数理解析研究所講究録 第2092巻 2018年 55-62

p進数体上の連分数アルゴリズムとその周期性

公立はこだて未来大学・システム情報科学部　斉藤 朝輝　(Asaki Saito)*
School of Systems Information Science, Future University Hakodate

津田塾大学・数学・計算機科学研究所　田村 純一　(Jun-ichi Tamura)
Institute for Mathematics and Computer Science, Tsuda College

東邦大学・理学部　安冨 真一　(Shin-ichi Yasutomi)
Faculty of Science, Toho University

1　はじめに

pを素数，$\mathbb{Q}_p$をp進数体，$\mathbb{Z}_p$をp進整数環とする．
実数の連分数展開の周期性に関しては，次の定理がよく知られている [3].

定理 1.1 (Lagrangeの定理). 実数αが2次無理数であることの必要十分条件は，αが周期的連分数展開をもつことである．

p進数の世界でも，様々な連分数アルゴリズムが考えられてきたが [6, 4, 2, 1]，任意の$\mathbb{Q}$上2次の$\mathbb{Q}_p$の元に対して，周期的展開をあたえるp進連分数アルゴリズムは，これまで存在しなかった．
我々は，$\alpha \in \mathbb{Q}_p$に対して，次の形の連分数を生成するアルゴリズムをいくつか構成した [5].

$$d_0 + \cfrac{t_1 p^{k_1}}{d_1 + \cfrac{t_2 p^{k_2}}{d_2 + \cfrac{t_3 p^{k_3}}{\ddots}}} \quad (k_n \in \mathbb{Z}_{>0},\ t_n \in \mathbb{Z} \setminus p\mathbb{Z},\ d_n \in \{1, \ldots, p-1\}\ (n \geq 1)). \tag{1}$$

ただし，d_0は$d_0 = [\alpha]_p$をみたす有理数である（$\alpha \in \mathbb{Q}_p$のp進整数部分$[\alpha]_p$の定義については (2) を参照のこと）．さらに，これらのアルゴリズムが，$\mathbb{Q}$上2次の$\mathbb{Q}_p$の元に対して周期的展開をあたえ，有理数に対して有限の展開をあたえることを示した．また，それぞれのアルゴリズムに関して，純周期的展開をもつ元を完全に特徴づけた．本稿では，これらの [5] の結果を紹介する．

2　p進連分数展開

以下では，特に断らない限り，αは$\mathbb{Q}_p$の元とする．また，αのp進展開を

$$\alpha = \sum_{i=-\infty}^{\infty} e_i p^i \quad (e_i = e_i(\alpha) \in \{0, 1, \ldots, p-1\})$$

*Email: saito@fun.ac.jp

とする（ただし，e_i $(i \leq 0)$ については，高々有限個の i でしか $e_i \neq 0$ にならない）．α の p 進整数部分 $[\alpha]_p$ および p 進小数部分 $\langle\alpha\rangle_p$ を

$$[\alpha]_p := \sum_{i=-\infty}^{0} e_i p^i, \qquad \langle\alpha\rangle_p := \sum_{i=1}^{\infty} e_i p^i \tag{2}$$

と定義する．この章では，α を

$$d_0 + \cfrac{t_1 p^{k_1}}{d_1 + \cfrac{t_2 p^{k_2}}{d_2 + \cfrac{t_3 p^{k_3}}{\ddots}}} \quad (k_i \in \mathbb{Z}_{>0},\ t_i, d_i \in \mathbb{Z}_p \setminus p\mathbb{Z}_p\ (i \geq 1))$$

という形の連分数に展開することを考える．ただし，$d_0 \in \mathbb{Q}$ は $d_0 = [\alpha]_p$ をみたすとする．このような連分数のクラスは，(1) の形の連分数を含むことを注意しておく．

t を $p\mathbb{Z}_p \setminus \{0\}$ から $\mathbb{Z}_p \setminus p\mathbb{Z}_p$ への写像とする．また，$v_p(\alpha)$ を，α の p 進付値とする．ここで，

$$\begin{aligned} &T : p\mathbb{Z}_p \setminus \{0\} \to p\mathbb{Z}_p, \\ &T(x) := \frac{t(x)p^{v_p(x)}}{x} - d(x) \end{aligned} \tag{3}$$

という形の写像の族を考える．ただし，d は，$p\mathbb{Z}_p \setminus \{0\}$ から $\mathbb{Z}_p \setminus p\mathbb{Z}_p$ への写像とする．ここで，$[d(x)]_p = \left[\frac{t(x)p^{v_p(x)}}{x}\right]_p \in \{1, \ldots, p-1\}$ となることは容易にわかる．よって，d の像 $\mathrm{Im}(d)$ が，$\mathrm{Im}(d) \subset \{1, \ldots, p-1\}$ をみたすならば，d は一意的に定まる．

$T^{n-1}(\langle\alpha\rangle_p) \neq 0$ $(n \in \mathbb{Z}_{>0})$ ならば，$T^{n-1}(\langle\alpha\rangle_p)$ は $T^n(\langle\alpha\rangle_p)$ を使って

$$T^{n-1}(\langle\alpha\rangle_p) = \frac{t(T^{n-1}(\langle\alpha\rangle_p))p^{v_p(T^{n-1}(\langle\alpha\rangle_p))}}{d(T^{n-1}(\langle\alpha\rangle_p)) + T^n(\langle\alpha\rangle_p)}$$

と表せる．$i \in \{1, \ldots, n\}$ に対して，

$$\begin{aligned} t_i &= t\left(T^{i-1}(\langle\alpha\rangle_p)\right), \\ k_i &= v_p\left(T^{i-1}(\langle\alpha\rangle_p)\right), \\ d_i &= d\left(T^{i-1}(\langle\alpha\rangle_p)\right) \end{aligned}$$

とおくと，

$$\alpha = [\alpha]_p + \cfrac{t_1 p^{k_1}}{d_1 + \cfrac{t_2 p^{k_2}}{d_2 + \cfrac{t_3 p^{k_3}}{\ddots + \cfrac{t_{n-1} p^{k_{n-1}}}{d_{n-1} + \cfrac{t_n p^{k_n}}{d_n + T^n(\langle\alpha\rangle_p)}}}}}$$

となる．

α の連分数展開に関して，以下の 3 つの場合が起こりうる．

(i) $\langle\alpha\rangle_p = 0$.

α の展開は $\alpha = [\alpha]_p$ となる（$\langle\alpha\rangle_p = 0$ は展開しない）．

(ii) $T^N(\langle\alpha\rangle_p)=0$ かつ $0\le n<N$ で $T^n(\langle\alpha\rangle_p)\neq 0$ となる $N\in\mathbb{Z}_{>0}$ が存在する．

このとき α は以下の有限連分数に展開される．

$$\alpha=[\alpha]_p+\cfrac{t_1p^{k_1}}{d_1+\cfrac{t_2p^{k_2}}{d_2+\cfrac{t_3p^{k_3}}{\ddots+\cfrac{t_Np^{k_N}}{d_N}}}}. \tag{4}$$

(iii) 全ての $n\in\mathbb{Z}_{\ge 0}$ で，$T^n(\langle\alpha\rangle_p)\neq 0$.

このとき α は以下の無限連分数に展開される．

$$[\alpha]_p+\cfrac{t_1p^{k_1}}{d_1+\cfrac{t_2p^{k_2}}{d_2+\cfrac{t_3p^{k_3}}{\ddots}}}. \tag{5}$$

ここで，次の 2 点について注意しておく．

(i) 写像 T としては様々なものを考えることができる．実際，5 章では，異なる 3 つの連分数アルゴリズムをあたえる．すなわち，$\alpha\in\mathbb{Q}_p$ に対して，(4) および (5) の連分数展開は一意的に定まらない．

(ii) $t(x)\equiv 1$ かつ $\mathrm{Im}(d)\subset\{1,\dots,p-1\}$ とすると，生成される連分数は Schneider の連分数 [6] となる．

3 連分数の収束性

2 章で述べた連分数の収束性を議論する上では，$p\mathbb{Z}_p\setminus\{0\}$ の元の展開だけを考えても一般性を失わない．(5) の t_i, k_i, d_i を使って，数列 $\{p_n\}_{n\ge -1}$ および $\{q_n\}_{n\ge -1}$ を，漸化式

$$\begin{cases} p_{-1}=1, & p_0=0, & p_n=d_np_{n-1}+t_np^{k_n}p_{n-2} & (n\ge 1),\\ q_{-1}=0, & q_0=1, & q_n=d_nq_{n-1}+t_np^{k_n}q_{n-2} & (n\ge 1). \end{cases}$$

によって定める．有限展開 (4) の場合には，$-1\le n\le N$ の範囲の n に対して，p_n と q_n を定める．

以下の関係が成り立つことは容易に示せる．

$$\cfrac{t_1p^{k_1}}{d_1+\cfrac{t_2p^{k_2}}{d_2+\cfrac{t_3p^{k_3}}{\ddots+\cfrac{t_np^{k_n}}{d_n}}}}=\frac{p_n}{q_n}\quad(n\ge 1),$$

$$\alpha=\frac{p_n+T^n(\alpha)p_{n-1}}{q_n+T^n(\alpha)q_{n-1}}\quad(n\ge 1),$$

$$p_{n-1}q_n - p_nq_{n-1} = \prod_{i=1}^{n}\left(-t_ip^{k_i}\right) \quad (n \geq 1),$$

$$|q_n|_p = 1 \quad (n \geq 0).$$

ただし，$|\alpha|_p$ は，$\alpha \in \mathbb{Q}_p$ の p 進絶対値を表す（つまり，$|\alpha|_p := 1/p^{v_p(\alpha)}$）．

2 章で述べた連分数の収束性に関して，以下の定理を示すことができる．

定理 3.1.

(i) $n \geq 1$ を整数とする．ただし，$T^N(\alpha) = 0$ となる整数 $N \geq 1$ が存在する場合には，$1 \leq n \leq N$ とする．このとき

$$\left|\alpha - \frac{p_n}{q_n}\right|_p = \frac{|T^n(\alpha)|_p}{p^{\sum_{i=1}^{n} k_i}}$$

となる．特に，$T^n(\alpha) \neq 0$ ならば，

$$\left|\alpha - \frac{p_n}{q_n}\right|_p = \frac{1}{p^{\sum_{i=1}^{n+1} k_i}}$$

となる．

(ii) 全ての $n \geq 1$ で，$T^n(\alpha) \neq 0$ とする．このとき

$$\lim_{n\to\infty} \frac{p_n}{q_n} = \alpha$$

となる．ただし，極限は，$\mathbb{Q}_p$ の通常の非アルキメデス的距離に関する極限を意味する．

4 基本写像 T_1 と T_2

A_p を，$p\mathbb{Z}_p$ の $\mathbb{Q}$ 上代数的な元で次数が高々2 のもの全てからなる集合とする．以下では，“$\mathbb{Q}$ 上代数的”を “代数的”，“$\mathbb{Q}$ 上 2 次” を “2 次” と略すことにする．ここでは，代数的な元 α の最小多項式として，最高次係数が正の整数係数多項式で，α を根としてもつもののうち次数が最小で，かつ，係数の最大公約数が 1 であるものを考える．$x \in A_p$ が 2 次のとき，x の最小多項式を $aX^2 + bX + c$ と表す．また，x が有理数のときは，最小多項式を $bX + c$ と表すことにする．$x \in A_p \setminus \{0\}$ に対して

$$u(x) := c|c|_p \in \mathbb{Z} \setminus p\mathbb{Z}$$

を対応させることにより，写像 $u : A_p \setminus \{0\} \to \mathbb{Z} \setminus p\mathbb{Z}$ を定義する．$A_p \setminus \{0\}$ から A_p への写像 T_1 と T_2 を，次のように定義する．

$$T_1(x) := \frac{u(x)p^{v_p(x)}}{x} - d_1(x),$$
$$T_2(x) := \frac{-u(x)p^{v_p(x)}}{x} - d_2(x).$$

ただし，d_1 と d_2 は $A_p \setminus \{0\}$ から $\{1, \ldots, p-1\}$ への写像で，一意的に定まる．定義域を考慮しなければ，T_1 と T_2 は写像 (3) の族に所属することを注意しておく．

次章で導入する連分数アルゴリズムは，$\mathbb{Q}_p$ の高々2 次の代数的な元の展開を，以下の補題で存在が保証されている $p\mathbb{Z}_p$ の元の展開に帰着させる．

補題 4.1 (Hensel の補題). $n \in \mathbb{Z}_{>0}$, $a_1 \in \mathbb{Z}\backslash p\mathbb{Z}$, $a_0 \in p\mathbb{Z}$ として $f(X) := X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ とする．このとき，$f(\alpha) = 0$ となる $\alpha \in p\mathbb{Z}_p$ がただ一つ存在する．

以下では，$b \in \mathbb{Z} \setminus p\mathbb{Z}$, $c \in p\mathbb{Z}$ である既約多項式 $X^2 + bX + c \in \mathbb{Z}[X]$ の根となる $p\mathbb{Z}_p$ の元を，2 次 Hensel 根と呼ぶことにする．同様に，$c \in p\mathbb{Z}$ である多項式 $X + c \in \mathbb{Z}[X]$ の根となる $p\mathbb{Z}_p$ の元（つまり，$-c$）を，1 次 Hensel 根と呼ぶことにする．

T_1 と T_2 は，2 次 Hensel 根を 2 次 Hensel 根にうつすことが証明できる．

5 連分数アルゴリズム

前章で導入した T_1 と T_2 を用いて，2 次の $\mathbb{Q}_p$ の元に対しては周期的展開をあたえ，有理数に対しては有限の展開をあたえる連分数アルゴリズムを構成できる．このようなアルゴリズムとしては様々なものを考えることができるが，本稿では 3 つのアルゴリズムを扱う．

前章と同様に，$x \in A_p$ の最小多項式を，x が 2 次の場合には $aX^2 + bX + c \in \mathbb{Z}[X]$ で表し，x が有理数の場合には $bX + c \in \mathbb{Z}[X]$ で表す．我々のアルゴリズムでは，あたえられた $x \in A_p \setminus \{0\}$ に対して，T_1 もしくは T_2 のどちらかが適用される．どちらが適用されるかは，x の次数にかかわらず，x の最小多項式の 2 つの係数 b と c とで決まる．以下では，各アルゴリズムで使用される写像 $T : A_p \setminus \{0\} \to A_p$ を指定することにより，3 つのアルゴリズムを指定する．

アルゴリズム A:

$$T(x) := T_2(x).$$

アルゴリズム B:

$$T(x) := \begin{cases} T_2(x) & \text{if } b \geq 0, \\ T_1(x) & \text{if } b < 0. \end{cases}$$

アルゴリズム C:

$$T(x) := \begin{cases} T_2(x) & \text{if } b \geq 0 \text{ and } c > 0, \\ T_1(x) & \text{otherwise.} \end{cases}$$

6 2 次の $\mathbb{Q}_p$ の元の展開

2 次 Hensel 根のアルゴリズム A, B, C による連分数展開の周期性に関して，以下の定理を示すことができる．

定理 6.1.

(i) アルゴリズム A（つまり，T_2）から得られる任意の *2* 次 *Hensel* 根の展開は，周期 *1* もしくは *2* で純周期的である．

(ii) アルゴリズム B から得られる任意の *2* 次 *Hensel* 根の展開は，周期 *1* で終局周期的（*eventually periodic*）である．

(iii) アルゴリズム Cから得られる任意の *2*次 *Hensel*根の展開は，終局周期的である．

次に，α を任意の 2 次の $\mathbb{Q}_p$ の元とし，α^σ を α 以外の α の共役元とする．以下の 6 つの場合に分けて考える．

Case 1 A: $|\alpha|_p < |\alpha^\sigma|_p$ かつ $|\alpha|_p \leq p^{-1}$,

B: $|\alpha|_p < |\alpha^\sigma|_p$ かつ $|\alpha|_p \geq 1$,

Case 2 A: $|\alpha|_p > |\alpha^\sigma|_p$ かつ $|\alpha|_p \leq p^{-1}$,

B: $|\alpha|_p > |\alpha^\sigma|_p$ かつ $|\alpha|_p \geq 1$,

Case 3 A: $|\alpha|_p = |\alpha^\sigma|_p$ かつ $|\alpha|_p \leq p^{-1}$,

B: $|\alpha|_p = |\alpha^\sigma|_p$ かつ $|\alpha|_p \geq 1$.

それぞれの場合について，以下のことが示せる．

Case 1A: $|\alpha|_p < |\alpha^\sigma|_p$ かつ $|\alpha|_p \leq p^{-1}$
T_1 もしくは T_2 を 1 回適用することにより，α は 2 次 Hensel 根にうつる．

Case 1B: $|\alpha|_p < |\alpha^\sigma|_p$ かつ $|\alpha|_p \geq 1$
$|\langle\alpha\rangle_p|_p \leq p^{-1}$ かつ $|\langle\alpha\rangle_p|_p < |\langle\alpha\rangle_p^\sigma|_p$ より，Case 1B は Case 1A に帰着する．

Case 2A: $|\alpha|_p > |\alpha^\sigma|_p$ かつ $|\alpha|_p \leq p^{-1}$
T_1 もしくは T_2 を 1 回適用することにより，Case 2A は Case 1A に帰着する．

Case 2B: $|\alpha|_p > |\alpha^\sigma|_p$ かつ $|\alpha|_p \geq 1$
$|\langle\alpha\rangle_p|_p \leq p^{-1}$ かつ $|\langle\alpha\rangle_p|_p < |\langle\alpha\rangle_p^\sigma|_p$ より，Case 2B は Case 1A に帰着する．

Case 3A: $|\alpha|_p = |\alpha^\sigma|_p$ かつ $|\alpha|_p \leq p^{-1}$
T_1 と T_2 を十分な回数反復適用することにより，Case 3A は，Case 1A もしくは Case 2A のどちらかに帰着する．

Case 3B: $|\alpha|_p = |\alpha^\sigma|_p$ かつ $|\alpha|_p \geq 1$
$|\langle\alpha\rangle_p|_p \neq |\langle\alpha\rangle_p^\sigma|_p$ ならば，Case 3B は Case 1A もしくは Case 2A に帰着する．そうでない場合は，Case 3B は Case 3A に帰着する．

結局，全ての場合で，T_1 と T_2 を何回か適用することにより，$\langle\alpha\rangle_p$ は 2 次 Hensel 根にうつる（このことは T_1 と T_2 を適用する順番によらない）．よって，定理 6.1 と合わせて次の結果が得られる．

定理 6.2. アルゴリズム *A, B, C*は，任意の $\mathbb{Q}$ 上 *2*次の $\mathbb{Q}_p$ の元に対して，周期的展開をあたえる．

7　有理数の展開

$\alpha = 0$ は 1 次 Hensel 根であるが，2 章で述べたように，$\alpha = 0$ はこれ以上展開しない．また，0 以外の任意の 1 次 Hensel 根に対して，どのアルゴリズムも有限の展開をあたえることが示せる．すなわち

定理 7.1. アルゴリズム A, B, C は，任意の *1* 次 *Hensel* 根に対して，有限展開をあたえる．

次に，α を任意の有理数とする．以下の 2 つの場合に分けて考える．

Case A: $|\alpha|_p \leq p^{-1}$,

Case B: $|\alpha|_p \geq 1$.

それぞれの場合について，以下のことが示せる．

Case A: $|\alpha|_p \leq p^{-1}$

α が 1 次 Hensel 根である場合には，我々のアルゴリズムは α に対し有限展開をあたえる（定理 7.1）．α が 1 次 Hensel 根でない場合には，T_1 もしくは T_2 を 1 回適用することにより，α は 1 次 Hensel 根にうつる．

Case B: $|\alpha|_p \geq 1$

$\langle\alpha\rangle_p \in \mathbb{Q}$ かつ $|\langle\alpha\rangle_p|_p \leq p^{-1}$ より，Case B は Case A に帰着する．

結局，有理数の展開は 1 次 Hensel 根の展開に帰着する．よって，定理 7.1 と合わせて次の結果が得られる．

定理 7.2. アルゴリズム A, B, C は，任意の有理数に対して，有限展開をあたえる．

8 純周期点の特徴づけ

最後に，それぞれのアルゴリズムに関して，純周期的展開をもつ元を特徴づけてみよう．ただし，純周期的展開においては，(1) の d_0 は 0 と考える．よって，純周期的展開をもつ元は $p\mathbb{Z}_p$ に含まれることになる．

定理 7.2 より，どのアルゴリズムでも，有理数の展開は周期的にならない．また，6 章で述べたように，2 次の $p\mathbb{Z}_p$ の元は T_1 と T_2 を何回か適用することにより 2 次 Hensel 根にうつる．よって，どのアルゴリズムでも，純周期的展開をもつ元の集合（既約集合）は，純周期的展開をもつ 2 次 Hensel 根の集合と一致する．

ここで，いくつか 2 次 Hensel 根の集合を定義する．2 次 Hensel 根 α を指定する際には，α と，α の最小多項式 X^2+bX+c の係数の組 (b,c) とを同一視すると便利なので，そうすることにする．S を，全ての 2 次 Hensel 根の集合，すなわち

$$S = \left\{(b,c) \in \mathbb{Z}^2 \mid b \in \mathbb{Z} \setminus p\mathbb{Z},\ c \in p\mathbb{Z}, X^2+bX+c \text{ は既約}\right\}$$

とする．また，集合 S_1, S_3, S_4, R, R_1, P_1 を以下のように定義する．

$$\begin{aligned}
S_1 &:= \{(b,c) \in S \mid b>0,\ c>0\},\\
S_3 &:= \{(b,c) \in S \mid b<0,\ c<0\},\\
S_4 &:= \{(b,c) \in S \mid b>0,\ c<0\},\\
R &:= \{(b,c) \in S \mid 1 \leq b \leq p-1\},\\
R_1 &:= \{(b,c) \in S_1 \mid 1 \leq b \leq p-1\},\\
P_1 &:= \left\{(b,c) \in S_1 \setminus R_1 \mid c < [b]_p \langle b\rangle_p\right\}.
\end{aligned}$$

アルゴリズム A は，全ての 2 次 Hensel 根に対して純周期的展開をあたえる（定理 6.1(i)）．また，アルゴリズム B による展開が純周期的となる 2 次 Hensel 根の集合は，R であることが簡単に示せる．さらに，アルゴリズム C による展開が純周期的となる 2 次 Hensel 根の集合は，$P_1 \cup R_1 \cup S_3 \cup S_4$ であることが証明できる．すなわち

定理 8.1. アルゴリズム A, B, C の既約集合は，それぞれ S, R, $P_1 \cup R_1 \cup S_3 \cup S_4$ である．

謝辞

本研究は JSPS 科研費 JP15K00342 の助成を受けたものです.

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), 1281–1292.

[3] J.-L. Lagrange, Additions au mémoire sur la résolution des équations numériques, Mém. Berl. 24 (1770).

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

[5] A. Saito, J.-I. Tamura, S. Yasutomi, Continued fraction algorithms and Lagrange's theorem in $\mathbb{Q}_p$, arXiv:1701.04615v1 [math.NT].

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