COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 67, No. 1 2019

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171–8501 JAPAN

# Continued Fraction Algorithms and Lagrange's Theorem in $\mathbb{Q}_p$

by

Asaki SAITO, Jun-ichi TAMURA, and Shin-ichi YASUTOMI

(Received October 10, 2018)

**Abstract.** We present several continued fraction algorithms, each of which gives an eventually periodic expansion for every quadratic element of $\mathbb{Q}_p$ over $\mathbb{Q}$ and gives a finite expansion for every rational number. We also give, for each of our algorithms, the complete characterization of elements having purely periodic expansions.

## 1. Introduction

In this paper, we intend to add a classical flavor to the $p$-adic world related to the well-known theorem of Lagrange (resp., Galois) on the complete characterization of eventually (resp., purely) periodic continued fractions (cf. [7], [5]; see also [9]).

In what follows, $p$ denotes a prime, $\mathbb{Q}_p$ the field of $p$-adic numbers, and $\mathbb{Z}_p$ the ring of $p$-adic integers. Schneider [11] gave an algorithm that generates continued fractions of the form

$$\cfrac{p^{k_1}}{d_1 + \cfrac{p^{k_2}}{d_2 + \cfrac{p^{k_3}}{\ddots}}} \quad \bigl(k_1 \in \mathbb{Z}_{\geq 0};\ k_{n+1} \in \mathbb{Z}_{>0}\,, d_n \in \{1, \dots, p-1\}\ (n \geq 1)\bigr)$$

and found periodic continued fractions for some quadratic elements of $\mathbb{Z}_p$ over $\mathbb{Q}$ (see also [3]). Ruban [10] gave an algorithm that generates continued fractions of the shape

$$g_0 + \cfrac{1}{g_1 + \cfrac{1}{g_2 + \cfrac{1}{\ddots}}},$$

where

$$g_n \in \left\{ \sum_{i=-m}^{0} e_i p^i \;\middle|\; m \in \mathbb{Z}_{\geq 0}\,, e_i \in \{0, 1, \dots, p-1\} \right\} \ (n \geq 0)\,.$$

---

*Key words and phrases.* Continued fraction algorithm, $p$-adic number, Lagrange's theorem

On the other hand, Weger [17] has found a class of infinitely many quadratic elements $\alpha \in \mathbb{Q}_p$ over $\mathbb{Q}$ such that the continued fraction expansion of $\alpha$ obtained by Schneider's algorithm is not periodic. Ooto [8] has found a similar result related to the algorithm given by Ruban. Weger [18] has considered that a simple and satisfactory $p$-adic continued fraction algorithm does not exist, and given a periodicity result of lattices concerning quadratic elements of $\mathbb{Q}_p$. Browkin [2] has proposed some $p$-adic continued fraction algorithms; nevertheless, the periodicity has not been proved for the continued fractions obtained by applying his algorithms to quadratic elements of $\mathbb{Q}_p$. By disclosing a link between $p$-adic numbers and the hermitian canonical forms of certain integral matrices, Tamura [12] has shown that a multidimensional periodic continued fraction converges to $\left(\alpha, \alpha^2, \ldots, \alpha^{n-1}\right)$ in the $p$-adic sense without considering algorithms of continued fraction expansion, where $\alpha$ is the root of a polynomial in $\mathbb{Z}[X]$ of degree $n$ stated in Lemma 4.1. Recently, Bekki [1] has shown the periodicity of his geodesic continued fraction algorithm, for some quadratic elements of $\mathbb{Q}_p$ with negative discriminants. However, it remains quite unclear whether or not there exists a simple algorithm that generates periodic continued fractions for all the quadratic elements of $\mathbb{Q}_p$.

The main objectives of this paper are to define some simple algorithms generating continued fractions of the form

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

and to give

(i) $p$-adic versions of Lagrange's theorem for the algorithms, i.e., the periodicity of the resulting continued fractions for all the quadratic elements of $\mathbb{Q}_p$ over $\mathbb{Q}$ (including those with positive discriminants), and

(ii) $p$-adic versions of Galois' theorem concerning purely periodic continued fractions.

Moreover, we show that the continued fraction expansions of an arbitrary rational number always terminate by our algorithms.

It is worth mentioning that our algorithms have a common background with those proposed in [13, 14, 15, 16, 4] in the design of continued fraction algorithms. As described earlier, Schneider's algorithm cannot give a periodic expansion for every quadratic element of $\mathbb{Q}_p$ over $\mathbb{Q}$. In contrast, our algorithms achieve the periodicity for every quadratic element by relaxing Schneider's restriction on numerators and by properly selecting $t_n$ in (1) from $\mathbb{Z} \setminus p\mathbb{Z}$.

The rest of this paper is organized as follows. In Section 2, we consider expanding $\alpha \in \mathbb{Q}_p$ into continued fractions whose form is more general than the form (1). In Section 3, we establish convergence properties of the continued fractions introduced in Section 2. In Section 4, we give two basic maps, $T_1$ and $T_2$, and present related lemmas. We define three algorithms in terms of these basic maps in Section 5. In Section 6, we show that each of our algorithms gives an eventually periodic expansion for every quadratic Hensel root, i.e., for every quadratic element of $\mathbb{Q}_p$ over $\mathbb{Q}$ whose existence is guaranteed by Hensel's Lemma. We do the same for every quadratic element in Section 7. In Sections 8 and 9, we show that the continued fractions for every rational number obtained by our algorithms always terminate. We conclude with several remarks in Section 10.

## 2. $p$-adic continued fraction expansions

In what follows, $\alpha$ denotes an element of $\mathbb{Q}_p$ unless otherwise mentioned. We mean by the $p$-adic expansion of $\alpha$ the series

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

with $e_i \neq 0$ at most finitely many $i \leq 0$. We define the $p$-adic integral and fractional parts of $\alpha$, denoted by $[\alpha]_p$ and $\langle\alpha\rangle_p$ respectively, as

$$[\alpha]_p := \sum_{i=-\infty}^{0} e_i p^i \quad \text{and} \quad \langle\alpha\rangle_p := \sum_{i=1}^{\infty} e_i p^i \,.$$

In this section, we consider expanding $\alpha$ into a continued fraction of the form

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

Note that this class of continued fractions contains ones of the form (1). Since the convergence of continued fractions can be proved in this general setting where $t_i$ and $d_i$ are in $\mathbb{Z}_p \setminus p\mathbb{Z}_p$, we deal with continued fractions of this form in this and the next sections. However, any of our algorithms introduced in Section 5 generates continued fractions whose $t_i$ and $d_i$ are in $\mathbb{Z} \setminus p\mathbb{Z}$ and $\{1, \dots, p-1\}$, respectively.

Let $t$ be a map from $\mathbb{Q}_p \setminus \{0\}$ to $\mathbb{Z}_p \setminus p\mathbb{Z}_p$. Then, $\frac{t(x)p^{v_p(x)}}{x} \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$ for all $x \in \mathbb{Q}_p \setminus \{0\}$, where $v_p(\alpha)$ denotes the $p$-adic additive valuation of $\alpha$. We consider a family of the maps of the form

$$\begin{aligned} T &: \mathbb{Q}_p \setminus \{0\} \to p\mathbb{Z}_p \,, \\ T(x) &:= \frac{t(x)p^{v_p(x)}}{x} - d(x) \,, \end{aligned} \tag{2}$$

where $d$ is a map from $\mathbb{Q}_p \setminus \{0\}$ to $\mathbb{Z}_p \setminus p\mathbb{Z}_p$. Since $d(x) = \frac{t(x)p^{v_p(x)}}{x} - T(x)$ and $T(x) \in p\mathbb{Z}_p$, we have $[d(x)]_p = \left[\frac{t(x)p^{v_p(x)}}{x}\right]_p \in \{1, \dots, p-1\}$ for all $x \in \mathbb{Q}_p \setminus \{0\}$. Hence, $d$ is uniquely determined if the image of $d$, denoted by $\mathrm{Im}(d)$, satisfies $\mathrm{Im}(d) \subset \{1, \dots, p-1\}$.

Since

$$x = \frac{t(x)p^{v_p(x)}}{d(x) + T(x)} \,,$$

we have

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

provided that $T^{n-1}(\alpha) \neq 0$ $(n \in \mathbb{Z}_{>0})$. Setting

$$\begin{aligned} t_i &:= t\bigl(T^{i-1}(\alpha)\bigr), \\ k_i &:= v_p\bigl(T^{i-1}(\alpha)\bigr), \\ d_i &:= d\bigl(T^{i-1}(\alpha)\bigr), \end{aligned}$$

for $i \in \{1, \dots, n\}$, we have

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

Related to the continued fraction expansion of $\alpha$, there occur three cases:

(i) $T^n(\alpha) \neq 0$ for all $n \in \mathbb{Z}_{\geq 0}$.

We can expand $\alpha$ into the infinite continued fraction

$$\cfrac{t_1 p^{k_1}}{d_1 + \cfrac{t_2 p^{k_2}}{d_2 + \cfrac{t_3 p^{k_3}}{\ddots}}}. \tag{3}$$

We will show that the continued fraction (3) converges to $\alpha$ in the succeeding section.

(ii) There exists $N \in \mathbb{Z}_{>0}$ such that $T^N(\alpha) = 0$ and $T^n(\alpha) \neq 0$ for all $0 \leq n < N$.

We can expand $\alpha$ into the finite continued fraction

$$\alpha = \cfrac{t_1 p^{k_1}}{d_1 + \cfrac{t_2 p^{k_2}}{d_2 + \cfrac{t_3 p^{k_3}}{\ddots + \cfrac{t_N p^{k_N}}{d_N}}}}. \tag{4}$$

(iii) $\alpha = 0$.

We do not expand $\alpha = 0$ any further.

REMARK 2.1.

(i) We can consider a variety of maps $T$. In fact, we will give three algorithms of continued fraction expansion in Section 5; consequently, the expression in continued fractions (3) and (4) are not uniquely determined for a given $\alpha \in \mathbb{Q}_p$.

(ii) The continued fractions considered by Schneider [11] are generated by setting $t(x) = 1$ for all $x \in \mathbb{Z}_p \setminus \{0\}$ and $\mathrm{Im}(d) \subset \{1, \dots, p-1\}$.

## 3. Convergence of continued fractions

In this section, we show that the continued fraction described in Section 2 always converges to $\alpha$ for $\alpha \in \mathbb{Q}_p$. Without loss of generality, we may assume that $\alpha \in p\mathbb{Z}_p \setminus \{0\}$ in this section.

We define two sequences $\{p_n\}_{n \geq -1}$ and $\{q_n\}_{n \geq -1}$ in terms of $t_i$, $k_i$, $d_i$ in (3) by the following recursion formulas:

$$\begin{cases} p_{-1} = 1\,, \quad p_0 = 0\,, \quad p_n = d_n p_{n-1} + t_n p^{k_n} p_{n-2} \quad (n \geq 1)\,, \\ q_{-1} = 0\,, \quad q_0 = 1\,, \quad q_n = d_n q_{n-1} + t_n p^{k_n} q_{n-2} \quad (n \geq 1)\,. \end{cases}$$

In the case of the finite expansion (4), we define $p_n$ and $q_n$ for $n$ with $-1 \leq n \leq N$.

Lemmas 3.1–3.3 given below are easily seen (cf. [9]).

LEMMA 3.1.

$$\cfrac{t_1 p^{k_1}}{d_1 + \cfrac{t_2 p^{k_2}}{d_2 + \cfrac{t_3 p^{k_3}}{\ddots + \cfrac{t_n p^{k_n}}{d_n}}}} = \frac{p_n}{q_n} \quad (n \geq 1)\ .$$

LEMMA 3.2.

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

LEMMA 3.3.

$$p_{n-1} q_n - p_n q_{n-1} = \prod_{i=1}^{n} \left( -t_i p^{k_i} \right) \quad (n \geq 1)\ .$$

We denote by $|\alpha|_p$ the $p$-adic absolute value of $\alpha \in \mathbb{Q}_p$, i.e., $|\alpha|_p := 1/p^{v_p(\alpha)}$.

LEMMA 3.4.

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

*Proof.* The claim is true for $n = 0$ and $n = 1$. Assuming that $|q_i|_p = 1$ holds for $0 \leq i \leq n$ with $n \geq 1$, we have $|q_{n+1}|_p = |d_{n+1} q_n + t_{n+1} p^{k_{n+1}} q_{n-1}|_p = 1$ since $|d_{n+1} q_n|_p = 1$ and $|t_{n+1} p^{k_{n+1}} q_{n-1}|_p \leq 1/p$. □

THEOREM 3.5.

(i) *Let $n$ be an integer with $n \geq 1$ or an integer with $1 \leq n \leq N$ if there exists an integer $N \geq 1$ such that $T^N(\alpha) = 0$. Then,*

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

*holds. In particular,*

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

*holds if $T^n(\alpha) \neq 0$.*

(ii) *Let $T^n(\alpha) \neq 0$ for all $n \geq 1$. Then,*

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

*holds.*

*Proof.* (i) By Lemma 3.2, we have

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

By Lemma 3.3, we have

$$\left|T^n(\alpha)\,(p_{n-1}q_n - p_nq_{n-1})\right|_p = \left|T^n(\alpha)\prod_{i=1}^{n}\left(-t_ip^{k_i}\right)\right|_p = \frac{|T^n(\alpha)|_p}{p^{\sum_{i=1}^{n} k_i}}.$$

By Lemma 3.4, we have

$$\left|\left(q_n + T^n(\alpha)q_{n-1}\right)q_n\right|_p = 1\,.$$

Hence, we get

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

If $T^n(\alpha) \neq 0$, then $|T^n(\alpha)|_p = 1/p^{k_{n+1}}$, which implies

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

The assertion (ii) immediately follows from (i). □

## 4. Two basic maps: $\mathbf{T_1}$ and $\mathbf{T_2}$

We later propose three continued fraction algorithms, each of which gives an eventually periodic expansion for every quadratic element of $\mathbb{Q}_p$ over $\mathbb{Q}$ and gives a finite expansion for every rational number. In this section, we introduce maps $T_1$ and $T_2$ on the basis of which we construct the algorithms.

We denote by $A_p$ the set of all the elements of $\mathbb{Q}_p$ which are algebraic over $\mathbb{Q}$ of degree at most two. For simplicity, we will abbreviate "algebraic over $\mathbb{Q}$" to "algebraic", and "quadratic over $\mathbb{Q}$" to "quadratic". We mean, by the minimal polynomial of an algebraic element $\alpha$, the integral polynomial of the lowest degree which has $\alpha$ as a root, whose leading coefficient is positive, and whose coefficients are coprime. We denote the minimal polynomial of $x \in A_p$ by $aX^2 + bX + c$ if $x$ is quadratic. We denote it by $bX + c$ if $x$ is rational. Note that $c \neq 0$ if and only if $x \neq 0$. Let us define a map $u : A_p \setminus \{0\} \to \mathbb{Z} \setminus p\mathbb{Z}$ by assigning

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

to each $x \in A_p \setminus \{0\}$. We put $A'_p := A_p \cap p\mathbb{Z}_p$. We define two maps $T_1$ and $T_2$ from $A_p \setminus \{0\}$ to $A'_p$ by

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

and

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

where $d_1$ and $d_2$ are maps from $A_p \setminus \{0\}$ to $\{1, \dots, p-1\}$ which are uniquely defined so as to let $T_1(x)$ and $T_2(x)$ belong to $p\mathbb{Z}_p$, and thus to $A'_p$, for every $x \in A_p \setminus \{0\}$. It is clear that $T_1$ and $T_2$ map any quadratic element of $A_p$ to a quadratic one. We remark that $T_1$ and $T_2$ belong to the family of the maps (2) if we ignore their domains.

Our algorithms introduced in the next section reduce expansions of algebraic elements of $\mathbb{Q}_p$ of degree at most two to expansions of those of $p\mathbb{Z}_p$ whose existence is guaranteed by the following well-known lemma (see, e.g., [6]).

LEMMA 4.1 (Hensel's Lemma). *Let* $f(X) := X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ *such that* $n \in \mathbb{Z}_{>0}$, $a_1 \in \mathbb{Z} \setminus p\mathbb{Z}$, *and* $a_0 \in p\mathbb{Z}$. *Then, there exists a unique* $\alpha \in p\mathbb{Z}_p$ *such that* $f(\alpha) = 0$.

In what follows, we call an element of $p\mathbb{Z}_p$ a *quadratic Hensel root* if it is a root of $X^2 + bX + c \in \mathbb{Z}[X]$ where $b \in \mathbb{Z} \setminus p\mathbb{Z}$, $c \in p\mathbb{Z}$, and $X^2 + bX + c$ is irreducible. Likewise, we call an element of $p\mathbb{Z}_p$ a *rational Hensel root* if it is a root of $X + c \in \mathbb{Z}[X]$ with $c \in p\mathbb{Z}$ (obviously, the root is $-c$).

LEMMA 4.2. $T_1$ *and* $T_2$ *map every quadratic Hensel root to a quadratic Hensel root.*

*Proof.* Let $\alpha \in p\mathbb{Z}_p$ be an arbitrary quadratic Hensel root. By definition, $\alpha$ has a minimal polynomial of the form $X^2 + bX + c \in \mathbb{Z}[X]$ with $b \in \mathbb{Z} \setminus p\mathbb{Z}$ and $c \in p\mathbb{Z}$. We see that the conjugate $\alpha^\sigma \neq \alpha$ of $\alpha$ satisfies $\alpha^\sigma \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$ since $\alpha^\sigma = -b - \alpha$. Since $\alpha = c/\alpha^\sigma$, we have $|\alpha|_p = |c|_p$. Recalling the definition of $u$, we see that

$$\frac{u(\alpha)p^{v_p(\alpha)}}{\alpha} = \frac{c}{\alpha} = \alpha^\sigma\,.$$

Let

$$\alpha^\sigma = \sum_{i=0}^{\infty} e_i p^i \quad \bigl(e_i \in \{0, 1, \dots, p-1\}, \quad e_0 \neq 0\bigr)\,.$$

Since $\alpha^\sigma$ is a root of $X^2 + bX + c$, we have $e_0\,(e_0 + b) \equiv 0 \pmod{p}$. Let $r$ be an element of $\{1, \dots, p-1\}$ satisfying $r \equiv b \pmod{p}$. Since $e_0 \neq 0$, we have $e_0 + b \equiv 0 \pmod{p}$, which implies $e_0 = p - r$. Thus, $d_1(\alpha) = p - r$, and we have $T_1(\alpha) = \alpha^\sigma - (p-r) \in p\mathbb{Z}_p$. By substituting $X + (p-r)$ for $X$ in $X^2 + bX + c$, we have the minimal polynomial of $T_1(\alpha)$ given by

$$X^2 + \bigl\{b + 2(p-r)\bigr\}X + (p-r)b + c + (p-r)^2 \in \mathbb{Z}[X]\,. \tag{5}$$

Since $\mathbb{Z} \setminus p\mathbb{Z} \ni b + 2(p-r) \equiv -r \pmod{p}$ and $(p-r)b + c + (p-r)^2 \in p\mathbb{Z}$, we see that $T_1(\alpha)$ is a quadratic Hensel root.

By a similar argument, we can show that $T_2(\alpha) = -\alpha^\sigma - r \in p\mathbb{Z}_p$ and its minimal polynomial is given by

$$X^2 + (-b + 2r)\,X - rb + c + r^2 \in \mathbb{Z}[X]\,. \tag{6}$$

Since $-b + 2r \in \mathbb{Z} \setminus p\mathbb{Z}$ and $-rb + c + r^2 \in p\mathbb{Z}$, we see that $T_2(\alpha)$ is also a quadratic Hensel root. □

REMARK 4.3. Both maps $T_1$ and $T_2$ preserve discriminants of the minimal polynomials of quadratic Hensel roots, i.e., the discriminants of (5) and (6) are equal to $b^2 - 4c$.

## 5. Continued fraction algorithms

On the basis of $T_1$ and $T_2$ introduced in the previous section, we can consider a variety of continued fraction algorithms which yield an eventually periodic expansion for every quadratic element of $\mathbb{Q}_p$ and yield a finite expansion for every rational number. In the present paper, we deal with three particular algorithms. As in Section 4, the minimal polynomial of $x \in A_p$ is denoted by $aX^2 + bX + c \in \mathbb{Z}[X]$ for quadratic $x$, and by $bX + c \in \mathbb{Z}[X]$ for rational $x$. Our algorithms decide which map, $T_1$ or $T_2$, is applied to a given $x \in A_p \setminus \{0\}$ on the basis of two coefficients of its minimal polynomial, namely the coefficient $b$ of $X$ and the constant term $c$, regardless of the degree of $x$. In the following, we specify our algorithms by specifying the map $T : A_p \setminus \{0\} \to A'_p$ used by each algorithm:

**Algorithm A:**

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

**Algorithm B:**

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

**Algorithm 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. Expansions of quadratic Hensel roots

In this section, we deal with the expansions of quadratic Hensel roots, on the basis of which we expand general quadratic elements of $\mathbb{Q}_p$. We show that each of our algorithms gives an eventually periodic expansion for any quadratic Hensel root. We will deal with the expansions of general quadratic elements of $\mathbb{Q}_p$ and those of rational numbers in the subsequent sections.

When considering an expansion of a quadratic Hensel root $\alpha$, it is convenient to identify $\alpha$ with the pair $(b, c)$ of coefficients of its minimal polynomial $X^2 + bX + c$. In the following, we will do so and allow writing $\alpha = (b, c)$. Similarly, we write $T(\alpha)$ also as $T(b, c)$. We note that in view of (5) and (6), we have

$$T_1(b, c) = \Big(b + 2(p - r), (p - r)b + c + (p - r)^2\Big), \tag{7}$$

and

$$T_2(b, c) = \big( - b + 2r, -rb + c + r^2\big), \tag{8}$$

where $r$ is an element of $\{1, \ldots, p - 1\}$ satisfying $r \equiv b \pmod p$.

Let $S$ be the set of all quadratic Hensel roots, i.e.,

$$S := \Big\{(b, c) \in \mathbb{Z}^2 \;\Big|\; b \in \mathbb{Z} \setminus p\mathbb{Z},\ c \in p\mathbb{Z}, \text{ and } X^2 + bX + c \text{ is irreducible}\Big\} .$$

We put

$$\begin{aligned} S_1 &:= \big\{(b, c) \in S \mid b > 0,\ c > 0\big\}, \\ S_2 &:= \big\{(b, c) \in S \mid b < 0,\ c > 0\big\}, \\ S_3 &:= \big\{(b, c) \in S \mid b < 0,\ c < 0\big\}, \\ S_4 &:= \big\{(b, c) \in S \mid b > 0,\ c < 0\big\}. \end{aligned}$$

We further put

$$\begin{aligned} R &:= \big\{(b, c) \in S \mid 1 \le b \le p - 1\big\}, \\ R_1 &:= \big\{(b, c) \in S_1 \mid 1 \le b \le p - 1\big\}, \\ R_4 &:= \big\{(b, c) \in S_4 \mid 1 \le b \le p - 1\big\}. \end{aligned}$$

In the following subsections, we give Theorems 6.1, 6.3, and 6.5 which state the periodicity of the continued fraction expansion obtained by Algorithms A, B, and C, for any given quadratic Hensel root.

### 6.1. Expansions of quadratic Hensel roots by Algorithm A

THEOREM 6.1. *The expansion of every quadratic Hensel root obtained by Algorithm A (i.e., $T_2$) is purely periodic with period one or two.*

*Proof.* Let $(b, c) \in S$. Let $r$ be an element of $\{1, \ldots, p - 1\}$ satisfying $r \equiv b \pmod p$. Then, $T_2(b, c) = \big(-b + 2r, -rb + c + r^2\big)$. Using $-b + 2r \equiv r \pmod p$, we easily see that $T_2^2(b, c) = (b, c)$. Thus, $(b, c)$ is a purely periodic point with period two or one. ☐

REMARK 6.2. It is easy to see that $(b, c) \in S$ is a fixed point of $T_2$ if and only if $(b, c) \in R$.

### 6.2. Expansions of quadratic Hensel roots by Algorithm B

THEOREM 6.3. *The expansion of every quadratic Hensel root obtained by Algorithm B is eventually periodic with period one.*

*Proof.* Let $(b, c) \in S$. We will show that $(b, c)$ is an eventually fixed point of the map $T$ associated with Algorithm B by considering the following three cases:

(i) $b \in \{1, \dots, p-1\}$. According to the definition of Algorithm B, we apply $T_2$ to $(b, c) \in R$. As described in Remark 6.2, such $(b, c)$ is a fixed point.

(ii) $b < 0$. We apply $T_1$ to $(b, c)$ with $b < 0$. We can write $b = -np + r$, where $n \in \mathbb{Z}_{>0}$ and $r \in \{1, \dots, p-1\}$. Let $(b', c') = T_1(b, c)$. Then, $b' = -(n-1)p + p - r$. Thus, the $n$-fold iteration of $T_1$ maps $(b, c)$ to a fixed point given in (i).

(iii) $b > p$. We apply $T_2$ to $(b, c)$ with $b > p$. We can write $b = np + r$, where $n \in \mathbb{Z}_{>0}$ and $r \in \{1, \dots, p-1\}$. Let $(b', c') = T_2(b, c)$. Since $b' = -np + r < 0$, this case reduces to (ii). ☐

By the proof of Theorem 6.3, we get the following corollary.

COROLLARY 6.4. *The set of purely periodic points of $T$ associated with Algorithm B within $S$ is $R$.*

### 6.3. Expansions of quadratic Hensel roots by Algorithm C

THEOREM 6.5. *The expansion of every quadratic Hensel root obtained by Algorithm C is eventually periodic.*

*Proof.* We will show that every orbit of $T$ associated with Algorithm C starting from a quadratic Hensel root is eventually periodic.

First, we need to discuss the dynamics of $T$ on $S$. We apply $T_2$ to $(b, c) \in S_1$ and $T_1$ to $(b, c) \in \bigcup_{i=2}^{4} S_i$. We see by (7) that there exists no fixed point of $T_1$ in $\bigcup_{i=2}^{4} S_i$ since $b \neq b + 2(p - r)$. Thus, the fixed points of $T$ on $S$ are those of $T_2$ in $S_1$, i.e., the points $(b, c) \in R_1$ (cf. Remark 6.2). We see by (7) that in $S_4$, the values of $b$ and $c$ strictly increase with each iteration of $T_1$, and thus every $(b, c) \in S_4$ is eventually mapped into $S_1$. Every $(b, c) \in S_1$ other than the fixed points is mapped into either $S_2$ or $S_3$ under $T_2$ (cf. Proof (iii) of Theorem 6.3). In $S_2$ and $S_3$, the value of $b$ strictly increases with each iteration of $T_1$, and every $(b, c) \in S_2 \cup S_3$ is eventually mapped into $R = R_1 \cup R_4$ (cf. Proof (ii) of Theorem 6.3).

Second, we should note that $T_1$ on $S$ is bijective. The inverse map $T_1^{-1} : S \to S$ is given by

$$T_1^{-1}(b, c) = \left(b - 2r, -rb + c + r^2\right), \tag{9}$$

where $r$ is an element of $\{1, \dots, p-1\}$ satisfying $r \equiv b \pmod{p}$.

Due to the dynamics of $T$ on $S$, any orbit starting from a quadratic Hensel root eventually enters either $R_1$ or $R_4$. If the orbit enters $R_1$, then the orbit is eventually periodic with period one since every element of $R_1$ is a fixed point.

In what follows, we will show that the orbit entering $R_4$ is also eventually periodic by showing that every element of $R_4$ is a purely periodic point. Let $(b_0, c_0) \in R_4$. Repeated iteration of $T$ (i.e., $T_1$) eventually maps $(b_0, c_0)$ into $S_1$. Two cases occur:

(i) $(b_0, c_0)$ is mapped into $S_1$ by iterating $T$ even times, i.e., there exists $n \in \mathbb{Z}_{>0}$ such that $T^{2n}(b_0, c_0) \in S_1$ and $T^i(b_0, c_0) \in S_4$ for $0 \leq i \leq 2n-1$.

(ii) $(b_0, c_0)$ is mapped into $S_1$ by iterating $T$ odd times, i.e., there exists $n \in \mathbb{Z}_{>0}$ such that $T^{2n-1}(b_0, c_0) \in S_1$ and $T^i(b_0, c_0) \in S_4$ for $0 \leq i \leq 2n-2$.

We note the following fact: Let $r := b_0 \in \{1, \ldots, p-1\}$. By induction, we can show

$$\begin{aligned} T_1^{2k}(b_0, c_0) &= (2pk + r,\ p^2k^2 + rpk + c_0) \qquad &(k \in \mathbb{Z}), \\ T_1^{2k-1}(b_0, c_0) &= (2pk - r,\ p^2k^2 - rpk + c_0) \qquad &(k \in \mathbb{Z}). \end{aligned}$$

Let us consider Case (i). We see that

$$\begin{aligned} T^{2n}(b_0, c_0) &= T_1^{2n}(b_0, c_0) \\ &= (2pn + r,\ p^2n^2 + rpn + c_0) \in S_1. \end{aligned}$$

Hence, we have

$$\begin{aligned} T^{2n+1}(b_0, c_0) &= T_2(2pn + r,\ p^2n^2 + rpn + c_0) \\ &= (-2pn + r,\ p^2n^2 - rpn + c_0). \end{aligned}$$

On the other hand, we see that

$$\begin{aligned} T_1^{-2n}(b_0, c_0) &= (-2pn + r,\ p^2n^2 - rpn + c_0) \\ &= T^{2n+1}(b_0, c_0). \end{aligned}$$

Since $-2pn + r < 0$, we have

$$\begin{aligned} (b_0, c_0) &= T_1^{2n} \circ T^{2n+1}(b_0, c_0) \\ &= T^{4n+1}(b_0, c_0). \end{aligned}$$

Therefore, in Case (i), $(b_0, c_0)$ is a purely periodic point.

In a similar manner, we can prove that also in Case (ii), $(b_0, c_0)$ is a purely periodic point. ☐

REMARK 6.6. We see from the proof of Theorem 6.5 that Algorithm C can generate periodic continued fractions of arbitrary long periods.

The following lemma characterizes the set of purely periodic points of $T$ associated with Algorithm C within $S$.

LEMMA 6.7. *The set of purely periodic points of $T$ associated with Algorithm C within $S$ is $P_1 \cup R_1 \cup S_3 \cup S_4$, where $P_1$ is defined by*

$$P_1 := \left\{(b, c) \in S_1 \setminus R_1 \;\middle|\; c < [b]_p \langle b \rangle_p \right\}.$$

*Proof.* Every element of $R_1$ and $R_4$ is a purely periodic point (cf. the proof of Theorem 6.5).

Every $(b, c) \in S_4 \setminus R_4$ is a purely periodic point since $(b, c)$ is mapped into $R_4$ by iterating $T_1^{-1}$. Thus, every element of $S_4$ is a purely periodic point.

It is not difficult to see that $(b, c) \in S_1 \setminus R_1$ is a purely periodic point if and only if $T_1^{-1}(b, c) \in S_4$ which, by (9), is equivalent to $c < rb - r^2 = [b]_p \langle b \rangle_p$. Hence, $P_1$ is the set of all purely periodic points in $S_1 \setminus R_1$.

There exists no purely periodic point in $S_2$. In fact, we can see this as follows: Let $(b, c)$ be an arbitrary element of $P_1$. We have $T_2(b, c) \in S_3$ since $-rb + c + r^2 = c - [b]_p \langle b \rangle_p < 0$ (cf. (8)). Hence, no purely periodic orbit enters $S_2$.

Every orbit starting from $(b, c) \in S_3$ passes through $R_4$ and $P_1$, and then it re-enters $S_3$. We denote by $(b_0, c_0)$ (resp., $(b_*, c_*)$) the point in $R_4$ (resp., in $P_1$) on the orbit. Obviously, there exists $m \in \mathbb{Z}_{>0}$ such that $(b, c) = T_1^{-m}(b_0, c_0)$. Since $T_2(b_*, c_*) \in S_3$ is a point on the purely periodic orbit passing through $(b_0, c_0)$, there exists $m_* \in \mathbb{Z}_{>0}$ such that $T_2(b_*, c_*) = T_1^{-m_*}(b_0, c_0)$. We easily see that $T_1^{-1} \circ T_2(b_*, c_*) = (-b_*, c_*)$. Since $b_* > p$ and $c_* > 0$, we see that $T_1^{-1} \circ T_2(b_*, c_*) \in S_2$, which implies $m \leq m_*$. Hence, $(b, c)$ is a point on the purely periodic orbit passing through $(b_0, c_0)$. Therefore, every $(b, c) \in S_3$ is a purely periodic point. □

## 7. Expansions of quadratic elements of $\mathbf{Q_p}$

Let $\alpha$ be an arbitrary quadratic element of $\mathbb{Q}_p$. In this section, we will first show that each of the three algorithms gives an eventually periodic expansion for $\alpha$, by showing that $\alpha$ is mapped to a quadratic Hensel root under some iterate of $T_1$ and $T_2$. We will then give a theorem that characterizes elements having purely periodic expansions for each algorithm. In the last part of this section, we will give some examples of expansions of quadratic elements of $\mathbb{Q}_p$.

Let $\alpha^\sigma$ be the conjugate of $\alpha$ other than $\alpha$. We consider the following three cases:

Case 1: $|\alpha|_p < |\alpha^\sigma|_p$,
Case 2: $|\alpha|_p > |\alpha^\sigma|_p$,
Case 3: $|\alpha|_p = |\alpha^\sigma|_p$.

Case 1: $|\alpha|_p < |\alpha^\sigma|_p$:

Let $aX^2 + bX + c \in \mathbb{Z}[X]$ be the minimal polynomial of $\alpha$. We see that

$$|\alpha^\sigma|_p = \left| -\frac{b}{a} - \alpha \right|_p = \left| \frac{b}{a} \right|_p$$

and

$$|\alpha|_p = \left| \frac{c}{a\alpha^\sigma} \right|_p = \left| \frac{c}{b} \right|_p .$$

Since $|\alpha|_p < |\alpha^\sigma|_p$, we have

$$\left| \frac{ac}{b^2} \right|_p < 1 . \tag{10}$$

Recalling the definition of $u$, we see that

$$\frac{u(\alpha) p^{v_p(\alpha)}}{\alpha} = \frac{u(\alpha)}{\alpha|\alpha|_p} = \frac{c|b|_p}{\alpha} \in \mathbb{Z}_p \setminus p\mathbb{Z}_p .$$

By substituting $c|b|_p/X$ for $X$ in $aX^2+bX+c$, we have the minimal polynomial of $c|b|_p/\alpha$ given by

$$X^2 + b|b|_pX + ac|b^2|_p \in \mathbb{Z}[X] .$$

Note that $b|b|_p \in \mathbb{Z} \setminus p\mathbb{Z}$, and $ac|b^2|_p \in p\mathbb{Z}$ by (10). Hence, $c|b|_p/\alpha$ is the conjugate of the quadratic Hensel root $c|b|_p/\alpha^\sigma$. By the proof of Lemma 4.2, we can see that the $p$-adic fractional part of the conjugate of a quadratic Hensel root is also a quadratic Hensel root. Therefore, $T_1(\alpha) = \langle c|b|_p/\alpha \rangle_p$ and $T_2(\alpha) = \langle -c|b|_p/\alpha \rangle_p$ are quadratic Hensel roots.

Consequently, in Case 1, $\alpha$ is mapped to a quadratic Hensel root under one iteration of either $T_1$ or $T_2$.

Case 2: $|\alpha|_p > |\alpha^\sigma|_p$:

Let $aX^2 + bX + c \in \mathbb{Z}[X]$ be the minimal polynomial of $\alpha$. Following a discussion similar to the one in Case 1, we see that

$$|\alpha|_p = \left|\frac{b}{a}\right|_p , \quad |\alpha^\sigma|_p = \left|\frac{c}{b}\right|_p , \quad \text{and} \quad \left|\frac{b^2}{ac}\right|_p > 1 . \tag{11}$$

Let us consider the case of applying $T_1$ to $\alpha$. Since

$$T_1(\alpha) = \frac{u(\alpha)}{\alpha|\alpha|_p} - d_1(\alpha) ,$$

the conjugate $T_1(\alpha)^\sigma \neq T_1(\alpha)$ of $T_1(\alpha)$ is given by

$$T_1(\alpha)^\sigma = \frac{u(\alpha)}{\alpha^\sigma|\alpha|_p} - d_1(\alpha) .$$

By (11), we have

$$\left|\frac{u(\alpha)}{\alpha^\sigma|\alpha|_p}\right|_p = \left|\frac{b^2}{ac}\right|_p > 1 .$$

Since $|d_1(\alpha)|_p = 1$, we have

$$\left|T_1(\alpha)^\sigma\right|_p = \left|\frac{u(\alpha)}{\alpha^\sigma|\alpha|_p}\right|_p > 1 .$$

Similarly, in the case of applying $T_2$ to $\alpha$, we see that $|T_2(\alpha)^\sigma|_p > 1$.

Since $|T_1(\alpha)|_p \leq p^{-1}$ and $|T_2(\alpha)|_p \leq p^{-1}$, we see that $|T_1(\alpha)|_p < |T_1(\alpha)^\sigma|_p$ and $|T_2(\alpha)|_p < |T_2(\alpha)^\sigma|_p$. Therefore, Case 2 reduces to Case 1 after one iteration of $T_1$ or $T_2$.

Case 3: $|\alpha|_p = |\alpha^\sigma|_p$:

Let $\{\epsilon_n\}_{n\geq 1}$ be an arbitrary sequence in the set $\{1, 2\}$. We obtain an expansion of $\alpha$ of the form (3) by applying $T_{\epsilon_n} \circ \cdots \circ T_{\epsilon_1}$ ($n \in \mathbb{Z}_{>0}$) to $\alpha$. Let us define a sequence $\{\alpha_n\}_{n\geq 0}$ by

$$\alpha_0 := \alpha \quad \text{and} \quad \alpha_n := T_{\epsilon_n} \circ \cdots \circ T_{\epsilon_1}(\alpha_0) \quad (n \geq 1) .$$

Assuming that $|\alpha_n|_p = |\alpha_n^\sigma|_p$ for all $n \in \mathbb{Z}_{\geq 0}$, it is not difficult to see that the expansion of $\alpha$ is identical with that of $\alpha^\sigma$ obtained by applying $T_{\epsilon_n} \circ \cdots \circ T_{\epsilon_1}$ ($n \in \mathbb{Z}_{>0}$) to $\alpha^\sigma$. Then, by Theorem 3.5 (ii), we get $\alpha = \alpha^\sigma$, which is a contradiction. This proves that there exists

$n \in \mathbb{Z}_{>0}$ such that $|\alpha_n|_p \neq |\alpha_n^\sigma|_p$. Therefore, Case 3 reduces to Case 1 or Case 2 after sufficient iterations of $T_1$ and $T_2$.

Consequently, in all the cases, $\alpha$ is mapped to a quadratic Hensel root under some iterate of $T_1$ and $T_2$, regardless of the order in which they are applied. Hence, by Theorems 6.1, 6.3, and 6.5, we have the following theorem.

THEOREM 7.1. *The expansion of every quadratic element of* $\mathbb{Q}_p$ *over* $\mathbb{Q}$ *obtained by each of Algorithms A, B, and C is eventually periodic.*

REMARK 7.2. In contrast to $T_2$ (i.e., Algorithm A), $T_1$ gives a nonperiodic expansion for every quadratic element of $\mathbb{Q}_p$. In fact, every quadratic element is mapped to a quadratic Hensel root by iterating $T_1$ as we have seen above, but it is clear by (7) that no quadratic Hensel root is a periodic point of $T_1$.

We now turn to the characterization of elements with purely periodic expansions for each algorithm. Note that elements with purely periodic expansions are necessarily in $p\mathbb{Z}_p$.

Except for quadratic Hensel roots, there exists no quadratic element of $p\mathbb{Z}_p$ whose expansion by our algorithms is purely periodic. This is because every quadratic element of $p\mathbb{Z}_p$ is mapped to a quadratic Hensel root under some iterate of $T_1$ and $T_2$.

By Theorem 9.1, which will be shown in Section 9, we also see that there exists no rational number whose expansion is periodic.

Consequently, for each algorithm, the set of elements having purely periodic expansions, i.e., the reduced set, is identical with the set of purely periodic points within the set $S$ of quadratic Hensel roots. Hence, by Theorem 6.1, Corollary 6.4, and Lemma 6.7, we have the following theorem.

THEOREM 7.3. *The reduced sets for Algorithms A, B, and C are given by* $S$, $R$, *and* $P_1 \cup R_1 \cup S_3 \cup S_4$, *respectively.*

We now give some examples of expansions of quadratic elements of $\mathbb{Q}_p$ obtained by our algorithms. Below, we denote the periodic pattern that first appears in a (purely or eventually) periodic expansion by using four asterisks ($*$) if the period is greater than one. We denote it by using two asterisks if the period is equal to one.

**Example 1:**

Let $p = 2$, and let $\alpha$ be the quadratic Hensel root of $X^2+X+2$. For this $\alpha$, Algorithms A, B, and C give the same expansion:

$$\alpha = \cfrac{\overset{*}{-2}}{\overset{*}{1} + \cfrac{-2}{1 + \cfrac{-2}{\ddots}}}.$$

**Example 2:**

Let $p = 2$, and let $\alpha$ be the quadratic Hensel root of $X^2 - 11X + 6$. Our algorithms give the following expansions for $\alpha$.

The expansion by Algorithm A:

$$\alpha = \cfrac{-\overset{*}{3} \times 2}{\overset{*}{1} + \cfrac{-\overset{*}{9} \times 2}{\overset{*}{1} + \cfrac{-3 \times 2}{1 + \cfrac{-9 \times 2}{1 + \cfrac{-3 \times 2}{\ddots}}}}}.$$

The expansion by Algorithm B:

$$\alpha = \cfrac{3 \times 2}{1 + \cfrac{-2^2}{1 + \cfrac{-3 \times 2^2}{1 + \cfrac{-9 \times 2}{1 + \cfrac{-11 \times 2}{1 + \cfrac{-3 \times 2^3}{1 + \cfrac{3 \overset{*}{\times} 2^3}{\overset{*}{1} + \cfrac{3 \times 2^3}{\ddots}}}}}}}}.$$

The expansion by Algorithm C:

$$\alpha = \cfrac{3\times 2}{1+\cfrac{\overset{*}{-2^2}}{\overset{*}{1}+\cfrac{-3\times 2^2}{1+\cfrac{-9\times 2}{1+\cfrac{-11\times 2}{1+\cfrac{-3\times 2^3}{1+\cfrac{-3\times 2^3}{1+\cfrac{-11\times 2}{1+\cfrac{-9\times 2}{1+\cfrac{-3\times 2^2}{1+\cfrac{-2^2}{1+\cfrac{\overset{*}{-3\times 2}}{\overset{*}{1}+\cfrac{-2^2}{1+\cfrac{-3\times 2^2}{\ddots}}}}}}}}}}}}}.$$

**Example 3:**

Let $p=3$, and let $\alpha$ be the quadratic Hensel root of $X^2-11X+6$.
The expansion by Algorithm A:

$$\alpha = \cfrac{\overset{*}{-2\times 3}}{\overset{*}{1}+\cfrac{\overset{*}{-2\times 3^2}}{\overset{*}{1}+\cfrac{-2\times 3}{1+\cfrac{-2\times 3^2}{1+\cfrac{-2\times 3}{\ddots}}}}}.$$

The expansion by Algorithm B:

$$\alpha = \cfrac{2\times 3}{2+\cfrac{-4\times 3}{1+\cfrac{-2\times 3^2}{2+\cfrac{-8\times 3}{1+\cfrac{\overset{*}{8\times 3}}{\overset{*}{1}+\cfrac{8\times 3}{\ddots}}}}}}.$$

The expansion by Algorithm C:

$$\alpha = \cfrac{2 \times 3}{2 + \cfrac{-\overset{*}{4} \times 3}{\overset{*}{1} + \cfrac{-2 \times 3^2}{2 + \cfrac{-8 \times 3}{1 + \cfrac{-8 \times 3}{2 + \cfrac{-2 \times 3^2}{1 + \cfrac{-4 \times 3}{2 + \cfrac{-\overset{*}{2} \times 3}{\overset{*}{2} + \cfrac{-4 \times 3}{1 + \cfrac{-2 \times 3^2}{\ddots}}}}}}}}}}.$$

**Example 4:**

Let $p = 3$, and let $\alpha$ be the root of $3X^2 - 5X + 1$ whose 3-adic absolute value $|\alpha|_3$ is equal to 3.

The expansion by Algorithm A:

$$\alpha = \cfrac{-3^{-1}}{1 + \cfrac{-3^2}{2 + \cfrac{-\overset{*}{3}^2}{\overset{*}{2} + \cfrac{-\overset{*}{3}^3}{\overset{*}{2} + \cfrac{-3^2}{2 + \cfrac{-3^3}{\ddots}}}}}}.$$

The expansion by Algorithm B:

$$\alpha = \cfrac{3^{-1}}{2 + \cfrac{-3}{1 + \cfrac{3}{2 + \cfrac{-3}{1 + \cfrac{\overset{*}{3}}{\overset{*}{1} + \cfrac{3}{1 + \cfrac{3}{\ddots}}}}}}}.$$

The expansion by Algorithm C:

$$\alpha = \cfrac{3^{-1}}{2 + \cfrac{-\,3}{1 + \cfrac{3}{2 + \cfrac{\overset{*}{-3}}{\overset{*}{1} + \cfrac{-\,3}{2 + \cfrac{\overset{*}{-3}}{\overset{*}{2} + \cfrac{-\,3}{1 + \cfrac{-\,3}{\ddots}}}}}}}}\,.$$

REMARK 7.4. There is a known, straightforward method for forming a continued fraction for a root of $X^2 + bX + c$, namely to iterate $X = -b - c/X$. Such a continued fraction converges if $|b|_p^2 > |c|_p$. However, this trivial method cannot give an expansion for every quadratic element of $\mathbb{Q}_p$. In addition, the partial denominators of the expansion are equal to $-b$ which is not usually in $\{1, \ldots, p-1\}$, or more precisely, which can take an arbitrarily large value. This method is quite different from our algorithms that realize the continued fraction expansion by the iterative application of properly selected linear fractional maps.

## 8. Expansions of rational Hensel roots

$\alpha = 0$ is the root of $X \in \mathbb{Z}[X]$ and thus is a rational Hensel root. As described in Section 2, we do not expand $\alpha = 0$ any further.

Let us consider expansions of rational Hensel roots other than 0, i.e., those of roots of $X + c \in \mathbb{Z}[X]$ with $c \in p\mathbb{Z} \setminus \{0\}$. Recall the definitions of our algorithms in Section 5. Since the coefficient $b$ of $X$ of the minimal polynomial in $\mathbb{Z}[X]$ satisfies $b = 1$ for every rational Hensel root, we can classify our algorithms into two classes:

Class I: Algorithms which apply $T_2$ to every rational Hensel root other than 0 (Algorithms A and B)

Class II: Algorithms which apply $T_2$ to a rational Hensel root if the coefficient $c$ of its minimal polynomial satisfies $c > 0$ and which apply $T_1$ if $c < 0$ (Algorithm C)

In the following, we show that whichever class an algorithm belongs to, it gives a finite expansion for every rational Hensel root other than 0.

Class I:

Let $\alpha$ be an arbitrary rational Hensel root other than 0. Applying $T_2$ to $\alpha$, we have

$$T_2(\alpha) = \frac{-u(\alpha)}{\alpha|\alpha|_p} - d_2(\alpha)\,.$$

Let $X+c \in \mathbb{Z}[X]$ be the minimal polynomial of $\alpha$. Since $\alpha = -c$, we see that $|\alpha|_p = |c|_p$. Since

$$\frac{-u(\alpha)}{\alpha|\alpha|_p} = 1\,,$$

we have $d_2(\alpha) = 1$, which implies

$$T_2(\alpha) = \frac{-c}{\alpha} - 1 = 0\,.$$

Therefore, $\alpha$ is expanded into the finite continued fraction

$$\alpha = \frac{-c}{1}$$

by each of the algorithms belonging to Class I.

Class II:

Let $\alpha$ be an arbitrary rational Hensel root other than 0, and let $X + c \in \mathbb{Z}[X]$ be the minimal polynomial of $\alpha$.

If $c > 0$, we apply $T_2$ to $\alpha$. Hence, $\alpha$ is expanded as

$$\alpha = \frac{-c}{1}$$

(cf. Class I).

Let us consider the case where $c < 0$. In this case, we apply $T_1$ to $\alpha$. Since

$$\frac{u(\alpha)}{\alpha|\alpha|_p} = -1\,,$$

we see that $d_1(\alpha) = p - 1$, which implies

$$T_1(\alpha) = \frac{c}{\alpha} - (p-1) = -p\,. \tag{12}$$

Note that $T_1(\alpha) = -p$ is also a rational Hensel root whose minimal polynomial is $X + p \in \mathbb{Z}[X]$. Since the constant term $p$ of $X + p$ is positive, $-p$ is expanded as

$$-p = \frac{-p}{1} \tag{13}$$

by using $T_2$. By (12) and (13), we see that $\alpha$ is expanded as

$$\alpha = \cfrac{c}{p - 1 + \cfrac{-\,p}{1}}$$

when $c < 0$.

Therefore, the algorithm belonging to Class II also gives a finite continued fraction for $\alpha$.

As a consequence, we get the following theorem.

THEOREM 8.1. *Each of Algorithms A, B, and C gives a finite expansion for every rational Hensel root.*

## 9. Expansions of rational numbers

In this section, we will show that each of the three algorithms gives a finite expansion for every rational number.

Let $\alpha$ be an arbitrary rational number. If $\alpha$ is a rational Hensel root, our algorithms give a finite expansion for $\alpha$ (cf. Theorem 8.1).

Let us consider the case where $\alpha$ is not a rational Hensel root. Let $bX + c \in \mathbb{Z}[X]$ be the minimal polynomial of $\alpha$. Obviously, $\alpha = -c/b$. We easily see that

$$\frac{u(\alpha)}{\alpha|\alpha|_p} = -b|b|_p \in \mathbb{Z} \setminus p\mathbb{Z},$$

which implies that $T_1(\alpha) = \left\langle -b|b|_p \right\rangle_p$ and $T_2(\alpha) = \left\langle b|b|_p \right\rangle_p$ are in $p\mathbb{Z}$, i.e., they are rational Hensel roots. Therefore, the expansion of $\alpha$ obtained by each of our algorithms is finite also in the case where $\alpha$ is not a rational Hensel root.

Summarizing the discussion above, we have the following theorem.

THEOREM 9.1. *Each of Algorithms A, B, and C gives a finite expansion for every rational number.*

## 10. Concluding remarks

It is worth making some remarks on the generality of our results.

1. We have dealt with continued fractions of the form (1), but we can also consider another basic type, namely continued fractions of the form

$$d_0 + \cfrac{t_1 p^{k_1}}{d_1 + \cfrac{t_2 p^{k_2}}{d_2 + \cfrac{t_3 p^{k_3}}{\ddots}}} \qquad \bigl(k_n \in \mathbb{Z}_{>0},\ t_n \in \mathbb{Z} \setminus p\mathbb{Z},\ d_n \in \{1, \dots, p-1\}\ (n \geq 1)\bigr) \tag{14}$$

   with $d_0 \in \mathbb{Q}_p$ such that $d_0 = [d_0]_p$. The convergence of continued fractions (14) is also guaranteed by Theorem 3.5. By applying our algorithms to the $p$-adic fractional part $\langle\alpha\rangle_p$ of $\alpha \in A_p$, we can generate continued fractions of the form (14). Even with this modification, all the theorems in this paper still hold.
2. We have focused on the expansion of the elements of $A_p$, but it is easy to extend our algorithms to cover all the elements of $\mathbb{Q}_p$. One of the simplest ways to do this is to expand every element of $\mathbb{Q}_p \setminus A_p$ by using the map $T$ such that $t$ and $d$ in (2) satisfy $t(x) = 1$ for all $x \in \mathbb{Q}_p \setminus A_p$ and $\mathrm{Im}(d) \subset \{1, \dots, p-1\}$. The convergence of resulting continued fractions is guaranteed, as we have seen in Section 3. Note that even with this extension, a given element of $\mathbb{Q}_p \setminus A_p$ has neither a periodic nor finite expansion since $\mathrm{Im}(t)$ and $\mathrm{Im}(d)$ are included in $\mathbb{Q}$.

Algorithms other than those presented here, as well as the extension of our approach to multidimensional $p$-adic continued fractions, will be reported in forthcoming papers.

**Acknowledgments.** This research was supported by JSPS KAKENHI Grant Numbers JP15K00342 and JP16KK0005.

## References

[ 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 ] P. Bundschuh, $p$-adische Kettenbrüche und Irrationalität $p$-adischer Zahlen, Elem. Math. 32 (1977) 36–40.

[ 4 ] M. Furukado, S. Ito, A. Saito, J.-I. Tamura, S. Yasutomi, A new multidimensional slow continued fraction algorithm and stepped surface, Experimental Math. 23 (2014) 390–410.

[ 5 ] É. Galois, Démonstration d'un théorème sur les fractions continues périodiques, Annales de mathématiques pures et appliquées 19 (1828/29) 294–301.

[ 6 ] N. Koblitz, $p$-adic Numbers, $p$-adic Analysis, and Zeta-Functions, 2nd ed., Springer, New York, 1984.

[ 7 ] J.-L. Lagrange, Additions au mémoire sur la résolution des équations numériques, Mém. Berl. 24 (1770). Reprinted in: Œuvres de Lagrange 2, Gauthier-Villars, Paris, 1868, pp. 581–652.

[ 8 ] T. Ooto, Transcendental $p$-adic continued fractions, Math. Z. 287 (2017) 1053–1064.

[ 9 ] O. Perron, Die Lehre von den Kettenbrüchen, Teubner, Leipzig, 1913.

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

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

[12] 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.

[13] J.-I. Tamura, S. Yasutomi, A new multidimensional continued fraction algorithm, Math. Comp. 78 (2009) 2209–2222.

[14] J.-I. Tamura, S. Yasutomi, Algebraic Jacobi-Perron algorithm for biquadratic numbers, in: Diophantine Analysis and Related Fields 2010, AIP Conf. Proc. 1264 (2010) 139–149.

[15] J.-I. Tamura, S. Yasutomi, A new algorithm of continued fractions related to real algebraic number fields of degree $\leq 5$, Integers 11B (2011) A16.

[16] J.-I. Tamura, S. Yasutomi, Some aspects of multidimensional continued fraction algorithms, in: Functions in Number Theory and Their Probabilistic Aspects, RIMS Kôkyûroku Bessatsu B34 (2012) 463–475.

[17] B. M. M. de Weger, Periodicity of $p$-adic continued fractions, Elem. Math. 43 (1988) 112–116.

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

Asaki SAITO
Department of Complex and Intelligent Systems
Future University Hakodate
116–2 Kamedanakano-cho, Hakodate
Hokkaido 041–8655, Japan
e-mail: saito@fun.ac.jp

Jun-ichi TAMURA
Institute for Mathematics and Computer Science
Tsuda College
2–1–1 Tsuda-machi, Kodaira
Tokyo 187–8577, Japan
e-mail: jtamura@tsuda.ac.jp

Shin-ichi YASUTOMI
Faculty of Science, Toho University
2–2–1 Miyama, Funabashi
Chiba 274–8510, Japan
e-mail: shinichi.yasutomi@sci.toho-u.ac.jp