,z],(2)}$ 連分数変換を繰り返したところ height が 10^{300} 未満で周期的になったものの個数である. 2^* は $\Phi_2^{[1,z],(2)}$ 連分数変換を繰り返したところ周期性を確認する前にその height が 10^{300} を越えてその変換の適用を停止させたものの個数. 3^*、4^* はそれぞれ $\Phi_2^{[-1,z],(2)}$ 連分数変換に関する同種の個数とする.

表 2

素数	1*	2*	3*	4*	素数	1*	2*	3*	4*
2	8393	7	8390	10	43	19800	0	19800	0
3	12584	16	12590	10	47	20000	0	20000	0
5	14792	8	14790	10	53	19800	0	19800	0
7	17196	4	17193	7	59	19800	0	19800	0
11	19200	0	19200	0	61	20000	0	20000	0
13	19200	0	19200	0	67	19800	0	19800	0
17	19397	3	19396	4	71	19800	0	19800	0
19	19600	0	19600	0	73	19800	0	19800	0
23	19800	0	19800	0	79	20000	0	20000	0
29	19800	0	19800	0	83	19800	0	19800	0
31	19800	0	19800	0	89	19800	0	19800	0
37	19800	0	19800	0	97	20000	0	20000	0
41	19800	0	19800	0					

この数値実験で注目すべきは周期的なものの割合が多いことである. $\Phi_2^{[\epsilon,z],(m)}$ 連分数展開で m を大きくすると周期的なものの割合が大きくなっていくようである. このことから [12] で議論したアルゴリズムのように連分数変換の各ステップで適切な項で割ることで周期的になるようにできる可能性を感じる.

表 3 では素数 $2 \leq p \leq 100$ に対し最小多項式が $x^6 + ax + bp, (0 < a \leqq 10, -10 \leq b \leq 10, ord_p(a) = 0)$ である $z \in p\mathbb{Z}_p$ に対して、擬似乱数 [9] を用いて $\mathbb{Q}(z)$ 内にいくつかのデータ $\mathbb{Q}$ 上 $1, \alpha_1, \alpha_2, \ldots, \alpha_5$ が線形独立な $(\alpha_1, \alpha_2, \ldots, \alpha_5)$ を生成しアルゴリズム $\Phi_3^{[z]}$ を適用したものである. 表 1 で 1^* は $\Phi_3^{[z]}$ 連分数変換を繰り返したところ height が 10^{300} 未満で周期的になったものの個数である. 2^* は $\Phi_3^{[z]}$ 連分数変換を繰り返したところ周期性を確認する前にその height が 10^{300} を越えてその変換の適用を停止させたものの個数.

表 3

素数	1^*	2^*	素数	1^*	2^*
2	9000	0	43	20000	0
3	13400	0	47	20000	0
5	15500	0	53	20000	0
7	17600	0	59	20000	0
11	19600	0	61	20000	0
13	19800	0	67	20000	0
17	19900	0	71	20000	0
19	19900	0	73	20000	0
23	19900	0	79	19900	0
29	19900	0	83	19900	0
31	19900	0	89	20000	0
37	19900	0	97	20000	0
41	19900	0			

この数値実験ではすべてのデータで周期性を確認することができた. これは予想が成立する可能性を多少なりとも示唆していると考える.

謝辞

本研究は JSPS 科研費 JP15K00342 の助成を受けている.

参考文献

[1] H.Bekki; On periodicity of geodesic continued fractions, J. Number Theory 177 (2017), 181-210.

[2] J. Browkin; Continued fractions in local fields. II. Math. Comp. 70 (2001), no. 235, 1281-1292.

[3] P. Bundschuh; p-adische Kettenbrüche und Irrationalität p-adischer Zahlen, Elem. Math. 32 (1977), no. 2, 36-40.

[4] L. Capuano. F. Veneziano, U. Zannier; An effective criterion for periodicity of l-adic continued fractions, arXiv:1801.06214.

[5] T. Ooto; Transcendental p-adic continued fractions, Math.Z(2017), no. 3-4, 1053-1064.

[6] A. A. Ruban; Certain metric properties of p-adic numbers, (Russian), Sibirsk. Mat. Zh. 11 (1970), 222-227.

[7] A. Saito, J.-I.Tamura, S. Yasutomi; p-adic continued fractions and Lagrange's theorem, arXiv:1701.04615.

[8] A. Saito, J.-I.Tamura, S. Yasutomi; Multidimensional p-adic continued fraction algorithms, arXiv:1705.06122.

[9] A. Saito, A.Yamaguchi; Pseudorandom number generation using chaotic true orbits of the Bernoulli map, Chaos 26 (2016), 063122.

[10] T. Schneider; Über p-adische Kettenbrüche, Symp. Math. 4 (1968/69), 181-189.

[11] J.-I.Tamura; A p-adic phenomenon related to certain integer matrices, and p-adic values of a multidimensional continued fraction, in: Summer School on the Theory of Uniform Distribution, RIMS Kôkyûroku Bessatsu **B29** (2012), 1-40.

[12] J.-I.Tamura, S. Yasutomi; A new multidimensional continued fraction algorithm, Math. Comp. 78 (2009), no. 268, 2209-2222.

[13] B. M. M.de Weger; Periodicity of p-adic continued fractions. Elem. Math. 43 (1988), no. 4, 112-116.

[14] B. M. M. de Weger; Approximation lattices of p-adic numbers, J. Number Theory 24 (1986), 70–88.

[15] S. Yasutomi; A multidimensional p-adic continued fraction algorithm and cubic number fields, in preparation.