On \( p \)-adic Continued Fractions and Quadratic Irrationals

by

Justin Miller

Copyright © Justin Miller 2007

A Dissertation Submitted to the Faculty of the

DEPARTMENT OF MATHEMATICS

In Partial Fulfillment of the Requirements
For the Degree of

DOCTOR OF PHILOSOPHY

In the Graduate College

THE UNIVERSITY OF ARIZONA

2007
THE UNIVERSITY OF ARIZONA
GRADUATE COLLEGE

As members of the Dissertation Committee, we certify that we have read the dissertation
prepared by Justin Thomson Miller
entitled On $p$-adic Continued Fractions and Quadratic Irrationals
and recommend that it be accepted as fulfilling the dissertation requirement for the
Degree of Doctor of Philosophy

__________________________________________ Date: (November 15, 2007)
(Dinesh Thakur)

__________________________________________ Date: (November 15, 2007)
(Daniel Madden)

__________________________________________ Date: (November 15, 2007)
(Klaus Lux)

Final approval and acceptance of this dissertation is contingent upon the candidate’s
submission of the final copies of the dissertation to the Graduate College.

I hereby certify that I have read this dissertation prepared under my direction and
recommend that it be accepted as fulfilling the dissertation requirement.

__________________________________________ Date: (November 15, 2007)
Dissertation Director: (Dinesh Thakur)
STATEMENT BY AUTHOR

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at The University of Arizona and is deposited in the University Library to be made available to borrowers under rules of the Library.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgment of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the copyright holder.

Signed: _______________ Justin T Miller
Acknowledgements

First, I would like to thank God for His lovingkindness, enduring patience, and for giving me a love for mathematics. Also, I would like to thank my wife for her patience and encouragement. Despite many delays in finishing this research, she patiently supported me in this endeavor.

Thanks go to Dr. Thakur for taking me on as his student, especially given my non-traditional role, working full-time in industry instead of studying full-time as a student. I appreciate his patience and understanding as this research took longer than expected. Also, I am grateful to him for directing me to this interesting dissertation topic, and for teaching me how be a better writer and researcher along the way.

Dr. Madden has been an excellent mentor to me as an undergraduate, and during the first few years as a graduate student. I appreciate the perspective he as given me on the study of mathematics. Also, I am thankful for his willingness to serve on my comprehensive examination committee and on my dissertation committee. Likewise, I appreciate the time and work Dr. Lux has spent being a member of both of these committees.

I would like to thank my mom and dad for all their love and support throughout the years. Although it took a number of years for it to sink in, they engendered in me a love for reading and learning, which helped me to discover my inclination towards mathematics.

Many thanks go to my employer, IBM, for supporting my pursuit of this degree, and for paying for many semesters of tuition. Especially, I would like to thank Bill Bostic, Roberta Lockaby, and George Wang for their support and for the accommodations they have made so that I could finish this degree.
DEDICATION

This paper is dedicated to my wife, Frances, for her loving patience and support.
# Table of Contents

List of Figures ......................................................... 8
List of Tables .......................................................... 9
Abstract ......................................................................... 10

Chapter 1. Introduction .................................................. 11
  1.1. Real Continued Fractions ....................................... 14
  1.2. $p$-adic Continued Fractions ................................. 17
      1.2.1. Schneider Continued Fractions ....................... 19
      1.2.2. Ruban Continued Fractions ......................... 21
      1.2.3. Browkin’s Results .................................. 22
  1.3. Approximation Lattices ...................................... 25
  1.4. Overview and Conventions ................................... 33

Chapter 2. General Definitions for $p$-adic Continued Fractions 35
  2.1. Integral Type Continued Fractions ......................... 37
      2.1.1. Continued Fractions from Approximation Lattices .. 39
      2.1.2. The $\ell$-Square Algorithm ....................... 48
  2.2. Simple Rational Type Continued Fractions ................ 51
  2.3. Numerical Results on Browkin’s Algorithms .............. 54
      2.3.1. Definitions of Browkin’s Continued Fraction Algorithms ... 55
      2.3.2. Analysis and Extension of Browkin’s Numerical Results .... 57
      2.3.3. Periodicity Results for Browkin’s Second Quadratic Algorithm 59

Chapter 3. Schneider Type Continued Fractions .................. 60
  3.1. Finiteness of Continued Fractions for Rational Numbers .. 62
  3.2. Periodicity Proof for Quadratic Irrationals .............. 65
  3.3. Numerical Results and Observations ..................... 72
      3.3.1. Periodicity in $\mathbb{Q}_p$ for $p > 3$ .............. 73
      3.3.2. Empirical Bounds on Remainders .................. 75
      3.3.3. Examples of a non-palindromic symmetry .......... 78

Chapter 4. Continued Fractions in $\mathbb{F}_q((t))$ ............... 79
  4.1. Continued Fractions in Non-archimedean Local Fields .... 79
  4.2. Rationals and Quadratic Irrationals in $\mathbb{F}_q((t))$ ..... 82
**Table of Contents—Continued**

**Appendix A. PARI/GP Code** .................................................. 92
   A.1. Integral Continued Fraction Code .................................. 92
   A.2. Browkin’s Algorithms ................................................. 94
   A.3. Code for Calculations in $\mathbb{F}_p((t))$ ..................... 101
   A.4. Other Code ............................................................ 103

**References** .......................................................................... 105
LIST OF FIGURES

FIGURE 3.1. Values of $D$ for which $\sqrt{D}$ has a periodic SCF . . . . . . . . . . 61
FIGURE 3.2. Maximum values of $|P_n|$ in the NQCF for $\sqrt{D}$ . . . . . . . . . . 76
FIGURE 3.3. Maximum values of $|P_n|$ in the NQCF for $\sqrt{D}$ . . . . . . . . . . 77
LIST OF TABLES

Table 2.1. Calculating the continued fraction for $\sqrt{499} \in \mathbb{Q}_3$ . . . . . . . . . . 47

Table 3.1. $D$ with $|D| \leq 100$, $\sqrt{D} \in \mathbb{Q}_p$, and no period in the NQCF of $\sqrt{D}$ after 2,000 terms . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 74

Table 3.2. Percentage of square roots whose NQCF have negative symmetry 78
ABSTRACT

In this dissertation we investigate prior definitions for $p$-adic continued fractions and introduce some new definitions. We introduce a continued fraction algorithm for quadratic irrationals, prove periodicity for $\mathbb{Q}_2$ and $\mathbb{Q}_3$, and numerically observe periodicity for $\mathbb{Q}_p$ when $p < 37$. Various observations and calculations regarding this algorithm are discussed, including a new type of symmetry observed in many of these periods, which is different from the palindromic symmetry observed for real continued fractions and some previously defined $p$-adic continued fractions.

Other results are proved for $p$-adic continued fractions of various forms. Sufficient criteria are given for a class of $p$-adic continued fractions of rational numbers to be finite. An algorithm is given which results in a periodic continued fraction of period length one for $\sqrt{D} \in \mathbb{Z}_p^\times$, $D \in \mathbb{Z}$, $D$ non-square; although, different $D$ require different parameters to be used in the algorithm. And, a connection is made between continued fractions and de Weger’s approximation lattices, so that periodic continued fractions can be generated from a periodic sequence of approximation lattices, for square roots in $\mathbb{Z}_p^\times$.

For simple $p$-adic continued fractions with rational coefficients, we discuss observations and calculations related to Browkin’s continued fraction algorithms.

In the last chapter, we apply some of the definitions and techniques developed in the earlier chapters for $\mathbb{Q}_p$ and $\mathbb{Z}$ to the $t$-adic function field case $\mathbb{F}_q((t))$ and $\mathbb{F}_q[t]$, respectively. We introduce a continued fraction algorithm for quadratic irrationals in $\mathbb{F}_q((t))$ that always produces periodic continued fractions.
Chapter 1

Introduction

A continued fraction is an expression of the form

\[ a_0 + \frac{b_0}{a_1 + \frac{b_1}{a_2 + \cdots + \frac{b_{n-1}}{a_n}}} \]

(1.1)
called a finite continued fraction, or of the form

\[ a_0 + \frac{b_0}{a_1 + \frac{b_1}{a_2 + \cdots}} \]

(1.2)
called an infinite continued fraction. The terms \( a_i, b_i, i = 0, 1, 2, \ldots \) are numbers from a field, but are usually restricted to a subset, such as \( \mathbb{Z} \) when the field is \( \mathbb{R} \) or \( \mathbb{Q}_p \), for some prime \( p \). The terms \( a_0, a_1, a_2, \ldots \) are called partial denominators in general, and are called partial quotients when \( b_i = 1 \) for all \( i \). Likewise, the terms \( b_0, b_1, b_2, \ldots \) are called partial numerators. When all partial numerators are equal to 1, the continued fraction is called simple, with the stipulation that \( a_i > 0 \) for \( i > 0 \) when the real numbers are in consideration. The partial numerators usually begin with \( b_1 \), however, we start with \( b_0 \).

The standard notation for a simple continued fraction is \([a_0, a_1, \ldots, a_n]\) in the finite case, and \([a_0, a_1, a_2, \ldots]\) in the infinite case. If the partial quotients become periodic after some point, then a bar is placed over the repeating partial quotients, as in \([a_0, \ldots, a_n, \overline{a_{n+1}, \ldots, a_{n+k}}]\). For continued fractions that are not simple, we use the notation

\[
\begin{bmatrix}
  b_0 & b_1 & \cdots & b_{n-1} \\
  a_0 & a_1 & \cdots & a_n
\end{bmatrix}
\]
in the finite case, and

\[
\begin{bmatrix}
  b_0 & b_1 & \cdots \\
  a_0 & a_1 & a_2 & \cdots
\end{bmatrix}
\]
in the infinite case. The same notation holds for general eventually periodic continued fractions as it does for eventually periodic simple continued fractions.

When a continued fraction is truncated and simplified it yields a fraction, as long as division by zero does not occur during the simplification, which is called a convergent. For example,

\[ C_i = \left[ \begin{array}{c} b_0 & \cdots & b_{i-1} \\ a_0 & a_1 & \cdots & a_i \end{array} \right]. \]

is the \( i \)th convergent. Usually the partial numerators and denominators are integral or rational, in which case convergents are rational. Finite continued fractions are always equal to a number in the field, as long as there is no division by zero, but for infinite continued fractions, the idea of representing a number needs to be defined. Convergents are meant to be approximations (usually rational) to a number (usually irrational). Thus, we say that an infinite continued fraction converges to a number, \( \alpha \), or is equal to \( \alpha \) if the sequences of convergents converges to \( \alpha \) with respect to some absolute value on the field under consideration.

Related to convergents are the sequences \((A_n)_{n \geq 0}\) and \((B_n)_{n \geq 0}\), defined recursively by

\[
A_{n+1} = a_{n+1}A_n + b_nA_{n-1}
\]
\[
B_{n+1} = a_{n+1}B_n + b_nB_{n-1},
\]

for \( n \geq 0 \), where \( A_0 = a_0 \), \( B_0 = 1 \), \( A_{-1} = 1 \), and \( B_{-1} = 0 \). The quotient \( A_n/B_n \) is equal to the \( n \)th convergent, which is easily proved by induction.

Given a continued fraction, another continued fraction, called the \( i \)th remainder, can be defined by starting with the \( i \)th partial denominator. That is, if \( \alpha \in F \) (some field) is represented by the continued fraction (1.1) or (1.2), then the \( i \)th remainder, \( \alpha_i \) is

\[
\alpha_i = \left[ \begin{array}{c} b_i & b_{i+1} & \cdots \\ a_i & a_{i+1} & a_{i+2} & \cdots \end{array} \right],
\]
which terminates based on the finiteness of $\alpha$. In particular, $\alpha = \alpha_0$. It is easily seen that if $\alpha$ has a continued fraction representation that converges to it, then all of the partial remainders converge as well.

Many useful relationships exist between all the terms defined above. Some of the ones we will occasionally use are the following, which are all easily proved by induction.

**Proposition 1.** Suppose $\alpha \in F$ has a continued fraction representation as in (1.1) or (1.2). The following are true:

- $A_n/B_n$ is the $n$th convergent
- if $\alpha_{n+1}$ is defined and $\alpha_n \neq a_n$

$$\frac{\alpha_{n+1}}{\alpha_n - a_n} = \frac{b_n}{\alpha_n - a_n}$$

- if $\alpha_{n+1}$ is defined

$$\alpha = \frac{\alpha_{n+1}A_n + b_nA_{n-1}}{\alpha_{n+1}B_n + b_nB_{n-1}}$$

Let $\{b_{i-1}/a_i\}$, for $i \geq 0$ where $b_{-1} = 1$, denote the matrix

$$\begin{pmatrix} b_{i-1} & 1 \\ a_i & b_i \end{pmatrix}$$

Then it is easy to see that

$$\{b_{-1}/a_0\}{b_0/a_1}\cdots{b_{i-1}/a_i} = \begin{pmatrix} B_{i-1} & B_i \\ A_{i-1} & A_i \end{pmatrix}$$

(1.3)

and

$$A_iB_{i-1} - A_{i-1}B_i = (-1)^{i-1}b_0 \cdots b_{i-1}$$

(1.4)

for $i \geq 0$.

An old, but not too familiar, theorem of Daniel Bernoulli allows one to generate a continued fraction from a sequence of rational approximations to it.
Theorem 1 (D. Bernoulli). Suppose \((A_n)_{n \geq 0}\) and \((B_n)_{n \geq 0}\) are sequences of numbers in some field for which \(B_0 = 1\) and \(A_n/B_n \neq A_{n+1}/B_{n+1}\) for all \(n \geq 0\). Then \(A_n/B_n\) are the convergents for the continued fraction

\[
a_0 + \frac{b_0}{a_1 + \frac{b_1}{a_2 + \cdots}},
\]

where \(a_0 = A_0, b_0 = A_1B_0 - A_0B_1, a_1 = B_1\) and

\[
a_{n+1} = \frac{A_{n+1}B_{n-1} - A_{n-1}B_{n+1}}{A_nB_{n-1} - A_{n-1}B_n},
\]

\[
b_n = \frac{A_nB_{n+1} - A_{n+1}B_n}{A_nB_{n-1} - A_{n-1}B_n},
\]

for \(n \geq 1\).

The proof is straightforward, using the properties above. The condition that \(A_n/B_n \neq A_{n+1}/B_{n+1}\) for all \(n \geq 0\) ensures that the partial numerators and denominators are defined and that no partial numerator is zero, which would terminate the continued fraction. The rational sequence \(A_n/B_n\) needs to converge, in whatever valued field is under consideration, in order for the resulting continued fraction to be more than just formal.

These general properties of continued fractions will suffice for our analysis. Further results will be restricted to a given valued field. General information about continued fractions can be found in [Khi97] and [JT80].

1.1 Real Continued Fractions

The most commonly studied continued fractions of real numbers are the simple continued fractions, where all partial denominators after the first are positive integers, and the first partial quotient will have the same sign as the number it represents. If \(\alpha \in \mathbb{R}\), then its continued fraction is generated by \(a_n = \lfloor \alpha_n \rfloor\), using the notation from the last section. This simple construction leads to the “best” rational approximations
to real numbers, and produces an eventually periodic expansion for irrational roots of quadratic polynomials in $\mathbb{Q}[x]$. In fact, the use of continued fractions began with finding approximations to square roots [JT80].

A *quadratic irrational* is the common term for an irrational root of a quadratic polynomial in $\mathbb{Q}[x]$. As such, a quadratic irrational in $\mathbb{R}$ is

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

for integers $P$, $Q$, and $D$, where $D$ is positive and non-square. If the root is taken to be real, rather than complex or $p$-adic, the quadratic is referred to as a *real quadratic irrational*. We usually omit the valued field containing the quadratic irrational, as it is usually clear from context. For other fields, the positive condition on $D$ is replaced by a necessary and sufficient condition for $D$ to have a square root in the field. If (1.2) is a continued fraction for the quadratic irrational $\alpha$, then each remainder, $\alpha_n$, is a quadratic irrational, which we denote by

$$\alpha_n = \frac{P_n + \sqrt{D}}{Q_n}. \quad (1.5)$$

The numbers $P_n$ and $Q_n$ satisfy the recurrence relations

$$P_{n+1} = a_nQ_n - P_n \quad (1.6)$$
$$Q_{n+1} = \frac{D - P_n^2}{b_nQ_n}. \quad (1.7)$$

For simple continued fractions, $P_n$ and $Q_n$ are integers, and it can be shown that they are bounded, so that the continued fraction for a quadratic irrational must eventually be periodic. This, along with the more straightforward converse, are a theorem of Lagrange.

**Theorem 2** (Lagrange). A simple continued fraction for a real number is eventually periodic if and only if the number is a quadratic irrational.
For brevity, we use the term periodic to mean eventually periodic, and the term purely periodic to mean periodic, where the periodic part starts with the first partial quotient. Finding analogues to Lagrange’s Theorem for the $p$-adics is one of the most studied aspects of $p$-adic continued fractions. Generally, it is easy to show that a periodic continued fraction is rational or a quadratic irrational, but no natural algorithm has been found that always produces periodic continued fractions for quadratic irrationals. Two other theorems on the structure of continued fractions for quadratic irrationals, for which $p$-adic analogues are desirable, are the following.

**Theorem 3.** Let $D \in \mathbb{Z}$ be positive and non-square. Then $\sqrt{D}$ has the continued fraction expansion

$$\sqrt{D} = [a_0, a_1, \ldots, a_n, 2a_0],$$

where $a_{i+1} = a_{n-i}$ for $0 \leq i < n$.

**Theorem 4.** A quadratic irrational, $\alpha$, is purely periodic precisely when $\alpha > 1$ and $-1 < \bar{\alpha} < 0$, where $\bar{\alpha}$ is the conjugate of $\alpha$.

The most important aspect of real continued fractions is their ability to provide good rational approximations to irrational numbers. If $\alpha \in \mathbb{R}$ and $A_n/B_n$ is a convergent from the simple continued fraction for $\alpha$, then $A_n/B_n$ is a best approximation to $\alpha$ in the following sense: if $|\alpha - p/q| < |\alpha - A_n/B_n|$, then $|q| > |B_n|$. Using continued fractions, it is possible to prove the following theorem of Hurwitz.

**Theorem 5 (Hurwitz).** Let $\alpha \in \mathbb{R}$ be an irrational number. Then there are infinitely many rational numbers, $p/q$, such that the inequality

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{\sqrt{5}q^2}$$

holds.

Although continued fractions are not necessary to prove Hurwitz’s Theorem—Farey fractions can be used instead, for example—using continued fractions provides
an easy way to compute rational numbers satisfying the inequality, as at least one of any three consecutive convergents for $\alpha$ satisfies the inequality [NZM91]. The factor $\sqrt{5}$ is also the best, since for any larger factor, there is an irrational number for which the inequality holds for only finitely many rational numbers. Some work has been done in finding analogues to Hurwitz’s Theorem in the $p$-adic case, using $p$-adic continued fractions or something similar [dW86]. Another theorem for which it would be interesting to have a $p$-adic analogue is the following.

**Theorem 6.** If $\alpha \in \mathbb{R}$ is irrational and $p/q$ is a rational number satisfying $q \geq 1$ and

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{2q^2},$$

then $p/q$ is a convergent of the simple continued fraction for $\alpha$.

Proofs for the theorems contained in this section can be found in many elementary number theory texts [NZM91].

### 1.2 $p$-adic Continued Fractions

Real continued fractions provide best rational approximations for real numbers, and have a nice structure for quadratic irrationals, which gives them a finite representation and provides a way to find the fundamental units in the quadratic fields they produce. For $p$-adic numbers, it is also desirable to construct continued fractions so that analogues of the theorems of Lagrange and Hurwitz hold.

The $p$-adic notation we use throughout is the following, where $p$ is a prime. The field of $p$-adic numbers, ring of $p$-adic integers, and group of $p$-adic units are denoted by $\mathbb{Q}_p$, $\mathbb{Z}_p$, and $\mathbb{Z}_p^\times$, respectively. If $a/b \in \mathbb{Q}^*$, $a, b, a', b' \in \mathbb{Z}$, $(a, b) = 1$, $a = p^e a'$, $b = p^f b'$, and $(a', p) = (b', p) = 1$, then the $p$-adic valuation $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ is given by $v_p(a/b) = e - f$ and $v_p(0) = +\infty$. When $p$ is clear from context, we use $v$ instead of $v_p$. The corresponding $p$-adic absolute value is defined and denoted by

$$|a|_p = p^{-v_p(a)},$$
where $\alpha \in \mathbb{Q}^\times$ and $|0|_p = 0$. Of course, the same relationship holds when the $p$-adic valuation and $p$-adic absolute value are extended to $\mathbb{Q}_p$.

For real numbers, the method for constructing continued fractions is clear, since for any real number, $\alpha$, there is only one integer, $a$, such that $0 \leq \alpha - a < 1$. In the $p$-adic case, if $\alpha \in \mathbb{Q}_p$, there are infinitely many integers $\alpha \in \mathbb{Z}$ such that $0 \leq |\alpha - a|_p < 1$, and no obvious way for choosing $a$ so that analogues of theorems about real continued fractions will hold. There are, however, at least two methods for choosing $a$ that seem to be the most simple. First, any integers that satisfy $0 \leq |\alpha - a|_p < 1$ are congruent modulo $p$, so why not choose $a$ to be in $\{0, \ldots, p-1\}$, and similarly for the other partial quotients? This was the approach taken by Schneider [Sch70]. The partial numerators are taken to be powers of $p$ equal in absolute value to $|\alpha_n - a_n|_p$, so that remainders are $p$-adic units. Hence, Schneider’s continued fraction are not simple. In order for the continued fraction to be simple, one can take $a_n$ to be a rational number $a'_n/p^{e_n}$, where $a'_n \in \{0, \ldots, p-1\}$ and $e_n = v_p(\alpha_n - a'_n)$. This was the approach taken by Ruban [Rub70].

Most studies of $p$-adic continued fractions look at properties of Schneider or Ruban continued fractions, or continued fractions that are defined using slight variations of Schneider’s or Ruban’s definitions. Browkin [Bro01] has done much work related to defining Ruban-like continued fractions that result in periodic expansions for many quadratic irrationals. However, despite much empirical evidence suggesting properties held by Browkin’s continued fractions, most have not been proved, and no analogue of Lagrange’s Theorem or Hurwitz’s Theorem has been proved for any $p$. For Schneider continued fractions, Tilborghs [Til90], using some results of de Weger’s [dW88], gives a necessary and sufficient condition for the periodicity of quadratic irrationals, which can be computed in linear time with respect to the size of the discriminant. This condition shows that Schneider continued fractions for quadratic irrationals are rarely periodic.
1.2.1 Schneider Continued Fractions

Schneider [Sch70] seems to be the first person to define a $p$-adic continued fraction algorithm in a natural way. Mahler [Mah40] gave a geometric representation of $p$-adic integers from which continued fractions could be derived in 1940, but it was not natural in the sense that constructing a continued fraction did not proceed simply by choosing partial quotients and constructing remainders iteratively. For a $p$-adic integer $\alpha \in \mathbb{Z}_p$, with representation

$$\alpha = \sum_{n=0}^{\infty} c_n p^n, \quad 0 \leq c_n < p,$$

Schneider defined his continued fraction by requiring that $a_0 = c_0$, $a_n \in \{1, \ldots, p-1\}$, $b_n = p^{e_n}$ for some $e_n$, and $v(\alpha_n) = 0$ for $n > 0$. These requirements can be simplified by using the following definition.

**Definition 1.** A *Schneider continued fraction* (SCF) for a $p$-adic integer $\alpha$ is one constructed in the following way:

1. $\alpha_0 = \alpha$, $\alpha_{n+1} = b_n/(\alpha_n - a_n)$
2. choose the unique $a_n \in \{0, \ldots, p-1\}$ such that $v(\alpha_n - a_n) > 0$
3. $b_n = p^{e_n}$ where $e_n = v(\alpha_n - a_n)$,

for $n \geq 0$, as long as $\alpha_n \neq a_n$. If $\alpha_n = a_n$ then the continued fraction terminates with $a_n$ as its final partial denominator and $b_{n-1}$ as its final partial numerator.

Schneider shows that the convergents generated by $\alpha$ converge to $\alpha$ $p$-adically, so that the continued fraction algorithm has value in approximating and representing $p$-adic integers. With this definition, not all rational numbers have a finite continued fraction representation. Bundschuh [Bun77] characterized which rational numbers have finite SCFs. Bundschuh also produced data on the continued fractions for square roots that suggested not all square roots have periodic SCFs [dW88].
de Weger [dW88] proved that not all square roots in \( \mathbb{Z}_p \) have periodic SCFs, showing that Lagrange’s Theorem does not hold for this type of continued fraction. His results, using the notation above for continued fractions of quadratic irrationals, are contained in the following theorem.

**Theorem 7** (de Weger). Let \( D \in \mathbb{Z} \) be a non-square, quadratic residue mod \( p \), and consider the SCF for \( \alpha = \sqrt{D} \), where
\[
\alpha_n = \frac{P_n + \sqrt{D}}{Q_n}.
\]
If \( P_n \) and \( Q_n \) have different signs, for some \( n \), and \( P_{n+1}^2 > D \), then \( \sqrt{D} \) does not have a periodic continued fraction. In particular, if \( D < 0 \), then \( \sqrt{D} \) has a non-periodic SCF.

Tilborghs [Til90], using the results of de Weger, gave a necessary and sufficient condition for \( \sqrt{D} \) to have a periodic SCF.

**Theorem 8** (Tilborghs). Using the notation of Theorem 7, the following are equivalent:

- The SCF for \( \sqrt{D} \) is periodic.
- \( P_n^2 < D \) for all \( n \geq 0 \).
- \( Q_n > 0 \) for all \( n \geq 0 \).

Tilborghs also obtained some results regarding the structure of periodic continued fractions, similar to Theorem 3.

**Theorem 9** (Tilborghs). Let \( p \) be an odd prime, and suppose the SCF for \( \sqrt{D} \) is periodic. If \( 1 \leq a_0 \leq (p - 1)/2 \) then
\[
\sqrt{D} = \left[ \begin{array}{cccc}
\frac{b_0}{a_0} & \frac{b_1}{a_1} & \cdots & \frac{b_{n-1}}{a_{n-1}} \\
\frac{a_1}{a_2} & \frac{a_2}{a_3} & \cdots & \frac{a_{n-1}}{a_n}
\end{array} \right]
\]
where \( a_i = a_{n-i} \) for \( 1 \leq i < n \) and \( b_i = b_{n-i-1} \), for \( 0 \leq i < n \), and \( a_n = 2a_0 \). If \( (p + 1)/2 \leq a_0 < p \), then \( a_0 = p - 1 \), \( a_n = 2a_0 - p \), and \( D = p^2 + 1 \).
Becker [Bec90] proved the same result, but for $D \in \mathbb{Q}$ with $v(D) = 0$ and $\sqrt{D} \in \mathbb{Q}_p \setminus \mathbb{Q}$. Becker also proves a similar theorem for $p = 2$, showing that the period cannot start until after $a_2$.

### 1.2.2 Ruban Continued Fractions

Ruban [Rub70] defined a $p$-adic continued fraction algorithm by defining analogues of the integer part and fractional part functions that are used to define continued fractions in the real case. That is, for a $p$-adic number

$$\alpha = \sum_{k=n}^{\infty} c_k p^k,$$

where $n \in \mathbb{Z}$, $c_k \in \{0, \ldots, p-1\}$ for $k \geq n$, and $c_n \neq 0$, the fractional part is defined by

$$\{\alpha\} = \sum_{k=n}^{0} c_k p^k \text{ if } n \leq 0, \text{ or } \{\alpha\} = 0 \text{ otherwise},$$

and the integer part is defined by

$$[\alpha] = \sum_{k=1}^{\infty} c_k p^k.$$

**Definition 2.** The Ruban continued fraction (RCF) for $\alpha \in p\mathbb{Z}_p$ is constructed in the following way:

1. $\alpha_0 = \alpha$, $\alpha_{n+1} = b_n/(\alpha_n - a_n)$
2. $a_0 = 0$ and $b_0 = 1$
3. $a_n = \{\alpha_n\}$ and $b_n = 1$

for $n \geq 0$, as long as $\alpha_n \neq a_n$. If $\alpha_n = a_n$ then the continued fraction terminates with $a_n$ as its final partial quotient.
This definition implies that $v(a_n) < 0$, $v(\alpha_n) < 0$, and $\alpha_n = 1/[(\alpha_{n-1})]$ for $n \geq 1$. Ruban showed that the continued fraction produced in this way always converges to the number it represents, and that any continued fraction with $a_0 = 0$, $v(a_n) < 0$, and $b_n = 1$, for $n \geq 1$ converges to a number in $p\mathbb{Z}_p$. Also, he derived various bounds on the convergents and on the numerators and denominators of the convergents. After deriving these basic properties of his continued fractions, he concentrated on their metric theory, as the purpose of his paper was to establish $p$-adic analogues of Khinchin’s results on the metric theory of real continued fractions [Khi97].

The first person to characterize the rational numbers with infinite RCFs was Laohakosol [Lao85]. Since RCFs have 1 as the constant partial numerator, we can denote Ruban continued fractions by the notation $[a_0, a_1, a_2, \ldots]$, as with simple continued fractions. Laohakosol proved the following.

**Theorem 10** (Laohakosol). Let $\alpha \in p\mathbb{Z}_p$. Then $\alpha$ is rational if and only if its RCF is finite, or is infinite with the periodic form

$$\alpha = [a_0, a_1, \ldots, a_k, (p-1)(1+p^{-1})].$$

Wang [Wan85], who was apparently unaware of Ruban’s work, also characterized the rational numbers with infinite RCFs, and further, gave a condition on the partial quotients sufficient for a $p$-adic number to be transcendental.

### 1.2.3 Browkin’s Results

Browkin [Bro78] defined a continued fraction algorithm for local fields by defining classes of maps on the field that behave like the fractional part map of Ruban. Let $K$ be a field that is complete with respect to a normalized discrete valuation $v$, let $\mathcal{O}_v$ be the valuation ring, and let $\mathfrak{m}_v$ be its unique maximum ideal. Also, let $\pi \in \mathcal{O}_v$ be a uniformizing element and let $\eta : K \to K/\mathfrak{m}_v$ be the canonical quotient map of abelian groups. To make the terminology easier, we give Browkin’s map, defined below, a name.
**Definition 3.** Let $s : K \to K$. Then $s$ is a *Browkin map* if it satisfies the following:

- $s(0) = 0$
- $s(a) = s(b)$ when $a - b \in m$
- $\eta s = \eta$.

This is a generalization of Ruban’s fractional part map, since the map

$$s \left( \sum_{k=n}^{\infty} c_k \pi^k \right) = \begin{cases} 
\sum_{k=n}^{0} c_k \pi^k & n \leq 0 \\
0 & n > 0 \end{cases},$$

(1.8)

where $c_k$ is in some set of representatives for $O_v / m_v$ and $c_n \neq 0$, is a Browkin map. Given a fixed Browkin map, $s$, Browkin defined a continued fraction for a number $\alpha \in K$ by $\alpha_0 = \alpha$, $a_n = s(\alpha_n)$, and $\alpha_{n+1} = 1/(\alpha_n - a_n)$ for $n \geq 0$. He proved that this definition generates a continued fraction that converges to $\alpha$, and that if $[a_0, a_1, \ldots]$ is a continued fraction with $v(a_n) < 0$ for $n \geq 0$, then the continued fraction converges to an element in $K$. For $\mathbb{Q}_p$, Browkin considered the Browkin map that sends an element $\alpha \in \mathbb{Q}_p$ to the unique representative in $(\alpha + m_v) \cap (-p/2, p/2]$. For $p > 2$, this is the same as the map $s$ defined by (1.8), where $\pi = p$ and the set of representatives is $\{- (p - 1)/2, \ldots, 0, \ldots, (p - 1)/2\}$.

**Definition 4.** Let $s : \mathbb{Q}_p \to \mathbb{Q}$ be the Browkin map defined in the previous paragraph for $p > 2$. The *first Browkin continued fraction* (BCF1) for $\alpha \in \mathbb{Q}_p$ is constructed in the following way:

1. $\alpha_0 = \alpha$, $\alpha_{n+1} = b_n/(\alpha_n - a_n)$
2. $b_n = 1$
3. $a_n = s(\alpha_n)$

for $n \geq 0$, as long as $\alpha_n \neq a_n$. If $\alpha_n = a_n$ then the continued fraction terminates with $a_n$ as its final partial quotient.
A nice property that BCF1s have is that continued fractions for rational numbers are finite [Bro78]. Browkin’s first paper [Bro78] consisted of establishing the definition and results mentioned already. At the end of his first paper, Browkin considered quadratic irrationals in the \( p \)-adic case, finding periods for a number of BCF1s of square roots in \( \mathbb{Q}_5 \), but noted that he could observe no period in the expansion of \( \sqrt{19} \in \mathbb{Q}_5 \).

Between Browkin’s first and second papers, Bedocchi wrote a number of papers studying BCF1s of quadratic irrationals [Bed88, Bed89, Bed90, Bed93]. In [Bed88], Bedocchi proves two important theorems regarding the structure of periodic Browkin continued fractions of quadratic irrationals. The first is analogous to Theorem 4, regarding real square roots.

**Theorem 11** (Bedocchi). If \( \alpha \in \mathbb{Q}_p \) has a periodic BCF1, then the expansion is purely periodic if and only if \( |\alpha|_p > 1 \) and \( |\overline{\alpha}|_p < 1 \), where \( \overline{\alpha} \) is the conjugate of \( \alpha \).

We know that \( \alpha \) must be a quadratic irrational, since Browkin showed that every rational number has a finite BCF1. Bedocchi’s second theorem has to do with when the period starts for a square root.

**Theorem 12** (Bedocchi). If \( D \in \mathbb{Z} \) is a non-square, and \( \sqrt{D} \in \mathbb{Q}_p \) has a periodic BCF1, then the period starts after two terms, unless \( p = 2 \) and \( D \equiv 4 \mod 8 \), in which case the period starts after three terms.

In his second paper [Bed89], Bedocchi shows that for \( p \geq 5 \) there are infinitely many integers \( D \), such that \( \sqrt{D} \in \mathbb{Q}_p \) has a periodic BCF1 with a period length of two. Further, he conjectures that all square roots of integers with periodic BCF1s have an even periodic length. Bedocchi’s third paper [Bed90] gives a way to answer this conjecture for a given \( p > 2 \) and odd periodic length \( k \). He shows that for such a \( p \) and \( k \), only finitely many \( D \in \mathbb{Z} \) can exist where \( \sqrt{D} \in \mathbb{Q}_p \) has a periodic BCF1 with periodic length \( k \). Further, he gives bounds on \( k \) and shows that if \( p \mid D \), then \( k \neq 3 \).
In his fourth paper [Bed93], he shows that a certain family of quadratic irrationals all have periodic BCF1s with similar periods.

In Browkin’s second paper [Bro01], he modifies his original algorithm to generate algorithms that produce periodic continued fractions for quadratic irrationals more frequently. He achieves this by allowing more flexibility in his choice of partial quotients, and even allows every other partial quotient to have valuation zero. His first new algorithm (BCF2) he shows to be equivalent to something like a Schneider continued fraction, where the partial denominators are integers in \{±1, \ldots, ±(p − 1)/2\} and each partial numerator is \(p\). The other two algorithms (BQCF1 and BQCF2) are specific to quadratic irrationals, and one seems to yield periodic continued fractions for all square roots of integers when \(p < 17\). Browkin did not provide any proofs for general periodicity for any \(\mathbb{Q}_p\) and his first mention of non-periodicity was for \(\mathbb{Q}_{23}\).

The three other algorithms are defined and discussed in Section 2.3.

There are, additionally, a couple of interesting lemmas regarding the kinds of numbers that can have periodic continued fractions (more general that Browkin or Ruban continued fractions) of periods two or four, with a single term before the period. For instance, Browkin shows as result of his lemmas that

\[
\sqrt{2p^2 + 2p + 1} = [p + 1, p^{-1}, 1, p^{-1}, 2p + 1].
\]

More analysis of Browkin’s algorithms, and their precise definitions, occurs in later sections.

1.3 Approximation Lattices

Inspired by the work of Mahler [Mah40], for each \(p\)-adic integer, de Weger [dW86] constructed a structure and a notion of periodicity such that \(p\)-adic quadratic irrationals have periodic structures. This result is the closest analogue of Lagrange’s Theorem that exists today, although it does not directly involve continued fractions.
and rational numbers have periodic structures as well. Mahler’s goal was to obtain an algorithm to provide best rational approximations to $p$-adic integers, using a geometrical method rather than generating the approximations from convergents of a continued fraction. The algorithm produces a sequence of $2 \times 2$ integral matrices where the product of the first $n + 1$ matrices is a matrix whose entries generate approximations of the $p$-adic integer to within $p^{-n}$. These matrices and their products are very similar to those in (1.3), and a corresponding continued fraction can be constructed by using an analogue of a theorem first proved by Daniel Bernoulli, Theorem 1, as pointed out to the author by de Weger. Even using Theorem 1, however, it is not easy to generate a periodic continued fraction from a periodic sequence of approximation lattices. This process is discussed in Section 2.1.1.

For a $p$-adic integer $\alpha$ de Weger defined the $n$th approximation lattice for $\alpha$ as

$$\Gamma_n = \left\{ (P, Q) \in \mathbb{Z}^2 \mid |P - Q\alpha|_p \leq \frac{1}{p^n} \right\}.$$  

In his paper, de Weger leaves out a few details, so we present de Weger’s results on the properties of approximation lattices and their relationship to $p$-adic numbers with more detail. In particular, we give proofs for the following three propositions. We note here the similarity between the sequence of lattices $(\Gamma_n)_{n \geq 0}$ and the definition of a multidimensional continued fraction given by Brentjes [Bre81], which is also defined in terms of sequences of lattices. The results on multidimensional continued fractions are similar to the results for naturally defined $p$-adic continued fractions in that no single definition results in periodicity for an entire class of numbers, and no single definition has all the desired properties analogous to real, simple continued fractions [Sch00].

Note that since

$$|Q - P\alpha^{-1}|_p = |\alpha^{-1}|_p |P - Q\alpha|_p,$$

the properties held by the approximation lattices of $\alpha$ and $\alpha^{-1}$ are the same. If $|\alpha|_p = p^{-k}$, then $\Gamma_n$ for $\alpha^{-1}$ is just $\Gamma_{n-k}$ for $\alpha$ with the coordinates of its elements
reversed. Thus, we restrict ourselves to the case where \( \alpha \in \mathbb{Z}_p \). In this case, it is clear that \( \Gamma_0 = \mathbb{Z}^2 \) and that \( \Gamma_{n+1} \subseteq \Gamma_n \) for all \( n \geq 0 \).

For a \( p \)-adic number

\[ \alpha = \sum_{k=n}^{\infty} c_k p^k, \]

denote the sum up to, but not including, the \( m \)th term by

\[ \{\alpha\}_m = \sum_{k=n}^{m-1} c_k p^k. \]

The following proposition describes the lattice structure of each approximation lattice. The results we use concerning lattices can be found in [Coh80, Ch. 4].

**Proposition 2** (de Weger). Let \( n \geq 0 \) be an integer and let \( \alpha \in \mathbb{Z}_p \). Then

(i) \( \Gamma_n \) is a lattice in \( \mathbb{Z}^2 \) of rank 2, and \( \{(p^n, 0), (\{\alpha\}_n, 1)\} \) is a basis for \( \Gamma_n \)

(ii) \( \det(\Gamma_n) = p^n \)

(iii) \( (P, Q), (R, S) \in \Gamma_n \) form a basis for \( \Gamma_n \) if and only if \( |PS - QR| = p^n \)

**Proof.** Suppose \( (P, Q), (R, S) \in \Gamma_n \). Then

\[
|(P - R) - (Q - S)\alpha|_p = |(P - Q\alpha) - (R - S\alpha)|_p \\
\leq \max(|P - Q\alpha|_p, |R - S\alpha|_p) \\
\leq \frac{1}{p^n},
\]

so \( \Gamma_n \) is a lattice in \( \mathbb{Z}^2 \). Denote \( (p^n, 0) = e_1 \) and \( (\{\alpha\}_n, 1) = e_2 \). Clearly \( e_1, e_2 \in \Gamma_n \). To see that \( \{e_1, e_2\} \) is a basis for \( \Gamma_n \), note that

\[
(P, Q) = \frac{P - Q\{\alpha\}_n}{p^n} e_1 + Q e_2,
\]

and the coefficient of \( e_1 \) is integral since \( (P, Q) \in \Gamma_n \). Thus, \( \Gamma_n \) is of rank 2 and has \( \{e_1, e_2\} \) as a basis.
The second part follows by taking the determinant of the matrix whose rows are $e_1$ and $e_2$. For the last part, $\{(P, Q), (R, S)\}$ is a basis for $\Gamma_n$ if and only if it is related to $\{e_1, e_2\}$ by a matrix $T \in \text{SL}_2(\mathbb{Z})$. That is, if and only if
\[
\det(T) = \frac{1}{p^{2n}} \left| \begin{pmatrix} P & Q \\ R & S \end{pmatrix} \begin{pmatrix} -\{\alpha\}_n \\ p^n \end{pmatrix} \right| = p^{-2n} [(P - Q\{\alpha\}_n)Sp^n - (R - S\{\alpha\}_n)Qp^n] = p^{-n}(PR - QS) = \pm 1.
\]
Thus, $\{(P, Q), (R, S)\}$ is a basis if and only if $|PR - QS| = p^n$. \qed

The index of $\Gamma_{n+1}$ in $\Gamma_n$ is defined to be the cardinality of $\Gamma_n/\Gamma_{n+1}$.

**Proposition 3** (de Weger). *Let $n \geq 0$ be an integer. The index of $\Gamma_{n+1}$ in $\Gamma_n$ is $p$.***

**Proof.** First, we give a criterion for an element of $\Gamma_n$ to be an element of $\Gamma_{n+1}$, with respect to the basis $\{e_1, e_2\}$. Since the elements of $\Gamma_n$ are given by
\[
\lambda_1(p^n, 0) + \lambda_2(\{\alpha\}_n, 1) = (\lambda_2\{\alpha\}_n + \lambda_1p^n, \lambda_2),
\]
where $\lambda_1, \lambda_2 \in \mathbb{Z}$, and the elements of $\Gamma_{n+1}$ are given by
\[
\mu_1(p^{n+1}, 0) + \mu_2(\{\alpha\}_{n+1}, 1) = (\mu_2\{\alpha\}_n + (\mu_2c_n + \mu_1p)p^n, \mu_2),
\]
where $\mu_1, \mu_2 \in \mathbb{Z}$, an element $\lambda_1e_1 + \lambda_2e_2 \in \Gamma_n$ is in $\Gamma_{n+1}$ if and only if $p | \lambda_1 - c_n\lambda_2$.

We can now see that the size of $\Gamma_n/\Gamma_{n+1}$ is $p$ by the surjective homomorphism $\Gamma_n \to \mathbb{Z}/p\mathbb{Z}$ given by
\[
(p^n, 0) \mapsto 1 + p\mathbb{Z} \text{ and } (\{\alpha\}_n, 1) \mapsto -c_n + p\mathbb{Z}.
\]
Then
\[
\lambda_1(p^n, 0) + \lambda_2(\{\alpha\}_n, 1) \mapsto (\lambda_1 - c_n\lambda_2) + p\mathbb{Z},
\]
so the kernel of the map is all elements $\lambda_1e_1 + \lambda_2e_2 \in \Gamma_n$ for which $p | \lambda_1 - c_m\lambda_2$, which is $\Gamma_{n+1}$. \qed
One could apply a lemma in [Coh80] that says that the index is the absolute value of the determinant of a matrix whose columns are a basis of $\Gamma_{n+1}$ expressed in terms of a basis for $\Gamma_n$, but the proof requires more facts about lattices to be developed and does not give a condition for an element of $\Gamma_n$ to be in $\Gamma_{n+1}$.

The final important property that approximation lattices have is that $p\Gamma_{n-1} \neq \Gamma_{n+1}$ for all $n \geq 1$. Let

$$Z^2 = \Lambda_0 \supset \Lambda_1 \supset \Lambda_2 \supset \cdots$$

be an arbitrary sequence of lattices in $Z^2$. The sequence is called of index $p$ if the index of $\Lambda_{n+1}$ in $\Lambda_n$ is $p$ for all $n \geq 0$, and the sequence is called irreducible if $p\Lambda_{n-1} \neq \Lambda_{n+1}$ for all $n \geq 1$. Thus, we have shown that the sequence of approximation lattices determined by a $p$-adic integer is irreducible and of index $p$. Conversely, it is almost true that an irreducible sequence of lattices of index $p$ (1.9) determines a $p$-adic integer. The only extra condition required is that for any basis $\{(P,Q), (R,S)\}$ of $\Lambda_1$, $Q$ and $S$ must be relatively prime. If $(Q,S) \neq 1$ then the sequence of lattice obtained by interchanging coordinates determines a $p$-adic integer, since in that case $(P,R) = 1$.

**Proposition 4** (de Weger). There is a one-to-one correspondence between the $p$-adic integers and the sequences of lattices $Z^2 = \Lambda_0 \supset \Lambda_1 \supset \cdots$ that are of index $p$, irreducible, and for which any basis $\{(P,Q), (R,S)\}$ of $\Lambda_1$ has the property that $(Q,S) = 1$. For a $p$-adic integer, $\alpha$, the corresponding sequences of lattices is the sequence of approximation lattices for $\alpha$. For a sequences of lattices, the corresponding $p$-adic integer, $\alpha$, is the unique $p$-adic integer for which $\{(p^n, 0), (\{\alpha\}_n, 1)\}$ is a basis for $\Lambda_n$, for all $n \geq 1$.

**Proof.** To see that the sequence $Z^2 = \Lambda_0 \supset \Lambda_1 \supset \cdots$ determines a $p$-adic integer, we show that there is a unique $\alpha \in \mathbb{Z}_p$ such that $\{(p^n, 0), (\{\alpha\}_n, 1)\}$ is a basis for $\Lambda_n$, $n \geq 1$. Suppose that $\{(P,Q), (R,S)\}$ is a basis for $\Lambda_1$ with $(Q,S) = 1$. By the lemma referred to in the previous paragraph, $PS - QR = \pm p$, and since $(Q,S) = 1$, either
$p \nmid Q$ or $p \nmid S$. Suppose, without loss of generality, that $p \nmid Q$. If $\{(p, 0), (a_0, 1)\}$ is a basis for $\Lambda_1$ then

\[
\frac{1}{p} \begin{pmatrix} P & Q \\ R & S \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -a_0 & p \end{pmatrix} = \frac{1}{p} \begin{pmatrix} P - a_0Q & pQ \\ R - a_0S & pS \end{pmatrix} \in \text{SL}_2(\mathbb{Z}).
\]

If we choose the unique $a_0 \in \{0, \ldots, p-1\}$ such that $a_0 \equiv PQ^{-1} \pmod{p}$ then $p \mid P - a_0Q$ and $p \mid R - a_0S$, since by $PS - QR = \pm p$—or $PS \equiv QR \pmod{p}$—we have

\[
R \equiv Q^{-1}QR \equiv Q^{-1}PS \equiv a_0S \pmod{p}.
\]

By this choice of $a_0$ the matrix product above is in $\text{SL}_2(\mathbb{Z})$.

Now suppose that $a_0, \ldots, a_{n-1}$ have been chosen so that $\{(p^k, 0), (a_0 + \cdots + a_{k-1}p^{k-1}, 1)\}$ is a basis for $\Lambda_k$, for all $k \leq n$. For efficiency, let us denote $a_0 + \cdots + a_{k-1}p^{k-1}$ by $A_k$. Suppose $\{(P, Q), (R, S)\} = \{\lambda_1e_1 + \lambda_2e_2, \mu_1e_1 + \mu_2e_2\}$ is a basis for $\Lambda_{n+1}$, where $e_1 = (p^n, 0)$ and $e_2 = (A_n, 1)$. If $p \mid Q$ then $p \mid \lambda_2$ and

\[
(P, Q) = p \left( \lambda_1p^{n-1} + \frac{\lambda_2}{p} A_n, \frac{\lambda_2}{p} \right)
\]

\[
= p \left( \left( \lambda_1 + a_{n-1} \frac{\lambda_2}{p} \right) p^{n-1} + \frac{\lambda_2}{p} A_{n-1}, \frac{\lambda_2}{p} \right)
\]

\[
= p \left[ \left( \lambda_1 + a_{n-1} \frac{\lambda_2}{p} \right) e_1' + \frac{\lambda_2}{p} e_2' \right] \in p\Lambda_{n-1},
\]

where $e_1' = (p^{n-1}, 0)$ and $e_2' = (A_{n-1}, 0)$ form a basis for $\Lambda_{n-1}$. Similarly, if $p \mid S$ then $(R, S) \in p\Lambda_{n-1}$. Since the sequence of lattices is irreducible, either $p \nmid Q$ or $p \nmid S$. Without loss of generality we suppose that $p \nmid Q$.

Since the sequence of lattices is of index $p$, $|\lambda_1\mu_2 - \lambda_2\mu_1| = p$, and the rest of the proof proceeds as in the case of $n = 1$. Namely, we want to show that $\Lambda_{n+1}$ has $pe_1$ and $a_ne_1 + e_2$ as a basis, for some $a_n \in \{0, \ldots, p-1\}$. This will happen if and only if

\[
\frac{1}{p} \begin{pmatrix} \lambda_1 & \lambda_2 \\ \mu_1 & \mu_2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -a_n & p \end{pmatrix} \in \text{SL}_2(\mathbb{Z}),
\]

which we have already shown is satisfied by the unique $a_n \in \{0, \ldots, p-1\}$ for which $a_n \equiv \lambda_1\lambda_2^{-1} \pmod{p}$. 

The unique $\alpha \in \mathbb{Z}_p$, such that $\{(p^n, 0), (\{\alpha\}_n, 1)\}$ is a basis for $\Lambda_n$, $n \geq 1$, is then

$$\alpha = a_0 + a_1 p + a_2 p^2 + \cdots .$$

As an analogue for periodicity of continued fractions, de Weger defined periodicity in a sequence of approximation lattices as follows.

**Definition 5.** A sequence $\Gamma_0 \supseteq \Gamma_1 \supseteq \cdots$ of approximation lattices for a $p$-adic integer is periodic if there is a linear transformation $\Xi : \mathbb{R}^2 \to \mathbb{R}^2$, an integer $n_0 \geq 0$, and an integer $k \geq 1$ such that $\Xi(\Gamma_n) = \Gamma_{n+k}$ for all $n \geq n_0$.

This periodicity translates into actual periodicity of a sequence of matrices. We adopt the same notation for what follows here and in Section 2.1.1 as de Weger. Suppose bases for $\Gamma_n$, $0 \leq n \leq n_0 + k - 1$, are chosen arbitrarily, which we denote by the rows of the matrices

$$C_n = \begin{pmatrix} P_n & Q_n \\ R_n & S_n \end{pmatrix}.$$ 

If $\chi^T$ is the matrix for $\Xi$ then we can get bases for $\Gamma_n$, $n = n_0 + i + jk$, $0 \leq i < k$, $j \geq 0$, from the rows of $C_n = C_{n_0+i} \chi^j$. If we denote by $\psi_n$ the matrix $\psi_n = C_{n+1} C_n^{-1}$, for $n \geq 0$, the sequences $(\psi_n)_{n \geq 0}$ is periodic starting with $n = n_0$ and with $k$ as the period length. To see this, suppose $n = n_0 + i + jk$, $0 \leq i < k - 1$, $j \geq 0$ as before. Then

$$\psi_n = C_{n+1} C_n^{-1} = C_{n_0+i+1} \chi^j (C_{n_0+i} \chi^j)^{-1} = C_{n_0+i+1} C_{n_0+i}^{-1} \psi_{n_0+i} .$$

If $i = k - 1$ then

$$\psi_n = C_{n+1} C_n^{-1} = C_{n_0} \chi^{j+1} (C_{n_0+k-1} \chi^j)^{-1} = C_{n_0} \chi C_{n_0+k-1}^{-1} = C_{n_0+k} C_{n_0+k-1}^{-1} = \psi_{n_0+k-1} .$$

We will see in Section 2.1.1 that the sequence $(\psi_n)_{n \geq 0}$ is an analogue for the sequence of partial denominators, and we give an algorithm for converting a periodic sequence
of approximation lattice into a periodic continued fraction, for square roots of integers in $\mathbb{Z}_p^\times$.

de Weger proved an analogue of Lagrange’s Theorem for approximation lattices.

**Theorem 13** (de Weger). *A sequence of approximation lattices for a $p$-adic integer, $\alpha$, is periodic if and only if $\alpha$ is rational or a quadratic irrational.*

In the proof of the theorem, de Weger constructs the map $\Xi$, which we detail in Section 2.1.1 and use in the algorithm to generate a periodic continued fraction for $\alpha$ from its periodic sequence of approximation lattices.

Another important result de Weger proved in [dW86] is an analogue of Hurwitz’s Theorem for any convex norm used to evaluate the “size” of a rational approximation. That is, for any convex norm $\Phi$, de Weger gives a number $\Delta(\Phi)$ for which

$$|P - Q\alpha|_p \leq \frac{1}{\Delta(\Phi)\Phi(P,Q)^2}$$

has infinitely many solutions for $\alpha \notin \mathbb{Q}$, and any $p$, but for which only finitely many solutions exist for sufficiently large $p$ when $\Delta(\Phi)$ is replaced by a larger real number. de Weger also gives an analogue of Theorem 6.

Approximation lattices provide a good mechanism for producing good rational approximations to irrational $p$-adic numbers. However, calculating $\chi$ for a periodic sequence of approximation lattices is not easy, and there is too much choice involved in the sequence $(\psi_n)_{n \geq 0}$ to have a satisfying, definitive periodic structure. A good complement to approximation lattices would be a continued fraction algorithm that can be applied to any $p$-adic number and that generates a strictly defined periodic continued fraction for quadratic irrationals. It would be even better if the algorithm had other nice properties, such as generating finite continued fractions for rational numbers or generating good rational approximations for irrational numbers.
1.4 Overview and Conventions

We start with some conventions that will save much repetition. Typically, we represent an element of $\mathbb{Q}_p$ by $\alpha$. Given some continued fraction representing $\alpha$ we assume, unless stated otherwise, that

- $a_n$ and $b_n$ represent the partial denominators and numerators, respectively
- $\alpha_n$ is the $n$th remainder, so $\alpha_{n+1} = b_n/(\alpha - a_n)$ and $\alpha_0 = \alpha$
- $A_n/B_n$ is the $n$th convergent.

The formulas in Proposition 1 hold among these values, and use of these formulas will not always be accompanied by a reference to the proposition.

If $\alpha$ is a quadratic irrational, then we also assume the meaning of $P_n$ and $Q_n$ as

$$
\alpha_n = \frac{P_n + \sqrt{D}}{Q_n},
$$

and we will use their recurrence formulas (1.6)-(1.7) without explicit reference to where they are defined. Using this convention will allow us to define continued fraction algorithms and talk about the algorithms without always re-defining what we mean by $a_n$, $b_n$, $\alpha_n$, $A_n$, $B_n$, $P_n$, and $Q_n$.

Given the number and variety of continued fractions we discuss in this paper, we adopt the following naming convention for continued fractions coming from an explicit algorithm or that belong to some general class. Continued fractions that are generated by some explicit algorithm that can be applied to arbitrary $p$-adic numbers or $p$-adic integers are abbreviated by acronyms ending in “CF”, like SCF (Schneider continued fraction), RCF (Ruban continued fraction), and BCF1-BCF2 (Browkin continued fractions). Continued fractions that are generated by an explicit algorithm that only applies to quadratic irrationals are abbreviated by acronyms ending in “QCF”, like BQCF1-BQCF2 (Browkin quadratic continued fractions) and NQCF (new quadratic continued fraction) defined below. For a general class of continued fractions, like
all simple continued fractions that converge \( p \)-adically, the class is abbreviated by an acronym ending in “TCF”, the T standing for type. Some examples below are ITCF (integral type continued fraction) and SRTCF (simple rational type continued fraction).

The next chapter introduces two general classes of continued fractions that converge \( p \)-adically. All of the continued fractions discussed so far fall into one of these two classes. Also in the next chapter, we show how to convert a periodic sequence of approximation lattices into a periodic continued fraction, and give a general \( p \)-adic continued fraction algorithm that produces periodic continued fractions for square roots, given the right parameters.

The third chapter discusses a subclass of one of the general classes of continued fractions introduced in Chapter 2. We give sufficient criteria for choosing partial denominators that an algorithm can follow that will always produce finite continued fractions for rational numbers. We introduce an algorithm for quadratic irrationals, for which we prove periodicity in \( \mathbb{Q}_2 \) and \( \mathbb{Q}_3 \) and then discuss numerical results for periodicity and the structure of periods for other \( p \)-adic fields. In the last chapter, we apply the techniques developed in Chapter 3 to bear on \( t \)-adic continued fractions in \( \mathbb{F}_q((t)) \).
Chapter 2

General Definitions for $p$-adic Continued Fractions

In this chapter we define two general classes of continued fractions. One class is not simple (i.e., the partial numerators are not necessarily 1) and has integral partial numerators and denominators, and the other class is simple with rational partial denominators. In each case, a continued fraction for some $\alpha \in \mathbb{Q}_p$ is defined to be in the class if its $n$th partial numerator and denominator $a_n$ and $b_n$, satisfy some relationship with the $n$th remainder, $\alpha_n$. For each class two convergence theorems follow. The first shows that given a number $\alpha$ and a continued fraction for it that satisfies the conditions in the class definition, the convergents of the continued fraction converge to $\alpha$ $p$-adically. The second theorem shows that if a number is defined by a continued fraction whose $a_n$ and $b_n$ satisfy certain conditions, then the convergents converge to a number, $\alpha \in \mathbb{Q}_p$, for which the conditions in the class definition are satisfied.

These two convergence theorems are important in light of the following example.

Example 1. Consider the continued fraction

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}}.$$ 

We show that it cannot converge to a number in $\mathbb{Q}_p$, in two ways. First, if it were to converge to some number $\alpha \in \mathbb{Q}_p$, then $|F_{n+1}/F_n - \alpha|_p$ would converge to zero, where $F_0 = 1$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$ for $n \geq 0$, are the Fibonacci numbers. However, it is easy to see that $|F_{n+1}/F_n - \alpha|_p \geq 1$ infinitely often. If $\alpha \equiv k \mod p$ then for

$$\left| \frac{F_{n+1}}{F_n} - \alpha \right|_p = \left| F_{n+1} - F_n \alpha \right|_p |F_n|^{-1}_p < 1$$
it is necessary that $|F_{n+1} - F_n\alpha|_p < 1$, or equivalently, that $F_{n+1} \equiv kF_n \pmod{p}$.

Suppose, that $F_{n+1} \not\equiv kF_n \pmod{p}$ occurs for only finitely many values of $n$, and that $n = N$ is the last time it occurs. Then

$$F_{N+1} = F_{N+3} - F_{N+2} \equiv kF_{N+2} - kF_{N+1} \pmod{p} \equiv k(F_{N+2} - F_{N+1}) \pmod{p} \equiv kF_N \pmod{p},$$

which contradicts the assumption about $F_{N+1}$. Thus, $F_{n+1} \not\equiv kF_n \pmod{p}$ is true for infinitely many $n$, in which case $|F_{n+1}/F_n - \alpha|_p \geq 1$ infinitely often.

Another way to show that the convergents cannot converge $p$-adically was explained to us by one of our committee members, Dan Madden, who had a discussion regarding this with Kurt Mahler. If the continued fraction converges to some number, $\alpha \in \mathbb{Q}_p$, then it must satisfy

$$\alpha^2 - \alpha - 1 = 0 \quad \text{since} \quad \alpha = 1 + \frac{1}{\alpha}.$$  

Then, since $\lim_n F_{n+1}/F_n = \alpha$ we must have

$$\lim_n \left( \frac{F_{n+1}}{F_n} \right)^2 - \left( \frac{F_{n+1}}{F_n} \right) - 1 = 0. \quad (2.1)$$

However, by the well known identity

$$F_{n+1}F_{n-1} - F_n^2 = \pm 1$$
$$F_{n+1}(F_{n+1} - F_n) - F_n^2 = \pm 1$$
$$F_{n+1}^2 - F_{n+1}F_n - F_n^2 = \pm 1,$$

we have

$$\left( \frac{F_{n+1}}{F_n} \right)^2 - \left( \frac{F_{n+1}}{F_n} \right) - 1 = \pm \frac{1}{F_n^2},$$

by dividing both sides by $F_n^2$. Since $|F_n|_p \leq 1$, the limit (2.1) cannot be satisfied, not even by a subsequence of the convergents.
2.1 Integral Type Continued Fractions

We introduce a general class of continued fractions whose partial numerators and denominators are all integers. Schneider’s continued fractions [Sch70], and a generalization of them we study in Chapter 3, are a subclass of integral type continued fractions.

Definition 6. Let $\alpha \in \mathbb{Z}_p^\times$. A continued fraction of the form (1.1) or (1.2) is an integral type continued fraction (ITCF) for $\alpha$ if $a_i, b_i \in \mathbb{Z}$ and $v(\alpha_i - a_i) = v(b_i) = e_i > 0$ for $i \geq 0$. If $\alpha \in \mathbb{Q}_p \setminus \mathbb{Z}_p^\times$, then the requirements are the same, except that $a_0 = 0$ and $b_0 = p^{v(\alpha)}$. In particular, if $\alpha$ is not a $p$-adic integer then $b_0$ is not integral.

We mention a few properties about these continued fractions that can be derived quickly. First, note that $v(\alpha_i) = v(a_i) = 0$ for $i > 0$, and this holds for $i = 0$, as well, if $\alpha$ is a $p$-adic unit. Second, since $v(B_0) = v(1) = 0$, $v(B_1) = v(a_1) = 0$ and

$$v(B_{n+1}) = v(a_{n+1}B_n + b_nB_{n-1}) = v(a_{n+1}B_n) = 0,$$

for $n \geq 1$, it follows that $v(B_n) = 0$ for all $n \geq 0$. In particular, $B_n \neq 0$ for all $n \geq 0$.

From (1.4), we have

$$|A_nB_{n-1} - A_{n-1}B_n|_p = p^{-(e_0 + ... + e_{n-1})}, \quad (2.2)$$

for $n > 0$. It then follows that

$$\left| \frac{A_n}{B_n} - \frac{A_{n-1}}{B_{n-1}} \right|_p = \frac{p^{-(e_0 + ... + e_{n-1})}}{|B_{n-1}B_n|_p} = p^{-(e_0 + ... + e_{n-1})} \quad (2.3)$$

for $n > 0$.

Theorem 14. The convergents of an ITCF for $\alpha \in \mathbb{Q}_p$ converge to $\alpha$. 
**Proof.** Suppose \( \alpha \) is represented by an ITCF, using the notation above. That is, suppose we have sequences \((\alpha_n)_{n \geq 0}, (a_n)_{n \geq 0}, \) and \((b_n)_{n \geq 0}\) that satisfy \(\alpha_{n+1} = b_n/(\alpha_n - a_n)\) and the conditions in the definition of an ITCF. By Proposition 1 and (2.2)

\[
\left| \frac{\alpha - A_n}{B_n} \right|_p = \left| \frac{\alpha_{n+1}A_n + b_nA_{n-1} - A_n}{\alpha_{n+1}B_n + b_nB_{n-1} - B_n} \right|_p
= \frac{|b_n(A_{n-1}B_n - A_nB_{n-1})|_p}{|\left(\alpha_{n+1}B_n + b_nB_{n-1}\right)B_n|_p}
\]

Since \(v(B_n) = 0\) for \(n \geq 0\), \(v((\alpha_{n+1}B_n + b_nB_{n-1})B_n) = 0\) as \(v(\alpha_{n+1}) = 0\). Therefore

\[
\left| \frac{\alpha - A_n}{B_n} \right|_p = p^{-(e_0 + \cdots + e_n)} < p^{-e_0}p^{-n} \to 0,
\]

which shows that the convergents converge to \(\alpha\). \(\square\)

**Theorem 15.** If a continued fraction has the properties that \(a_i, b_i \in \mathbb{Z}, v(a_i) = 0,\) and \(v(b_i) = e_i > 0\) for all \(i \geq 0\), then all the convergents are defined and converge to a number \(\alpha \in \mathbb{Z}_p^\times\). If the continued fraction has the property above for \(i \geq 1, a_0 = 0, b_0 = p^{e_0},\) and \(e_0 \neq 0,\) then the convergents converge to a non-unit \(\alpha \in \mathbb{Q}_p\). Furthermore, the continued fraction is an ITCF for \(\alpha\).

**Proof.** Suppose a continued fraction has the first set of properties. Since \(v(B_n) = 0\) for \(n \geq 0\), all the convergents exist, and by (2.3) we have

\[
\left| \frac{A_{n+1}}{B_{n+1}} - \frac{A_n}{B_n} \right|_p = p^{-(e_0 + \cdots + e_n)} < p^{-n},
\]

for all \(n \geq 0\). Thus, as an immediate consequence of the ultrametric inequality, \((A_n/B_n)_{n \geq 0}\) is a Cauchy sequence and converges to some \(\alpha \in \mathbb{Q}_p\). As with \(B_n\), it is easy to see that \(v(A_n) = 0\) for all \(n\), in this case, so

\[
v(\alpha) = \lim_n v(A_n/B_n) = \lim_n 0 = 0,
\]

and \(\alpha \in \mathbb{Z}_p^\times\).
To show that the continued fraction is an ITCF for \( \alpha \), it remains to show that 
\[ v(\alpha_n - a_n) = v(b_n) = e_n \] 
for \( n \geq 0 \). To start the process, we need to show that 
\[ \lim_n v(A_n/B_n - a_0) = v(b_0). \] 
For \( n = 1 \),
\[
v(A_1/B_1 - a_0) = v(A_1 - a_0 B_1) = v(a_0 a_1 + b_0 - a_0 a_1) = v(b_0).
\]
Assume that \( v(A_i - a_0 B_i) = v(b_0) \) for all \( i \leq n \). Then
\[
v(A_{n+1}/B_{n+1} - a_0) = v(A_{n+1} - a_0 B_{n+1})
\]
\[
= v((a_{n+1} A_n + b_n A_{n-1}) - a_0 (a_{n+1} B_n + b_n B_{n-1}))
\]
\[
= v(a_{n+1} (A_n - a_0 B_n) + b_n (A_{n-1} - a_0 B_{n-1})
\]
\[
= v(b_0),
\]
since \( v(a_{n+1}) = 0 \) and \( v(b_n) > 0 \). Thus, \( v(\alpha_0 - a_0) = v(b_0) \). By induction, it can be shown that the continued fraction
\[
\begin{bmatrix}
  & b_n & b_{n+1} & \cdots \\
 a_n & a_{n+1} & a_{n+2} & \cdots
\end{bmatrix}
\]
converges to \( \alpha_n \), and so by the same logic that showed \( v(\alpha - a_0) = v(b_0) \), we have \( v(\alpha_n - a_n) = v(b_n) \).

If \( a_0 = 0 \), \( b_0 = p^{e_0} \), and \( e_0 \neq 0 \), then
\[
\left| \frac{A_{n+1}}{B_{n+1}} - \frac{A_n}{B_n} \right|_p = p^{-(e_0 + \cdots + e_n)} < p^{-e_0} p^{-n+1},
\]
so \((A_n/B_n)_{n \geq 0}\) is a Cauchy sequence and converges to some \( \alpha \in \mathbb{Q}_p \). By induction, \( v(A_n) = e_0 \) and \( v(B_n) = 0 \) for \( n \geq 1 \), so \( v(\alpha) = e_0 \neq 0 \), which shows that \( \alpha \) is not a \( p \)-adic unit. The argument that the continued fractions is an ITCF for \( \alpha \) is exactly the same.

\[ \square \]

2.1.1 Continued Fractions from Approximation Lattices

As de Weger suggested to us, in order to convert a sequence of approximation lattices to a continued fraction we need to apply Bernoulli’s Theorem, Theorem 1, to rational
approximations of a $p$-adic number. Suppose that $\alpha \in \mathbb{Q}_p$ and that $(A_n)_{n\geq 0}, (B_n)_{n\geq 0}$ are sequences of integers for which $|\alpha - A_n/B_n|_p$ converges to zero, and for which $B_0 = 1$. Then we can apply the theorem to get a $p$-adic continued fraction converging to $\alpha$.

The following example illustrates the use of Bernoulli’s Theorem.

**Example 2.** Let $\alpha = c_0 + c_1 p + c_2 p^2 + \cdots \in \mathbb{Z}_p$ where $c_n \neq 0$ for all $n \geq 0$. Using the notation of Section 1.3, if $A_n = \{\alpha\}_n$ and $B_n = 1$ we can apply Bernoulli’s Theorem to get the particularly interesting continued fraction

$$\alpha = \left(\frac{-c_1 p}{c_0 + c_1 p}\right) + \left(\frac{-c_0 c_2 p}{c_1 + c_2 p}\right) + \left(\frac{-c_1 c_3 p}{c_2 + c_3 p}\right) + \cdots$$

(2.4)

after making all the partial numerators and partial denominators integral by clearing out denominators.

If some of the $p$-adic digits are zero $\alpha$ can be re-written as $\alpha = c'_0 + c'_1 p + c'_2 p^2 + \cdots$ where $c'_n \neq 0$ for $n \geq 0$ by borrowing, and allowing borrowed $p$-adic digits to be $p$. For example,

$$1 + p^2 + p^4 + p^6 + \cdots = 1 + p \cdot p + p \cdot p^2 + (p - 1) \cdot p^3 + p \cdot p^4 + (p - 1) \cdot p^5 + \cdots$$

In this way, any $p$-adic integer can be written in the form (2.4).

The partial numerators and denominators resulting from Bernoulli’s Theorem might not be integral. However, it is easy to construct and equal continued fraction with integral partial numerators and denominators simply by clearing denominators, as long as the first partial denominator is integral, which is the case in Theorem 1. For example, if $a_{n+1} = p_{n+1}/q_{n+1}$ and $b_n = r_n/s_n$, where $p_n, q_n, r_n, s_n \in \mathbb{Z}$ for $n \geq 0$,
then
\[
a_0 + \frac{r_0}{s_0} + \frac{r_1}{s_1} + \frac{r_2}{s_2} + \frac{r_3}{s_3} + \frac{r_4}{s_4} + \cdots
\]
equals
\[
a_0 + \frac{r_0 q_1}{p_1 s_0 + r_1 s_0 q_2} + \frac{r_2 s_1 q_2}{p_2 s_1 + r_2 s_1 q_3} + \frac{r_3 s_2 q_3}{p_3 s_2 + r_3 s_2 q_4} + \cdots.
\]

To setup the framework connecting approximation lattices and continued fractions, let \(\alpha \in \mathbb{Z}_p\) be a quadratic irrational, and \((\Gamma_n)_{n \geq 0}\) its sequence of approximation lattices. By definition, if the sequence is periodic there exists a linear mapping \(\Xi : \mathbb{R}^2 \to \mathbb{R}^2\), an integer \(k > 0\), and an integer \(n_0 \geq 0\) such that \(\Xi(\Gamma_n) = \Gamma_{n+k}\) for all \(n \geq n_0\). Still using the notion of \([dW86]\) that was introduced in Section 1.3, if \(\chi^T\) is the matrix for \(\Xi\), then we can choose bases \(\{(P_n, Q_n), (R_n, S_n)\}\) of \(\Gamma_n\), with
\[
C_n = \begin{pmatrix} P_n & Q_n \\ R_n & S_n \end{pmatrix},
\]
such that \(C_{n+k} = C_n \chi\) for \(n \geq n_0\). Then the sequences of matrices, \((\psi_n)_{n \geq 0}\), defined by \(C_{n+1} = \psi_n C_n\) are periodic.

Using \((R_{n-1})_{n \geq 1}\) and \((S_{n-1})_{n \geq 1}\) for the sequences \((A_n)_{n \geq 0}\) and \((B_n)_{n \geq 0}\) in Theorem 1, we show that the resulting continued fraction is periodic when \(\alpha = \sqrt{D} \in \mathbb{Z}_p^\times\). First, we assume that \(C_n\) has been chosen for \(n = 0, \ldots, n_0 + k - 1\) by some method, and then \(C_{n_0 + i + jk} = C_{n_0 + i} \chi^j\) for \(i = 0, \ldots, k - 1\) and \(j \geq 0\).

We show the periodicity of the partial numerators and denominators by showing the periodicity of \(R_{n+1} S_{n-1} - R_{n-1} S_{n+1}\) and \(R_n S_{n+1} - R_{n+1} S_n\) for \(n \geq n_0 + k - 2\). Since
\[
C_{n+2} C_n^{-1} = \pm p^n \begin{pmatrix} P_{n+2} & Q_{n+2} \\ R_{n+1} & S_{n+1} \end{pmatrix} \begin{pmatrix} S_{n-1} & -Q_n \\ -R_{n-1} & P_n \end{pmatrix} = \begin{pmatrix} R_{n+1} S_{n-1} & \ast \\ R_{n-1} S_{n+1} & \ast \end{pmatrix},
\]
it is sufficient to prove the periodicity of \( C_{n+2}C_n^{-1} \) for \( n \geq n_0 + k - 2 \). This follows immediately from

\[
C_{n+jk+2}C_{n+jk}^{-1} = C_{n+2} \chi^j(C_n \chi^j)^{-1} = C_{n+2}C_n^{-1}.
\]

Periodicity of \( R_nS_{n+1} - R_{n+1}S_n \) follows in the same way by considering \( C_{n+2}C_n^{-1} \). In order to apply Theorem 1 we need to show that \( R_n/S_n \neq R_{n+1}/S_{n+1} \) for all \( n \geq 0 \). In order for this to be true, however, the choice of bases in \( C_0, \ldots, C_{n_0+k-1} \) needs to be done in a way that ensures \( R_n/S_n \neq R_{n+1}/S_{n+1} \) will be satisfied. For example, if \( \alpha \) has 0 as its \( n \)th \( p \)-adic digit, then \( (\{\alpha\}_n, 1) \) and \( (\{\alpha\}_{n+1}, 1) \) are equal, and part of bases for \( \Gamma_n \) and \( \Gamma_{n+1} \).

An ITCF whose partial numerators are all \( p \) generates convergents that form a basis for the approximation lattice of the number, \( \alpha \in \mathbb{Z}_p \), generating the continued fraction. More precisely, \( \{(pA_{n-1}, pB_{n-1}), (A_n, B_n)\} \) is a basis for \( \Gamma_{n+1} \) because

\[
|pA_{n-1}B_n - pA_nB_{n-1}|_p = p^{-(n+1)}
\]

and

\[
\left| \alpha - \frac{A_n}{B_n} \right|_p = p^{-(n+1)} \text{ and } |B_n|_p = 1
\]

for all \( n \geq 0 \). There are a number of easy ways in which to produce an ITCF with \( p \) as the constant partial numerator. For example, if

\[
\alpha_n = c_0 + c_1 p + c_2 p^2 + \cdots
\]

is the \( n \)th remainder then we simply can choose \( a_n = c_0 + (c_1 - 1)p \) if \( c_0 + (c_1 - 1)p \neq 0 \) and \( a_n = 2p \) otherwise.

To construct \( C_1, \ldots, C_{n_0+k-1} \) we calculate the first \( n_0 + k - 3 \) partial quotients of such a continued fraction, which gives us

\[
C_n = \begin{pmatrix} pA_{n-1} & pB_{n-1} \\ A_{n-1} & B_{n-1} \end{pmatrix}
\]
for $1 \leq n \leq n_0 + k - 1$. By construction, $A_n/B_n \neq A_{n+1}/B_{n+1}$ for $0 \leq n \leq n_0 + k - 3$,
since these quotients are convergents of a continued fraction. If $A_{n_0 + k - 1}/B_{n_0 + k - 1} \neq A_{n_0 + k - 2}/B_{n_0 + k - 2}$
then $A_n/B_n \neq A_{n+1}/B_{n+1}$ for all $n \geq 0$ by periodicity of $A_{n+1}B_n - A_nB_{n+1}$, where $(A_n, B_n)$ is the bottom row of the matrix $C_{n+1}$
for $n \geq n_0 + k - 1$. Thus, it remains to show that $A_{n_0 + k - 1}/B_{n_0 + k - 1} \neq A_{n_0 + k - 2}/B_{n_0 + k - 2}$ in order to have
an algorithm for constructing a periodic continued fraction from a periodic sequence
of approximation lattices, which we do by showing that the entry in the second row
and first column of $C_{n_0 + k}C_{n_0 + k - 1}^{-1}$ is non-zero.

We prove this for quadratic irrationals of the form $\sqrt{D} \in \mathbb{Z}_p$ with $p \nmid D$.

**Lemma 1.** $A_{n_0 + k}B_{n_0 + k - 1} - A_{n_0 + k - 1}B_{n_0 + k} \neq 0$

**Proof.** By de Weger's proof of periodicity we need to consider the quadratic order, $\mathcal{O}$, generated by 1 and $\sqrt{D}$, and its prime ideal

$$p = \{ \xi \in \mathcal{O} : |\xi|_p \leq p^{-1} \}.$$ 

Then $n_0 = 1$ and $k$ is the smallest integer such that $p^k = (\phi)$ is principal for some $\phi = x + y\sqrt{D} \in \mathcal{O}$. Since

$$p^k = \{ \xi \in \mathcal{O} : |\xi|_p \leq p^{-k} \},$$

we have $v(\phi) = k$. The map $p^n \to p^{n+k}$ given by $\xi \mapsto \xi \phi$ induces the map $\Xi : \Gamma_n \to \Gamma_{n+k}$ with transpose matrix

$$\chi = \begin{pmatrix} x & -y \\ -yD & x \end{pmatrix}.$$ 

Since $v(\phi) = k$, if $v(x), v(y) \leq k$ then $v(x) = v(y)$; otherwise, if $v(x) \neq v(y)$ then
$v(x), v(y) \geq k$ with at least one strictly greater. On the other hand, since $\det(\chi) = x^2 - y^2D = \pm p^k$, we must have that $v(x) \leq k/2$ or $v(y) \leq k/2$, so $v(x) = v(y) \leq k/2$. 


Then

\[
C_{n_0+k}C_{n_0+k+1}^{-1} = C_{n_0}\chi C_{n_0+k+1}^{-1} \\
= \left( \frac{-1}{p} \right)^{n_0+k} \left( \begin{array}{cc} pA_{n_0-2} & pB_{n_0-2} \\ A_{n_0-1} & B_{n_0-1} \end{array} \right) \chi \left( \begin{array}{cc} B_{n_0+k-2} & -pB_{n_0+k-3} \\ -A_{n_0+k-2} & pA_{n_0+k-3} \end{array} \right) \\
= \left( \begin{array}{cc} p(X_{11}x + Y_{11}y) & p(X_{12}x + Y_{12}y) \\ X_{21}x + Y_{21}y & X_{22}x + Y_{22}y \end{array} \right),
\]

where

\[
X_{11} = A_{n_0-2}B_{n_0+k-2} - A_{n_0+k-2}B_{n_0-2} \\
X_{12} = -(A_{n_0-2}B_{n_0+k-3} - A_{n_0+k-3}B_{n_0-2}) \\
X_{21} = A_{n_0-1}B_{n_0+k-2} - A_{n_0+k-2}B_{n_0-1} \\
X_{22} = -(A_{n_0-1}B_{n_0+k-3} - A_{n_0+k-3}B_{n_0-1})
\]

and

\[
Y_{11} = A_{n_0-2}A_{n_0+k-2} - B_{n_0-2}B_{n_0+k-2}D \\
Y_{12} = -(A_{n_0-2}A_{n_0+k-3} - B_{n_0-2}B_{n_0+k-3}D) \\
Y_{21} = A_{n_0-1}A_{n_0+k-2} - B_{n_0-1}B_{n_0+k-2}D \\
Y_{22} = -(A_{n_0-1}A_{n_0+k-3} - B_{n_0-1}B_{n_0+k-3}D).
\]

Since \(A_{n_0+k-1}B_{n_0+k-2} - A_{n_0+k-2}B_{n_0+k-1} = X_{21}x + Y_{21}y\), and

\[
X_{21}x + Y_{21}y = X_{21}x + (A_{n_0-1} - B_{n_0-1}\sqrt{D})(A_{n_0+k-2} + B_{n_0+k-2}\sqrt{D})y \\
- (A_{n_0-1}B_{n_0+k-2} - A_{n_0+k-2}B_{n_0-1})\sqrt{D}y,
\]

we have

\[
X_{21}x + Y_{21}y = (A_{n_0-1}B_{n_0+k-2} - A_{n_0+k-2}B_{n_0-1})(x + y\sqrt{D}) \\
- (A_{n_0-1} - B_{n_0-1}\sqrt{D})(A_{n_0+k-2} + B_{n_0+k-2}\sqrt{D})y.
\]

To show that \(X_{21}x + Y_{21}y \neq 0\) we calculate its \(p\)-adic absolute value. We know that \(|x + y\sqrt{D}|_p = p^{-k}, \ |y|_p \geq p^{-k/2}, \ |A_{n_0-1} - B_{n_0-1}\sqrt{D}|_p = p^{-n_0}, \) and
\[ |A_{n_0+k-2} + B_{n_0+k-2}\sqrt{D}|_p \] equals 1 if \( p > 2 \) and equals \( p^{-(n_0+k-2)} \) for \( p = 2 \). Thus, the only complete unknown is
\[
|A_{n_0-1}B_{n_0+k-2} - A_{n_0+k-2}B_{n_0-1}|_p,
\]
which we show is equal to \( p^{-(n_0+1)} \) for \( k > 1 \), by induction. In the case \( k = 1 \), \( X_{21} = 0 \) and so the \( p \)-adic absolute value is greater than or equal to \( p^{-(2n_0+(3/2)k-1)} \).

For the case \( k = 2 \) in (2.5), we have
\[
|A_{n_0-1}B_{n_0} - A_{n_0}B_{n_0-1}|_p = p^{-(n_0+1)} \text{ by (1.4)}.
\]
For the case \( k = 3 \) we have
\[
A_{n_0-1}B_{n_0+1} - A_{n_0+1}B_{n_0-1} = A_{n_0-1}(a_{n_0+1}B_{n_0} + pB_{n_0-1})
\]
\[
- (a_{n_0+1}A_{n_0} + pA_{n_0-1})B_{n_0-1} = a_{n_0+1}(A_{n_0-1}B_{n_0} - A_{n_0}B_{n_0-1}),
\]
which has absolute value \( p^{-(n_0+1)} \). Now suppose that (2.5) holds for two through \( k \), and consider the case of \( k + 1 \):
\[
A_{n_0-1}B_{n_0+k-1} - A_{n_0+k-1}B_{n_0-1} = A_{n_0-1}(a_{n_0+k-1}B_{n_0+k-2} + pB_{n_0+k-3})
\]
\[
- (a_{n_0+1}A_{n_0+k-2} + pA_{n_0+k-3})B_{n_0-1} = a_{n_0+k+1}(A_{n_0-1}B_{n_0+k-2} - A_{n_0+k-2}B_{n_0-1})
\]
\[
+ p(A_{n_0-1}B_{n_0+k-3} - A_{n_0+k-3}B_{n_0-1}),
\]
which has a \( p \)-adic absolute value of \( p^{-(n_0+1)} \) by the induction hypothesis. Thus, we have (2.5) is greater than or equal to \( p^{n_0+k/2} \) for \( p > 2 \) and is equal to \( p^{-(n_0+k+1)} \) for \( p = 2 \). In any case, since (2.5) is greater than zero, \( A_{n_0+k}B_{n_0+k-1} - A_{n_0+k-1}B_{n_0+k} \neq 0 \).

As a corollary of the preceding lemma, the following algorithm produces a periodic continued fraction from a periodic sequence of approximation lattices for \( \sqrt{D} \in \mathbb{Q}_p \), where \( D \) is a non-square integer and \( p \nmid D \).

**Algorithm 1.** This algorithm takes a non-square integer, \( D \), with a square root in \( \mathbb{Q}_p \) such that \( p \nmid D \), and produces a periodic continued fraction from the periodic sequence
of approximation lattices. The algorithm uses methods in the proof of periodicity of a sequence of approximation lattices in [dW86], Theorem 1, and the preceding lemma as its justification. Let \( \mathfrak{O} \) be the quadratic order generated by 1 and \( \sqrt{D} \), and let

\[ p = \{ \xi \in \mathfrak{O} : |\xi|_p \leq p^{-1} \} \]

be a prime ideal in \( \mathfrak{O} \).

1. Find the smallest positive integer \( k \) such that \( p^k = (\phi) \) is principal, for some \( \phi = x + y\sqrt{D} \in \mathfrak{O} \).

2. Calculate integers \( a_0, \ldots, a_{k-1} \) in the following way.
   a. \( a_0 = \sqrt{D}, a_{n+1} = p/(a_n - a_n) \) for \( n = 0, \ldots, k - 2 \)
   b. let \( a'_n \in \{1, \ldots, p - 1\} \) such that \( a_n \equiv a'_n \pmod{p} \)
   c. if \( v(a_n - a'_n) = 1 \) set \( a_n = a'_n \); otherwise, set \( a_n = a'_n - p \)

3. Set
   \[ C_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \psi_n = \begin{pmatrix} 0 & p \\ 1 & a_n \end{pmatrix}, \quad C_{n+1} = \psi_n C_n \]
   for \( n = 0, \ldots, k - 1 \).

4. Set
   \[ C_{k+1} = C_k \begin{pmatrix} x & -y \\ -yD & x \end{pmatrix} \]

5. Calculate \( a_k \) and \( b_{k-1} \) from Theorem 1, where the values of \( A_n \) and \( B_n \) come from
   \[ C_{n+1} = \begin{pmatrix} P_n & Q_n \\ A_n & B_n \end{pmatrix}, \]
   for \( n = 0, \ldots, k \).

6. The periodic continued fraction is then
   \[ \sqrt{D} = \left[ \begin{array}{cccccc} p & p & \cdots & p & b_{k-1} \\ a_0 & a_1 & a_2 & \cdots & a_{k-1} & a_k \end{array} \right]_p \]
Example 3. Let \( D = 499 \) and \( p = 3 \). Then \( \mathcal{D} = \mathbb{Z}[\sqrt{499}] \), \( p = 3\mathbb{Z} + (2 + \sqrt{499})\mathbb{Z} \), and \( p^5 = (16 - \sqrt{499})\mathcal{D} \) is the first power of \( p \) which is principal. One calculates the values \( a_0, \ldots, a_4 \) as in Table 2.1 and calculates

\[
C_6 = \begin{pmatrix} 3 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 16 & 1 \\ 499 & 16 \end{pmatrix} = \begin{pmatrix} 48 & 3 \\ 515 & 17 \end{pmatrix}.
\]

Using the formulas in Theorem 1

\[
a_5 = \frac{515(-5) - 1(17)}{16(-5) - 1(1)} = 32 \quad \text{and} \quad b_4 = \frac{16(17) - 515(1)}{16(-5) - 1(1)} = 3,
\]

so \( P_6 = 32(1) - 31 = 1 \) and \( Q_6 = (499 - 1)/3 = 166 \), which shows that the continued fraction is, indeed, periodic. Thus,

\[
\sqrt{499} = \left[ \begin{array}{cccccc} 3 & 3 & 3 & 3 & 3 \\ -1 & 1 & -1 & 1 & 32 \end{array} \right]
\]

Given the algorithm’s use of Theorem 1, it is not guaranteed that \( a_{n_0+k} \) or \( b_{n_0+k-1} \) are integers. However, they have been integers in every case we have tried, which includes all values of \( D \) that are square-free, \( D \equiv 2, 3 \pmod{4} \), and \(-5000 \leq D \leq -5\). As we mentioned before, however, the continued fraction can be converted into one with integral partial numerators and denominators simply by clearing denominators. In some cases, \( b_{n_0+k-1} \) had prime factors besides \( p \), so one cannot necessarily convert the continued fraction generated from the algorithm into one with partial numerators that are always \( p \). In the case where \( b_{n_0+k-1} = -p \), one can factor out the \(-1\) and propagate it through the partial numerators and denominators of the next period,
cancelling it out with the $-1$ factor of $b_{n_0 + 2k - 1}$, and changing the signs of the partial denominators in between. This creates a period that is twice the size of the original, where all the partial numerators are $p$ and the second half of the partial denominators have the opposite sign of their counterparts in the first half of the period.

**Example 4.** Using the algorithm above to generate a continued fraction for $\sqrt{-5} \in \mathbb{Q}_3$, we get

\[
\sqrt{-5} = \left[ \begin{array}{cc}
3 & -3 \\
1 & 2 \\
\end{array} \right] \\
= \left[ \begin{array}{cccc}
3 & 3 & -3 & -3 \\
1 & 2 & -2 & 2 \\
\end{array} \right] \\
= \left[ \begin{array}{cccc}
3 & 3 & 3 & -3 \\
1 & 2 & 2 & -2 \\
\end{array} \right] \\
= \left[ \begin{array}{cccc}
3 & 3 & 3 & 3 \\
1 & 2 & 2 & -2 \\
\end{array} \right]
\]

In general, this transformation changes a continued fraction of the form

\[
\left[ \begin{array}{cccc}
p & \cdots & p & -p \\
a_0 & a_1 & \cdots & a_{n-1} & a_n \\
\end{array} \right]
\]

into the equal continued fraction

\[
\left[ \begin{array}{cccccccc}
p & \cdots & p & p & p & \cdots & p & p \\
a_0 & a_1 & \cdots & a_{n-1} & -a_n & -a_1 & \cdots & -a_{n-1} & a_n \\
\end{array} \right].
\]

We observe this type of symmetry, which we call *negative symmetry*, as a natural result of a continued fraction algorithm defined in Section 3.2.

### 2.1.2 The $\ell$-Square Algorithm

In this section we present a general continued fraction algorithm, depending on a positive integer $\ell$, so that for each square root of an integer and sufficiently large $\ell$ the resulting continued fraction is periodic. Let $\ell$ be a positive integer, $\alpha \in \mathbb{Z}_p^\times$, define
$P_{-1} = 0$, and for now let $p > 2$. Then the partial quotients $a_n$ and $b_n$ are obtained from $\alpha_n$ and $P_{n-1}$ in the following way. If

$$\alpha_n = c_0 + c_1 p + c_2 p^2 + \cdots, \quad (2.6)$$

set

$$a_n = c_0, \quad P_n = a_n - P_{n-1},$$

$$b_n' = (\alpha_n - P_{n-1})^2 - P_n^2 = d_k p^k + d_{k+1} p^{k+1} + \cdots \quad (2.7)$$

$$b_n = d_k p^k + d_{k+1} p^{k+1} + \cdots + d_{k+\ell-1} p^{k+\ell-1},$$

where (2.6) and (2.7) are $p$-adic expansions with respect to some set of representatives, possibly different for $\alpha_n$ and $b_n'$.

To see that this is an ITCF we need to show that $k > 0$ and $v(\alpha_n - a_n) = v(b_n)$. The first part follows from

$$(\alpha_n - P_{n-1})^2 - P_n^2 = (\alpha_n - P_{n-1})^2 - (a_n - P_{n-1})^2 = (\alpha_n - a_n)(\alpha_n + a_n - 2P_{n-1}), \quad (2.8)$$

since $v(\alpha_n - a_n) > 0$. To verify that $v(\alpha_n - a_n) = v(b_n)$ we just need to check, given (2.8) and $v(b_n) = v(b_n')$, that $v(\alpha_n + a_n - 2P_{n-1}) = 0$ for $n \geq 0$. Since $p > 2$ this holds for $n = 0$. To show that this holds for $n > 0$ we prove by induction that $\alpha_n \equiv a_n \equiv 2a_0 \pmod{p}$ and $P_{n-1} \equiv a_0 \pmod{p}$ for $n \geq 1$. Given (2.8), we can write $\alpha_{n+1}$ as

$$\alpha_{n+1} = \frac{b_n}{\alpha_n - a_n} = \frac{(\alpha_n - P_{n-1})^2 - P_n^2 - d_{k+\ell} p^{k+\ell} - d_{k+\ell+1} p^{k+\ell+1} - \cdots}{\alpha_n - a_n} = \frac{(\alpha_n - a_n)(\alpha_n + a_n - 2P_{n-1}) - p^{k+\ell}(d_{k+\ell} + d_{k+\ell+1} p + \cdots)}{\alpha_n - a_n} = (\alpha_n + a_n - 2P_{n-1}) + (\alpha_n - a_n)^{-1}\beta, \quad (2.9)$$

where $\beta \in \mathbb{Z}_p$ has $v(\beta) \geq k + \ell > k$. 
For \( n = 0 \) we have \( k = v(\alpha_0 - a_0) \) since \( k = v(\alpha_0^2 - a_0^2) = v(\alpha_0 - a_0) + v(\alpha_0 + a_0) \), and \( v(\alpha_0 + a_0) = 0 \) since \( p \) is odd. Thus, reducing (2.9) modulo \( p \) we get \( \alpha_1 \equiv \alpha_0 + a_0 \equiv 2a_0 \pmod{p} \). By definition, \( P_0 = a_0 - P_{-1} = a_0 \), so the first case is true. Now suppose that \( \alpha_n \equiv a_n \equiv 2a_0 \pmod{p} \) for some \( n \geq 1 \). By (2.8), \( v(\alpha_n - a_n) \leq k \), so reducing (2.9) for \( \alpha_{n+1} \) above modulo \( p \) give \( \alpha_{n+1} \equiv 2a_0 \pmod{p} \) and \( P_n \equiv a_n - P_{n-1} \equiv a_0 \pmod{p} \).

By induction we have \( \alpha_n \equiv a_n \equiv 2a_0 \pmod{p} \) and \( P_{n-1} \equiv a_0 \pmod{p} \) for all \( n \geq 1 \). Then \( v(\alpha_n + a_n - 2P_{n-1}) = 0 \) for \( n \geq 1 \) and \( v(\alpha_0 + a_0) = 0 \), since \( p \) is odd, so \( v(\alpha_n - a_n) = v(b_n) \) and the continued fraction produced by the algorithm is an ITCF.

The algorithm does not limit what representatives are chosen for \( \alpha_n \) or \( b'_n \) in their series representation. If the set of representatives for the \( \alpha_n \) are fixed throughout the algorithm, then by what we have proven, the first partial denominator is some \( a_0 \) and each partial denominator after that is the representative of \( 2a_0 \).

**Example 5.** We get the following continued fractions for \( \sqrt{2} \in \mathbb{Q}_7 \) with various sets of representatives for the \( \alpha_n \), where \(-1\) is one of the representatives for the expansion of the \( b'_n \), and where \( \ell = 1 \):

\[
\begin{bmatrix}
-7 & -7 & -7 & -7 & \cdots \\
3 & 6 & 6 & 6 & \cdots \\
-7 & -14 & -7 & -14 & \cdots \\
3 & -1 & -1 & -1 & \cdots \\
17 & 20 & 20 & 20 & \cdots 
\end{bmatrix}
\begin{align*}
0 & \leq c_i \leq p - 1 \\
p/2 & < c_i < p/2 \\
2p & \leq c_i \leq 3p - 1
\end{align*}
\]

The first two appear to be periodic, and we prove here that the first case is indeed periodic.

**Theorem 16.** Let \( D \) be a non-square integer not divisible by \( p \), \( p > 2 \), that has a square root in \( \mathbb{Q}_p \) and let \( \{0, \ldots, p - 1\} \) be coefficients in the \( p \)-adic expansions of the \( \alpha_n \). If the set of representatives for the \( b'_n \) and \( \ell \) are chosen so that \( b_0 = b'_0 = D - a_0^2 \)
then the $\ell$-square algorithm produces the continued fraction

$$\sqrt{D} = \left[ \frac{b_0}{a_0 \, 2a_0} \right],$$

where $\sqrt{D}$ is the square root with $0 < a_0 < p/2$. In particular, if $D < a_0^2$ we can take $\{-(p-1), \ldots, -1, 0\}$ as the set of representatives for the $b'_n$, and otherwise $\{0, 1, \ldots, p-1\}$, with $\ell > \lceil \log_p(|D - a_0^2|) \rceil - v(D - a_0^2)$.

**Proof.** If $b_0 = b'_0$ then since $b'_0 = \alpha_0^2 - a_0^2 = D - a_0^2$ we have

$$\alpha_1 = \frac{b_0}{a_0 - a_0} = \alpha_0 + a_0,$$

which shows that $a_1 = 2a_0$. Then by what has been shows before, $a_n = 2a_0$ for $n \geq 1$, and so $P_n = a_0$ for $n \geq 0$. Also, we then have

$$b'_1 = (\alpha_1 - a_0)^2 - a_0^2 = \alpha_0^2 - a_0^2 = b'_0 = b_0,$$

so $b_1 = b_0$. Suppose that $\alpha_n = \alpha_0 + a_0$ and $b_n = b_0$ for some $n \geq 1$. Then

$$\alpha_{n+1} = \frac{b_n}{\alpha_n - a_n} = \frac{b_0}{\alpha_0 - a_0} = \alpha_0 + a_0,$$

and $b'_{n+1} = b_{n+1} = b_0$ as before. Thus, the continued fraction is as stated. \[\square\]

This theorem can be proven in isolation by simply observing that $\alpha_0^2 - a_0^2 = (\alpha_0 - a_0)(\alpha_0 + a_0) = b$ is some integer divisible by $p$, and that dividing by $(\alpha_0 + a_0)$ and then adding $a_0$ we get

$$\alpha_0 = a_0 + \frac{b}{a_0 + a_0}.$$

This construction works for real numbers as well, as long as $D > 0$, of course.

### 2.2 Simple Rational Type Continued Fractions

We define a class of simple $p$-adic continued fraction that generalize the definition of Ruban [Rub70], and include the $p$-adic continued fractions studied by Browkin [Bro78,
Bro01], Laohakosol [Lao85], Wang [Wan85], Bedocchi [Bed88, Bed89, Bed90, Bed93], and Kacha [Kac99]. These continued fraction differ from Schneider type continued fractions in that they are simple, the partial quotients consisting of rational numbers whose denominators are divisible by powers of $p$.

**Definition 7.** Let $\alpha \in \mathbb{Q}_p \setminus p\mathbb{Z}_p$. A continued fraction of the form (1.1) or (1.2) is a simple rational type continued fraction (SRTCF) for $\alpha$ if $a_i \in \mathbb{Q}$, $b_i = 1$, and $v(\alpha_i - a_i) = e_i > 0$ for $i \geq 0$. If $\alpha \in p\mathbb{Z}_p$ the requirements are the same, except that $a_0 = 0$.

Since an SRTCF is simple, we denote it by $[a_0; a_1, a_2, \ldots]$. This definition is simply motivated by the desire to have a simple continued fraction representation that provides rational approximations to $p$-adic numbers. The condition that $v(\alpha_i - a_i) > 0$ ensures convergence, so we cannot restrict the partial quotients to the integers. Suppose that $a_i = r_i/s_i \neq 0$ is reduced. If $p \mid r_i$ then $p \nmid s_i$ and $v(\alpha_i - r_i/s_i) = v(\alpha_i) \leq 0$, so $p \nmid r_i$. Since $v(\alpha_i - r_i/s_i) > 0$ we must have $v(s_i) = -v(a_i) = -v(\alpha_i)$. This implies that

$$e_i = v(\alpha_i - a_i) = v\left(\frac{1}{\alpha_{i+1}}\right) = -v(a_{i+1})$$

for $i \geq 0$. For $a_0 \neq 0$ we define $e_{-1} = -v(a_0)$.

If $v(\alpha) \leq 0$ then, by induction, $v(A_i) = -(e_{-1} + \cdots + e_{i-1})$ and $v(B_{i+1}) = -(e_0 + \cdots + e_i)$ for $i \geq 0$, and $v(B_0) = v(1) = 0$. Otherwise, if $v(\alpha) > 0$, then $v(A_{i+1}) = -(e_1 + \cdots + e_i)$ and $v(B_i) = -(e_0 + \cdots + e_{i-1})$ for $i \geq 1$, $v(A_0) = +\infty$, $v(A_1) = 0$, and $v(B_0) = 0$. We can now prove analogues of Theorem 14 and Theorem 15, which are also more general versions of two theorems proved by Browkin in [Bro78].

**Theorem 17.** The convergents of a SRTCF for $\alpha \in \mathbb{Q}_p$ converge to $\alpha$.

**Proof.** Suppose $\alpha$ is represented by an SRTCF, using the notation above. That is, suppose we have sequences $(\alpha_n)_{n \geq 0}$, $(a_n)_{n \geq 0}$, and $(b_n)_{n \geq 0}$ that satisfy $\alpha_{n+1} = b_n/(\alpha_n - a_n)$ and the conditions in the definition of an SRTCF. We know from the
previous paragraph that the convergents exist, since $v(B_i) < \infty$ for $i \geq 0$. Assume without loss of generality that $v(\alpha) \leq 0$. By the same logic as in the proof of Theorem 14,
\[
\left| \frac{\alpha - A_n}{B_n} \right|_p \leq \frac{1}{|(\alpha_{n+1}B_n + B_{n-1})B_n|_p} = p^{-(2e_0+\cdots+e_{n-1})+e_n} \leq p^{-(2n+1)},
\]
which goes to zero.

The next theorem shows that a SRTCF expansion has convergents that converge to a $p$-adic number.

**Theorem 18.** If a simple continued fraction has rational partial quotients $a_i = r_i/s_i \neq 0$, $(r_i, s_i) = 1$, such that $p \mid s_i$ for $i \geq 0$ then the continued fraction converges to some $\alpha \in \mathbb{Q}_p \setminus p\mathbb{Z}_p$. If the condition holds for $i \geq 1$ and $a_0 = 0$ then the continued fraction converges to some $\alpha \in p\mathbb{Z}_p$. Furthermore, the continued fraction is an SRTCF for $\alpha$, in either case.

**Proof.** Define $e_i = -v(a_{i+1})$ for $i \geq 0$ and $e_{-1} = -v(a_0)$ if $a_0 \neq 0$. Then all the relations in the paragraph preceding Theorem 17 hold regarding the convergents of the continued fraction. In particular, all the convergents exist, and by (2.3) we have
\[
\left| \frac{A_n}{B_n} \right|_p \leq p^{-(2n+1)},
\]
for $n \geq 1$. Thus, as an immediate consequence of the ultrametric inequality, $(A_n/B_n)$ is a Cauchy sequence and converges to some $\alpha \in \mathbb{Q}_p$. Suppose $a_0 \neq 0$. Then
\[
v(\alpha) = \lim_n v(A_n/B_n) = \lim_n e_{-1} = -e_{-1} < 0,
\]
so $\alpha \in \mathbb{Q}_p \setminus p\mathbb{Z}_p$. If $a_0 = 0$ then $v(A_n/B_n) = e_0$, so $\alpha \in p\mathbb{Z}_p$. To show that the continued fraction is a simple continued fraction for $\alpha$, we first must show that $v(\alpha_0 - a_0) = e_0$. Suppose that $a_0 \neq 0$. Then
\[
v(A_1/B_1 - a_0) = v((a_0a_1 + 1)/a_1 - a_0) = -v(a_1) + v(1) = e_0.
\]
Assume that $v(A_k/B_k - a_0) = e_0$ for $1 \leq k \leq n$, so $v(A_k - a_0 B_k) = e_0 + v(B_k)$. Then

$$
v(A_{n+1}/B_{n+1} - a_0) = -v(B_{n+1}) + v(A_{n+1} - a_0 B_{n+1})
= -v(B_{n+1}) + v(a_{n+1}(A_n - a_0 B_n) + (A_{n-1} - a_0 B_{n-1}))
= -v(B_{n+1}) - e_n + e_0 + v(B_n)
= e_0,
$$
so $v(\alpha_0-a_0) = \lim_{n \to \infty} v(A_n/B_n-a_0) = e_0$ by induction. To show that $v(\alpha_n-a_n) = e_n$ it suffices to show by induction that $\alpha_n = [a_n; a_{n+1}, \ldots]$ and use the same argument as above, which is straightforward.

\[\square\]

### 2.3 Numerical Results on Browkin’s Algorithms

Browkin’s second paper [Bro01] was the starting point for this research, and so we have double checked and extended the numerical results of Browkin. Before discussing the results, we define the three other algorithms given in his paper. The first algorithm is BCF1, which was also defined in his first paper [Bro78]. Each algorithm uses maps analogues to the Browkin map used in Definition 4 to define BCF1s. We define these maps here, which are from $\mathbb{Q}_p$ to $\mathbb{Q}_p$, and defined from the $p$-adic expansion

$$\alpha = \sum_{k=n}^{\infty} c_k p^k,$$

where $c_k \in \{- (p - 1)/2, \ldots, (p - 1)/2\}$. We use a different notation from Browkin, so that the subscripts on the maps will identify to which algorithm they belong.

The following two maps are used as a part of all three of the remaining Browkin algorithms:

$$s(\alpha) = \sum_{k=n}^{0} c_k p^k \quad \text{and} \quad t(\alpha) = \sum_{k=n}^{-1} c_k p^k.$$

Each of these has a variant that takes into account the sign of the result:

$$s'(\alpha) = s(\alpha) - p \text{ sgn}(s(\alpha)) \quad \text{and} \quad t'(\alpha) = t(\alpha) - \text{sgn}(t(\alpha)).$$
Browkin’s second algorithm uses the map

\[ t_{BCF2}(\alpha) = \begin{cases} t(\alpha) & \text{if } v(\alpha - t(\alpha)) = 0 \\ t'(\alpha) & \text{otherwise,} \end{cases} \]

in its definition, which is the following, where \( s_{BCF2} = s \).

### 2.3.1 Definitions of Browkin’s Continued Fraction Algorithms

**Definition 8.** The second Browkin continued fraction (BCF2) for \( \alpha \in \mathbb{Q}_p \) is constructed in the following way:

1. \( \alpha_0 = \alpha, \alpha_{n+1} = b_n/(\alpha_n - a_n) \)

2. \( b_n = 1 \)

3. \( a_n = s_{BCF2}(\alpha_n) \) if \( n \) is even

4. \( a_n = t_{BCF2}(\alpha_n) \) if \( n \) is odd

for \( n \geq 0 \), as long as \( \alpha_n \neq a_n \). If \( \alpha_n = a_n \) then the continued fraction terminates with \( a_n \) as its final partial quotient.

When \( n \) is odd \( v(\alpha_n - a_n) = 0 \), so this continued fraction is not quite an RTCF or SRTCF. Browkin proved that a continued fraction defined in this way converges, and it is clear that by relaxing the condition that \( v(\alpha_n - a_n) > 0 \) for all \( n \geq 0 \), in the definition of RTCF and SRTCF, to just requiring that \( v(\alpha_n - a_n) \geq 0 \) for \( n \geq 0 \) and \( v(\alpha_n - a_n) > 0 \) infinitely often the resulting continued fraction has the convergence properties of Theorem 17 and Theorem 18. Browkin does not give a motivation for this definition, but it results in continued fractions that are periodic more often than BCF1s. An interesting question about BCF2s is whether or not every BCF2 of a rational number is finite.
The last two algorithms Browkin defined apply only to quadratic irrationals. Suppose \( \alpha = \frac{p + \sqrt{D}}{q} \in \mathbb{Q}_p \), \( P, Q \in \mathbb{Z} \), \( D \in \mathbb{Q} \), \( \sqrt{D} \notin \mathbb{Q} \). Then we define the following maps:

\[
\begin{align*}
  s_{BQCF1}(\alpha) &= \begin{cases} 
    s(\alpha) & \text{if } \text{sgn}(s(\alpha)) = \text{sgn}(PQ) \\
    s'(\alpha) & \text{otherwise},
  \end{cases} \\
  \overline{t_1}(\alpha) &= \begin{cases} 
    t(\alpha) & \text{if } \text{sgn}(t(\alpha)) = \text{sgn}(PQ) \\
    t'(\alpha) & \text{otherwise},
  \end{cases}
\end{align*}
\]

which is assuming \( PQ \neq 0 \), and

\[
\begin{align*}
  s_{BQCF2}(\alpha) &= \begin{cases} 
    s(\alpha) & \text{if } \left| \frac{p}{q} - s(\alpha) \right| < \left| \frac{p}{q} - s'(\alpha) \right| \\
    s'(\alpha) & \text{otherwise},
  \end{cases} \\
  \overline{t_2}(\alpha) &= \begin{cases} 
    t(\alpha) & \text{if } \left| \frac{p}{q} - t(\alpha) \right| < \left| \frac{p}{q} - t'(\alpha) \right| \\
    t'(\alpha) & \text{otherwise},
  \end{cases}
\end{align*}
\]

where \( | \cdot | \) is the real absolute value. If \( s(\alpha) \neq 0 \) then \( |s(\alpha)| < p \), so then the signs of \( s(\alpha) \) and \( s'(\alpha) \) are opposite. Thus, \( s_{BQCF1}(\alpha) \) chooses to use the map whose result will have the same sign as \( PQ \), when \( PQ \neq 0 \). The analogous statement for \( \overline{t_1}(\alpha) \) is true, as well.

The two algorithms for quadratic irrationals are defined in the same way as the algorithm for BCF2s, but \( s_{BCF2} \) and \( t_{BCF2} \) are replaced by \( s_{BCQF_n} \) and \( t_{BQCF_n} \), respectively, where \( n = 1, 2 \). The maps \( t_{BQCF_n} \), \( n = 1, 2 \), are defined by

\[
t_{BQCF_n} = \begin{cases} 
    t(\alpha) & \text{if } v(\alpha - t'(\alpha)) > 0 \\
    t'(\alpha) & \text{if } v(\alpha - t(\alpha)) > 0 \\
    \overline{t_n} & \text{otherwise}.
  \end{cases}
\]

Thus, Browkin’s two quadratic algorithms are defined as follows.

**Definition 9.** The first Browkin quadratic continued fraction (BQCF1) and the second Browkin quadratic continued fraction (BQCF2) for a quadratic irrational \( \alpha \in \mathbb{Q}_p \) are constructed in the following way:

1. \( \alpha_0 = \alpha, \alpha_{n+1} = b_n/(\alpha_n - a_n) \)
2. \( b_n = 1 \)

3. \( a_n = s_{\text{BQCF}k}(\alpha_n) \) if \( n \) is even

4. \( a_n = t_{\text{BQCF}k}(\alpha_n) \) if \( n \) is odd,

where \( k = 1, 2 \) and \( n \geq 0 \), as long as \( \alpha_n \neq a_n \). If \( \alpha_n = a_n \) then the continued fraction terminates with \( a_n \) as its final partial quotient.

2.3.2 Analysis and Extension of Browkin’s Numerical Results

For a small number of \( p \)-adic fields, Browkin performed calculations to determine how often he could observe periodicity with his four algorithms (BCF1, BCF2, BQCF1, and BQCF2). Browkin found that periodicity was observed more often when using the quadratic algorithms, periodicity was observed more for BCF2s than BCF1s, and that periodicity was observed more for BQCF2 than BQCF1. In fact, it appeared that in some \( p \)-adic fields the BQCF2 algorithm always produced periodicity. We repeated all of Browkin’s calculations and determined, numerically, the \( p \)-adic fields for which BQCF2s appear to always produce periodic continued fractions.

For the calculations involving BCF1s our results agreed. However, there were some discrepancies between Browkin’s results and our results for the three other algorithms. Browkin first considered \( \sqrt{D} \) for \( 1 \leq d \leq 100 \) in \( \mathbb{Q}_5 \). Our first difference was for the BCF2 of \( \alpha = \alpha_0 = \sqrt{34} \). We agreed up through

\[
\alpha_5 = 2 \cdot 5^{-2} + 4 \cdot 5^{-1} + 4 + 2 \cdot 5 + 2 \cdot 5^2 + 5^3 + 5^4 + 3 \cdot 5^5 + 4 \cdot 5^6 + 3 \cdot 5^7 + \cdots,
\]

but then Browkin got a different value for \( a_5 \). We calculate that \( a_5 = 22/25 \) and he calculated that \( b_5 = -28/25 \). Since 5 is odd, we need to use \( t_{\text{BCF}2}(\alpha_5) \) to calculate \( a_5 \). Since \( t(\alpha_5) = 2 \cdot 5^{-2} - 5^{-1} = -3/25 \) and \( v(\alpha_5 - t(\alpha_5)) = 1 \),

\[
t_{\text{BCF}2}(\alpha_5) = t'(\alpha_5) = -\frac{3}{25} - (-1) = \frac{22}{25}.
\]
We conclude, therefore, that Browkin’s PARI/GP code had some sort of bug. Here is a summary of all the other differences between our results for BCF2s in \( \mathbb{Q}_5 \): smaller period for \( \sqrt{34} \), no period observed for \( \sqrt{39} \), smaller and later starting period for \( \sqrt{54} \), smaller period for \( \sqrt{56} \), longer period for \( \sqrt{69} \), no period observed for \( \sqrt{99} \), and we observed a period for \( \sqrt{91} \), namely

\[
\sqrt{91} = \left[ 1, -\frac{1}{5}, 1, \frac{2}{5}, 2, \frac{14}{25}, -1, -\frac{4}{5}, 1, -\frac{4}{5}, 1, \frac{2}{5}, -\frac{2}{5}, 1, \frac{8}{25}, 1, -\frac{2}{5}, 2, \frac{1}{5} \right].
\]

For BQCF1 and BQCF2, the only difference we had in \( \mathbb{Q}_5 \) was for \( \sqrt{39} \), for which we calculated a different period length and start of the period.

In \( \mathbb{Q}_{23} \) our results agreed with Browkin’s, except that Browkin says the longest period for a BCQF2 of \( \sqrt{D} \), \( 1 \leq D \leq 500 \) is 112, which occurs for \( \sqrt{462} \). We found that this was the second longest period, and that the BQCF2 for \( \sqrt{404} \) had the longest period, with a length of 128. The extent of Browkin’s calculations for \( \mathbb{Q}_{23} \) was calculating the BCF1 of \( \sqrt{D} \) for \( 1 \leq D \leq 200 \)—for which a period was observed (after 1000 terms in my calculations) in only the three cases \( D = 75, 98, 167 \)—and calculating the BQCF2 of \( \sqrt{D} \) for \( 1 \leq D \leq 500 \), for which a period was observed 160 out of 219 cases.

In \( \mathbb{Q}_{21961} \) our results agreed, in that the only values of \( D \), \( 1 \leq D \leq 500 \), for which a period in the BQCF2 of \( \sqrt{D} \) was observed after 1000 terms were \( D = 3, 57, 178, 228, 240, 363 \). The only difference, which must simply be a typo in Browkin’s paper, was that we calculated that

\[
\sqrt{178} = \left[ 210, -\frac{210}{21961}, 420 \right],
\]

while Browkin reports the continued fraction as

\[
\sqrt{178} = \left[ 210, -\frac{2120}{21961}, 420 \right].
\]
2.3.3 Periodicity Results for Browkin’s Second Quadratic Algorithm

In addition to repeating the calculations done by Browkin, we determined the values of $p$ for which the BQCF2 algorithm always produces periodic continued fractions for $\sqrt{D} \in \mathbb{Q}_p$, $D \in \mathbb{Z}$, where $D$ is in some large range. For $p = 3, 5, 7, 11, 13$, the BQCF2 of $\sqrt{D} \in \mathbb{Q}_p$ was periodic for all $|D| \leq 10,000$. For $p = 17$, there were 51 values of $D$ between 0 and 1,000 for which the end of a period was not observed after 2,000 partial quotients. For the smallest such $D$, $D = 188$, no period was observed after 20,000 terms. Since Browkin did not check the fields $\mathbb{Q}_p$ for $5 < p < 23$, the first example he gives of a square root for which not period has been observed for the BQCF2 is $\sqrt{93} \in \mathbb{Q}_{23}$. Given the results of Browkin for $\mathbb{Q}_p$ with $p = 23, 257, 21961$, numerically, the BQCF2 algorithm produces fewer periodic continued fractions for $\sqrt{D}$ as $p$ gets larger.
We define a class of $p$-adic continued fractions that are similar to Schneider’s definition [Sch70] in that all partial numerators are powers of $p$, and all partial denominators (except possibly the first) are integers not divisible by $p$. For these types of continued fractions, the power of $p$ in the $i$th partial numerator is the degree to which the $i$th convergent is a better approximation than the $(i - 1)$st convergent.

**Definition 10.** Let $\alpha \in \mathbb{Z}_p^\times$. A continued fraction of the form (1.1) or (1.2) is a **Schneider type continued fraction** (STCF) for $\alpha$ if $a_i, b_i \in \mathbb{Z}, v(a_i) = 0, b_i = p^{e_i},$ and $v(\alpha_i - a_i) = e_i > 0$ for $i \geq 0$. If $\alpha \in \mathbb{Q}_p \setminus \mathbb{Z}_p^\times$, then the requirements are the same, except that $a_0 = 0$ and $e_0 = v(\alpha)$. In particular, it may happen that $e_0 < 0$.

To simplify the notation, an STCF is denoted by

$$\begin{bmatrix} e_0 & e_1 & \cdots \\ a_0 & a_1 & a_2 & \cdots \end{bmatrix} = \begin{bmatrix} p^{e_0} & p^{e_1} & \cdots \\ a_0 & a_1 & a_2 & \cdots \end{bmatrix}.$$ 

By Theorem 14 and Theorem 15 we know that an STCF for a $p$-adic number converges to it, and that any continued fraction with $a_i, b_i \in \mathbb{Z}, v(a_i) = 0, b_i = p^{e_i},$ and $e_i > 0$ for all $i \geq 0$ is an STCF for some $p$-adic unit. Likewise, if a continued fraction has $a_i, b_i \in \mathbb{Z}, v(a_i) = 0, b_i = p^{e_i},$ and $e_i > 0$ for all $i \geq 1, a_0 = 0$ and $e_0 \neq 0$, then the continued fraction is an STCF for a non-unit in $\mathbb{Q}_p$.

The only STCF that exists in the literature is Schneider’s original definition of a $p$-adic continued fraction, the SCF defined in Section 1.2.1. Although natural, the continued fractions do not possess structural properties analogues to real continued fractions. In Corollary 3 we show, as Bundushuch [Bun77] did originally, that some rational numbers have an infinite (periodic) SCF. Also, periodicity for square roots is rare. Using Tilborghs’ necessary and sufficient condition for periodicity of square roots...
roots, Theorem 8, we calculated the first few values of $D$ for which $\sqrt{D}$ has a periodic SCF in $\mathbb{Q}_p$, for $p \leq 19$. The results are displayed in Figure 3.

The vertical axis gives the values of $D$ and the horizontal axis indicates the integer’s ordinal value among the values of $D$ with a periodic square root. For example, 20 is the first integer whose square root has a periodic SCF in $\mathbb{Q}_{19}$, and 1,303,235 is the 167th.

The plateaus we have checked can be explained by the following proposition, mentioned in [dW88].

**Proposition 5.** If $D = e^2 + dp^k$ where $1 \leq e \leq \frac{1}{2}(p - 1)$ and $d|2e$, then $\sqrt{D}$ has a periodic SCF, with period one if $d = 1$ and period two if $d > 1$.

For example, the plateau between 138 and 146 for $p = 19$ is $D = e^2 + dp^k$ for...
\[ d = 2, \ k = 4, \text{ and } 1 \leq e \leq 9. \]

### 3.1 Finiteness of Continued Fractions for Rational Numbers

The continued fractions defined by Schneider do not have the property that all rational numbers have finite continued fractions. Those rational numbers without a finite SCF were classified by Bundschuh [Bun77]. We give here a condition on the partial quotients, \( a_n \), that results in finite continued fractions for rational numbers, and has Bundschuh’s result as a corollary.

Suppose \( \alpha = R/S \in \mathbb{Q} \), where \( R, S \in \mathbb{Z} \) and \( S > 1 \). Define sequences of integers, \( R_n \) and \( S_n \), by \( R_0 = R \), \( S_0 = S \), and

\[
R_{n+1} = \text{sgn}(R_n - a_n S_n)S_n \tag{3.1}
\]

\[
S_{n+1} = \frac{1}{p^{e_n}} |R_n - a_n S_n| \tag{3.2}
\]

when \( n > 0 \) and \( \alpha_{n+1} \) is defined. Then we can see by induction that the \( n \)th remainder is given by \( \alpha_n = R_n/S_n \). This is true for \( n = 0 \) by definition, so assume that \( \alpha_n = R_n/S_n \) and \( \alpha_{n+1} \) is defined. Then

\[
\alpha_{n+1} = \frac{p^{e_n}}{\alpha_n - a_n} = \frac{p^{e_n}}{R_n/S_n - a_n} = \frac{p^{e_n} S_n}{R_n - a_n S_n} = \frac{\text{sgn}(R_n - a_n S_n) S_n}{p^{-e_n} |R_n - a_n S_n|} = \frac{R_{n+1}}{S_{n+1}},
\]

so \( \alpha_n = R_n/S_n \) for all \( n \) for which \( \alpha_n \) is defined. The fact that \( S_{n+1} \in \mathbb{Z} \) follows from the definition of \( \alpha_n \), \( a_n \), and \( e_n \). The denominators, \( S_n \), are always positive.

**Lemma 2.** Suppose \( \alpha \in \mathbb{Q} \cap \mathbb{Z}_p \), \( |a_n| < p \) for all \( n \geq 0 \), \( S_{n-1} \neq S_n \), and \( S_n < S_{n+1} \) for some \( n > 0 \). Then \( S_{n+2} < S_{n+1} \) and \( S_{n+1} < S_{n-1} \).
Proof. To see that $S_{n+2} < S_{n+1}$, we have by definition that

\[
S_{n+2} = \frac{1}{p^{e_{n+1}}} |R_{n+1} - a_{n+1}S_{n+1}| \\
= \frac{1}{p^{e_{n+1}}} |\text{sgn}(R_{n+1})S_n - a_{n+1}S_{n+1}| \\
\leq \frac{1}{p} (S_n + |a_{n+1}|)S_{n+1} \\
< \frac{1 + |a_{n+1}|}{p} S_{n+1} \\
\leq S_{n+1},
\]

since $S_n < S_{n+1}$ and $|a_n| \leq p - 1$.

Note that the above implies that $S_{n-1} \geq S_n$, since otherwise, $S_{n+1} < S_n$. Thus, $S_{n-1} > S_n$, so

\[
S_{n+1} = \frac{1}{p^{e_n}} |R_n - a_nS_n| \\
= \frac{1}{p^{e_n}} |\text{sgn}(R_n)S_{n-1} - a_nS_n| \\
\leq \frac{1}{p} (S_{n-1} + |a_n|S_n) \\
< \frac{1 + |a_n|}{p} S_{n-1} \\
\leq S_{n-1}.
\]

\[\square\]

Theorem 19. If $\alpha \in \mathbb{Q}$ has a Schneider type continued fraction with $|a_n| < p$ for all $n \geq 0$, then the continued fraction is finite or $\alpha_n = \pm 1$ for some $n$.

Proof. Without loss of generality, suppose that $\alpha \in \mathbb{Z}_p$. If $S_n = S_{n+1}$, then

\[
\alpha_{n+1} = R_{n+1}/S_{n+1} = \pm S_n/S_{n+1} = \pm 1,
\]

so the goal is to show that if $S_n \neq S_{n+1}$ for all $n \geq 0$ then the continued fraction is finite. Thus, suppose that $S_n \neq S_{n+1}$ for all $n \geq 0$. 


We first show, by induction, that $S_{n+k} < \max(S_n, S_{n+1})$ for $k \geq 2$. If $S_{n+2} > S_{n+1}$, then $S_{n+2} < S_n$ and $S_{n+1} < S_n$ by Lemma 2. If $S_{n+2} < S_{n+1}$ then $S_{n+2} < S_{n+1} \leq \max(S_n, S_{n+1})$. Now suppose the result holds for all $2 \leq \ell \leq k$ and consider $S_{n+k+1}$. If $S_{n+k+1} < S_{n+k}$ then the inequality holds for $k + 1$ by the induction hypothesis.

Otherwise, $S_{n+k+1} > S_{n+k}$ and so $S_{n+k+1} < S_{n+k-1}$ and $S_{n+k-1} \leq \max(S_n, S_{n+1})$, either by the induction hypothesis or because $n + k - 1 = n + 1$.

Suppose that the $n$ such that $S_n > S_{n-1}$ are enumerated by $N_1, N_2, \ldots$. By Lemma 2, $S_{N_{k+1}} < S_{N_k}$, so $N_{k+1} > N_k + 1$. If $N_{k+1} = N_k + 2$, then $S_{N_{k+1}} < S_{N_k}$ by Lemma 2, since $S_{N_{k+1}} = S_{N_k+2} > S_{N_k+1}$. If $N_{k+1} > N_k + 2$ then

$$S_{N_{k+1}} < \max(S_{N_{k+1}}, S_{N_k+2}) = S_{N_{k+1}} < S_{N_k}.$$  

In any case, $S_{N_{k+1}} < S_{N_k}$, so

$$S_{N_1} > S_{N_2} > S_{N_3} > \cdots > 0$$

must be a finite sequence, and for some sufficiently large $N$, $S_n < S_{n-1}$ for all $n \geq N$. But then

$$S_{N-1} > S_N > S_{N+1} > \cdots > 0,$$

so the continued fraction must terminate. Thus, the continued fraction is finite or $S_n = S_{n+1}$ for some $n$, in which case $\alpha_{n+1} = \pm 1$.

From this theorem there are two corollaries describing how to generate finite continued fractions for rational numbers.

**Corollary 1.** Suppose $p > 2$, $\alpha \in \mathbb{Q}$ and $\alpha$ has an STCF with $|a_n| < p-1$ for all $n \geq 0$. Then the continued fraction is finite.

**Proof.** If $a_n = \pm 1$, then the continued fraction terminates with $\alpha_n$, since there is only one choice for $a_n$, which is $a_n = \alpha_n$. Thus, by Theorem 19 the continued fraction is finite.

$\square$
Corollary 2. Suppose $p = 2$ and for $\alpha \in \mathbb{Q}$ an STCF is generated by taking $a_n = 1$ when $n$ is even and $a_n = -1$ when $n$ is odd. Then the continued fraction is finite.

Proof. Suppose $\alpha_n = \pm 1$. If $n$ is even and $\alpha_n = 1$ or $n$ is odd and $\alpha_n = -1$, then $a_n = \alpha_n$ and the continued fraction is finite. If $n$ is even and $\alpha_n = -1$, then $\alpha_{n+1} = 2/(-2) = -1$ and $a_{n+1} = -1$, so the continued fraction terminates. Likewise, if $n$ is odd and $\alpha_n = 1$, then $\alpha_{n+1} = 2/2 = 1$ and $a_{n+1} = 1$, so the continued fraction terminates. By Theorem 19, the continued fraction is finite in any case. \qed

Observe that there are infinitely many ways to represent a rational number, $\alpha$, as an STCF. Assuming that $\alpha \in \mathbb{Z}_p^\times$, one may choose $a_0, \ldots, a_N$ as one desires, for some $N \geq 0$, as long as $\alpha_n \equiv a_n \pmod{p}$ for $0 \leq n \leq N$. Then $\alpha_{N+1} \in \mathbb{Q} \cap \mathbb{Z}_p^\times$, and if one chooses the partial quotients such that partial quotients satisfy the conditions of Corollary 1 or Corollary 2, then the continued fraction will terminate.

Corollary 3 (Bundschuh). Suppose $\alpha \in \mathbb{Q}_p$. Then $\alpha \in \mathbb{Q}$ if and only if the SCF for $\alpha$ is finite or is periodic with

$$\alpha = \left[\frac{p^{e_0}}{a_0} \quad \frac{p^{e_{n-1}}}{a_1} \quad \cdots \quad \frac{p}{a_n} \quad \frac{p}{p - 1}\right]$$

Proof. The SCF for $-1$ is purely periodic with $e_n = 1$ and $a_n = p - 1$ for all $n \geq 0$, so any SCF with this periodic part is rational. If $\alpha$ is rational but does not have a finite SCF, then by Theorem 19, $\alpha_n = \pm 1$ for some $n$. If $\alpha_n = 1$ then $a_n = 1$ and the continued fraction terminates, so $\alpha = \pm 1$. In that case, $a_n = p - 1$, $\alpha_n - a_n = -p$, $e_n = 1$, and $\alpha_{n+1} = p^{e_n}/(\alpha_n - a_n) = -1$, so the SCF has the prescribed form. \qed

3.2 Periodicity Proof for Quadratic Irrationals

In this section we define a continued fraction generating algorithm for quadratic irrationals that is designed with the goal of producing periodicity. Since an ITCF for a quadratic irrational will be periodic if and only if the values $|P_n|$ and $|Q_n|$ of the
remainders are bounded, this algorithm attempts to produce periodicity by choosing partial numerators that minimize $|P_n|$.

**Definition 11.** An NQCF (new quadratic continued fraction) for a quadratic irrational $\alpha \in \mathbb{Q}_p$ is an STCF where $a_n$ is chosen to minimize $|P_n|$. More specifically, the NQCF for $\alpha$ is generated by choosing $a_n$ and $b_n$ in the following way:

1. set $\overline{a_n} \in \{0, \ldots, p - 1\}$ so that $\overline{a_n} \equiv a_n \pmod{p}$
2. set $k = \left\lceil \frac{1}{p} \left( \frac{P_n}{Q_n} - \overline{a_n} \right) \right\rceil$
3. $a_n = \overline{a_n} + k'p$ and $b_n = p^e_n$ where $e_n = v(\alpha_n - a_n)$,

where $\lceil x \rceil$ is the nearest integer to $x$. The algorithm comes from the following. In order to make the continued fraction an STCF, ensuring convergence, the only restriction on $a_n$ is that $a_n \equiv \alpha_n \pmod{p}$. Thus, $a_n = \overline{a_n} + kp$ for some $k \in \mathbb{Z}$, where $\overline{a_n} \in \{0, \ldots, p - 1\}$. When choosing $a_n$, $P_n$ and $Q_n$ are given, so we choose $a_n$ to minimize $|P_{n+1}|$. By the familiar recurrence relation,

$$P_{n+1} = a_n Q_n - P_n = (\overline{a_n} + kp)Q_n - P.$$ 

Solving $P_{n+1} = 0$ for $k$ produces the desired value of $a_n$ if $k$ is integral, and otherwise, the integer closest to $k$ produces the desired $a_n$.

Since $P_{n+1} = (\overline{a_n}Q_n - P) + kpQ_n$ is chosen to be minimal, we know that $|P_{n+1}| \leq \frac{p}{2}|Q_n|$. This bound, along with the familiar recurrence relations between the $P_n$’s and $Q_n$’s, are the only facts used in the proofs of the following lemma and theorem (except for the case $p = 3$ and $|Q_0| \leq 2$). As such, the lemma and theorem hold for any STCF algorithm that keeps $|P_{n+1}| \leq \frac{p}{2}|Q_n|$. For example, one could choose $a_n$ so that $P_{n+1}$ is less than or equal to $\frac{p}{2}|Q_n|$ but as close to it as possible.

Recall that for a continued fraction of a quadratic irrational, the remainders are
given by formulas (1.5)-(1.7). That is,

\[ P_{n+1} = a_nQ_n - P_n \]
\[ Q_{n+1} = \frac{D - P_{n+1}^2}{p^{e_n}Q_n}. \]

We classify what forms \( P_n \) and \( Q_n \) can take, using methods similar to de Weger [dW88].

**Proposition 6.** For all \( n \geq 0 \), \( P_n, Q_n \in \frac{1}{Q_0} \mathbb{Z} \).

**Proof.** The proof proceeds by induction on \( n \). Since \( P_0, Q_0 \in \mathbb{Z} \), the claim holds for \( n = 0 \). Suppose \( P_k, Q_k \in \frac{1}{Q_0} \mathbb{Z} \) for \( k \geq n \). Since \( P_{n+1} = a_nQ_n - P_n \), \( P_{n+1} \in \frac{1}{Q_0} \mathbb{Z} \).

Decomposing \( D - P_{n+1}^2 \),

\[ D - P_{n+1}^2 = (\sqrt{D} - P_{n+1})(\sqrt{D} + P_{n+1}) \]
\[ = (\sqrt{D} + P_n - a_nQ_n)(\sqrt{D} + P_{n+1}) \]
\[ = (a_n - a_n)Q_n(\sqrt{D} + P_{n+1}), \]

we see that \( v(D - P_{n+1}^2) \geq v(p^{e_n}Q_n) \), so we simply need to show that

\[ Q_0Q_n \mid Q_0^2(D - P_{n+1}^2), \]

since

\[ Q_{n+1} = \frac{D - P_{n+1}^2}{p^{e_n}Q_n} = \frac{Q_0^2(D - P_{n+1}^2)}{p^{e_n}Q_0^2Q_n} = \frac{1}{Q_0} \left( \frac{Q_0^2(D - P_{n+1}^2)}{p^{e_n}Q_0Q_n} \right). \]

Then

\[ Q_0^2(D - P_{n+1}^2) = Q_0^2(D - P_n^2 + 2a_nP_nQ_n - a_n^2Q_n^2) \]
\[ = Q_0(Q_0(D - P_n^2) + Q_0Q_n(2a_nP_n - a_n^2Q_n)) \]
\[ = Q_0Q_n[Q_0(p^{e_n-1}Q_{n-1} + 2a_nP_n - a_n^2Q_n)] \]

is divisible by \( Q_0Q_n \), since the part in brackets is integral by the induction hypothesis. Thus, the proposition holds by induction. \( \square \)
The preceding proposition allows us to translate boundedness of the $P_n$ and $Q_n$ into periodicity results for most cases. Namely, suppose that given a quadratic irrational $\alpha = (P + \sqrt{D})/Q$ there is an algorithm that deterministically generates an integer $a$ such that $\alpha \equiv a \pmod{p}$. For example, taking the first $p$-adic digit in the standard $p$-adic expansion would be such an algorithm. These algorithms can generate STCFs for a quadratic irrational by applying the algorithm to the remainders. In these cases, the STCF is clearly periodic if and only if $(P_n, Q_n) = (P_m, Q_m)$ for some distinct $n, m \geq 0$, so the STCF is periodic exactly when there are only finitely many values for $(P_n, Q_n)$. By Proposition 6, $(P_n, Q_n)$ takes on only finitely many values exactly when $P_n$ and $Q_n$ are bounded. Thus, the primary strategy for proving that an STCF, formed by the kind of algorithm mentioned before, is periodic is to show that $P_n$ and $Q_n$ are bounded. To be more concise, we call this type of algorithm indiscriminant, since it depends only on the current remainder and does not take into account previous remainders, the parity of $n$, etc.

**Lemma 3.** The NQCF for $\alpha = \frac{P + \sqrt{-2}}{Q}$, $P, Q \in \mathbb{Z}$, $Q \neq 0$, in $\mathbb{Q}_3$ is periodic.

**Proof.** By Proposition 6 it is sufficient to prove that $Q_n$ and $P_n$ are bounded, which we do by induction on $n$. Since $a_n$ is chosen so that $|P_{n+1}|$ is minimal, and all the choices differ by a multiple of $3Q_n$, it follows that $|P_{n+1}| \leq \frac{3}{2}|Q_n|$. Thus, it suffices to show that $|Q_n|$ is bounded. For $|Q_0| > 2$ we show that $|Q_n| \leq |Q_0|$, which is clearly true for $n = 0$ and which we assume for $|Q_n|$. By (1.7)

$$|Q_{n+1}| \leq \frac{\frac{3}{2}Q_n^2 + 2}{3|Q_n|} = \frac{3}{4}|Q_n| + \frac{2}{3|Q_n|},$$

and $\frac{1}{|Q_0|} \leq |Q_n| \leq |Q_0|$. On this interval $f(x) = \frac{3}{4}x + \frac{2}{3x}$ and its second derivative are both positive, so the maximum absolute value is attained at one of the end points. If $f(x)$ has its maximum value at $x = \frac{1}{|Q_0|}$ then

$$|Q_{n+1}| \leq \frac{3}{4|Q_0|} + \frac{2}{3}|Q_0| \leq |Q_0|.$$
where the last inequality is true for $|Q_0| \geq \frac{3}{2}$, which we assume. If $f(x)$ has its maximum at $x = |Q_0|$ then

$$|Q_{n+1}| \leq \frac{3}{4}|Q_0| + \frac{2}{3|Q_0|} \leq |Q_0|,$$

where the last inequality is true for $|Q_0| \geq \frac{3\sqrt{2}}{2}$, which we assume. If $f(x)$ has its maximum at $x = |Q_0|$ then

$$|Q_{n+1}| \leq \frac{3}{4}|Q_0| + \frac{2}{3|Q_0|} \leq |Q_0|,$$

where the last inequality is true for $|Q_0| \geq \frac{3\sqrt{2}}{2}$, which is also covered by $|Q_0| > 2$.

Thus, the lemma is true for $|Q_0| > 2$.

Suppose $|Q_0| \leq 2$. Then either $|Q_1| > 2$, in which case $\frac{P_1 + \sqrt{-2}}{Q_1}$ has a periodic NQCF, and so $\alpha$ does also, or $|Q_1| \leq 2$ and $|P_1| \leq \frac{3}{2}|Q_0|$. Therefore, there are finitely many cases left to consider, which are as follows:

- $P = 0$ and $Q = \pm 1, \pm 2$

$$\sqrt{-2} = \begin{bmatrix} 3 & 3 \\ 1 & -2 \\ 2 & \end{bmatrix}_3, \quad -\sqrt{-2} = \begin{bmatrix} 3 & 3 \\ -1 & 2 \\ -2 & \end{bmatrix}_3$$

$$\frac{\sqrt{-2}}{2} = \begin{bmatrix} 3 & 3 & 3 \\ -1 & 1 & 2 \\ -2 & \end{bmatrix}_3, \quad -\frac{\sqrt{-2}}{2} = \begin{bmatrix} 3 & 3 & 3 \\ 1 & -1 & -2 \\ 2 & \end{bmatrix}_3$$

- $P = \pm 1$ and $Q = \pm 1$

$$1 + \sqrt{-2} = \begin{bmatrix} 3 & 3 \\ 2 & -2 \\ 2 & \end{bmatrix}_3, \quad -1 + \sqrt{-2} = \begin{bmatrix} 3 & 3 \\ 0 & -2 \\ 2 & \end{bmatrix}_3$$

$$1 - \sqrt{-2} = \begin{bmatrix} 3 & 3 \\ 0 & 2 \\ -2 & \end{bmatrix}_3, \quad -1 - \sqrt{-2} = \begin{bmatrix} 3 & 3 \\ -2 & 2 \\ -2 & \end{bmatrix}_3$$

- $P = \pm 1$ and $Q = \pm 2$

$$\frac{1 + \sqrt{-2}}{2} = \begin{bmatrix} 3 & 9 & 9 \\ 1 & -1 & -2 \\ 2 & \end{bmatrix}_3, \quad -\frac{1 + \sqrt{-2}}{2} = \begin{bmatrix} 3 & 9 & 9 \\ 0 & -1 & -2 \\ 2 & \end{bmatrix}_3$$

$$\frac{-1 - \sqrt{-2}}{2} = \begin{bmatrix} 3 & 9 & 9 \\ -1 & 1 & 2 \\ -2 & \end{bmatrix}_3, \quad \frac{1 - \sqrt{-2}}{2} = \begin{bmatrix} 3 & 9 & 9 \\ 0 & 1 & 2 \\ -2 & \end{bmatrix}_3$$
• $P = \pm 2$ and $Q = \pm 2$

$$
\frac{2+\sqrt{-2}}{2} = \begin{bmatrix} 3 & 3 & 3 \\ 0 & 1 & -2 & 2 \end{bmatrix}_3 \quad \quad \frac{-2+\sqrt{-2}}{2} = \begin{bmatrix} -2 & 1 & -2 & 2 \\ 3 & 3 & 3 \end{bmatrix}_3
$$

$$
\frac{-2-\sqrt{-2}}{2} = \begin{bmatrix} 3 & 3 & 3 \\ 0 & -1 & -2 & 2 \end{bmatrix}_3 \quad \quad \frac{2-\sqrt{-2}}{2} = \begin{bmatrix} 2 & -1 & -2 & 2 \\ 3 & 3 & 3 \end{bmatrix}_3
$$

• $P = \pm 3$ and $Q = \pm 2$

$$
\frac{3+\sqrt{-2}}{2} = \begin{bmatrix} 3 & 9 & 9 \\ 2 & -1 & -2 & 2 \end{bmatrix}_3 \quad \quad \frac{-3+\sqrt{-2}}{2} = \begin{bmatrix} -1 & -1 & -2 & 2 \\ 3 & 9 & 9 \end{bmatrix}_3
$$

$$
\frac{-3-\sqrt{-2}}{2} = \begin{bmatrix} 3 & 9 & 9 \\ -2 & 1 & 2 & -2 \end{bmatrix}_3 \quad \quad \frac{3-\sqrt{-2}}{2} = \begin{bmatrix} 1 & 1 & 2 & -2 \\ 3 & 9 & 9 \end{bmatrix}_3
$$

Thus, the lemma is true for all $P, Q \in \mathbb{Z}$, $Q \neq 0$.

The following theorem provides an analogue of Lagrange’s theorem in $\mathbb{Q}_2$ and $\mathbb{Q}_3$.

**Theorem 20.** NQCFs are periodic for quadratic irrationals in $\mathbb{Q}_p$ for $p = 2, 3$.

**Proof.** By Proposition 6 it is sufficient to prove that $Q_n$ and $P_n$ are bounded, which we do by induction on $n$. Since $a_n$ is chosen so that $|P_{n+1}|$ is minimal, and all the choices differ by a multiple of $pQ_n$, it follows that $|P_{n+1}| \leq \frac{p}{2}|Q_n|$. Thus, it suffices to show that $|Q_n|$ is bounded.

First suppose that $D < 0$, and assume that

$$
|Q_n| \leq \frac{|Q_0|}{p}(|D| + 1) = \frac{|Q_0|}{p}(1 - D). \quad (3.3)
$$

This is true for $|Q_0|$ when $p \leq 1 - D$, or $D \leq 1 - p$, which is $D \leq -1$ for $p = 2$ and $D \leq -2$ when $p = 3$. Since the largest negative integers with $p$-adic square roots are $-7$ for $p = 2$ and $-2$ for $p = 3$, we have (3.3) for $n = 0$ as the basis for the induction.

By (1.7), $|P_{n+1}| \leq \frac{p}{2}|Q_n|$ and the induction hypothesis,

$$
|Q_{n+1}| \leq \frac{1}{p} \frac{|D - p^2 Q_n^2|}{|Q_n|} = \frac{1}{p} \frac{|D|}{|Q_n|} - \frac{p^2}{4} |Q_n| \quad . \quad (3.4)
$$
Since $Q_n \in \frac{1}{Q_0} \mathbb{Z}$, we have $\frac{1}{|Q_0|} \leq |Q_n| \leq \frac{|Q_0|}{p} (1 - D)$. Let $f(x) = D/x - \frac{p^2}{4}x$. On the given interval for $|Q_n|$, $f(x)$ has a local maximum at $y = \frac{2}{p} \sqrt{|D|}$, $f(y) = -p \sqrt{|D|} < 0$ and $f''(x) < 0$, so $f(x)$ has maximum absolute value at one of the end points of the interval.

To get the $\frac{|Q_0|}{p} (1 - D)$ bound on $|Q_{n+1}|$, we will want the left endpoint to produce the largest maximum absolute value. Solving

$$f \left( \frac{1}{|Q_0|} \right) = f \left( \frac{|Q_0|}{p} (1 - D) \right)$$

for $D$ shows that $f(x)$ has the largest absolute value at $\frac{1}{|Q_0|}$ except when $D$ is strictly between

$$d_1 = \frac{p}{-4 + p} \text{ and } d_2 = \frac{-p}{Q_0^2} + 1.$$

For $p = 2$, $d_1 = -1$ and $-1 \leq d_2 < 1$. Since the largest negative integer with a 2-adic square root is $D = -7$, we may always assume $f(x)$ has the largest absolute value at $\frac{1}{|Q_0|}$ for $p = 2$. For $p = 3$, $d_1 = -3$ and $-2 \leq d_2 < 1$. Thus, we will consider $D = -2$ separately, and assume $D \leq -5$ for now. Since $f(x)$ has largest absolute value at $\frac{1}{|Q_0|}$, substituting $\frac{1}{|Q_0|}$ for $|Q_n|$ in (3.4) gives

$$|Q_{n+1}| \leq \frac{1}{p} |Q_0|D - \frac{p^2}{4|Q_0|} = \frac{|Q_0|}{p} \left| \left( \frac{p}{2|Q_0|} \right)^2 - D \right| .$$

If $p = 2$, then $(p/2|Q_0|)^2 \leq 1$, so $|Q_{n+1}| \leq \frac{|Q_0|}{p} (1 - D)$, and similarly for $p = 3$ and $|Q_0| > 1$. If $p = 3$ and $|Q_0| = 1$, then $|Q_{n+1}|$ is integral and bounded by the floor of $\frac{1}{3}(\frac{9}{4} - D)$. Since $D \equiv 1 \pmod{3}$, the floor is $\frac{1}{3}(1 - D)$, which is the required bound. Thus, NQCFS of quadratic irrationals with $p = 2$ and $D < 0$ and $p = 3$ and $D < -2$ are periodic. The case of $p = 3$ and $D = -2$ is handled by Lemma 3.

Now suppose that $D > 0$. We will show that $|Q_n| \leq \frac{|Q_0|}{p} (D + 1)$. This is true for $|Q_0|$ when $D \geq 1$ for $p = 2$ and $D \geq 2$ for $p = 3$. Since the first non-square values of $D$ to consider are $D = 17$ for $p = 2$ and $D = 7$ for $p = 3$, we have the bound for $|Q_0|$
and assume it holds for $|Q_n|$. If $P^2_{n+1} \leq (|Q_0| + 1)D$ then by (1.7)

$$|Q_{n+1}| \leq \frac{1}{p} |D - P^2_{n+1}| \leq \frac{|Q_0|}{p} D < \frac{|Q_0|}{p} (D + 1).$$

If $P^2_{n+1} > (|Q_0| + 1)D$, then $|Q_n| > \frac{2}{p} \sqrt{(|Q_0| + 1)D}$, and from (3.4) we just need to consider $f(x) = D/x - \frac{p^2}{4} x$ on the interval $\left(\frac{2}{p} \sqrt{(|Q_0| + 1)D}, \frac{|Q_0|}{p} (D + 1)\right]$. On this interval, $f(x)$ and $f'(x)$ are both negative, so $f(x)$ has its maximum absolute value at $x = \frac{|Q_0|}{p} (D + 1)$. Substituting this into (3.4) gives

$$|Q_{n+1}| \leq \frac{1}{p} \left| \frac{pD}{|Q_0|(D + 1)} - \frac{p|Q_0|(D + 1)}{4} \right|$$

$$= \frac{|Q_0|}{p} (D + 1) \left| \frac{pD}{Q^2_0(D + 1)^2} - \frac{p}{4} \right|$$

$$= \frac{|Q_0|}{p} (D + 1) \frac{|pQ^2_0(D + 1)^2 - 4pD|}{|4Q^2_0(D + 1)^2|}$$

Both the numerator and denominator are positive for $D > 1$, so

$$\frac{pQ^2_0(D + 1)^2 - 4pD}{4Q^2_0(D + 1)^2} < \frac{pQ^2_0(D + 1)^2}{4Q^2_0(D + 1)^2} = \frac{p}{4} < 1,$$

which shows that $|Q_{n+1}| < \frac{|Q_0|}{p} (D + 1)$ as required.

We are unable to find a general continued fraction algorithm—that can be applied to an arbitrary $\alpha \in Q_p$—that produces an NQCF when applied to a quadratic irrational. It is an interesting open problem to find such an algorithm, since this would be more analogous to Lagrange’s Theorem in the real case.

### 3.3 Numerical Results and Observations

We have performed many calculations regarding NQCFs of quadratic irrationals. Here we describe the extent of these calculations and report various interesting observations.
3.3.1 Periodicity in $\mathbb{Q}_p$ for $p > 3$

Although Theorem 20 only proves periodicity for $\mathbb{Q}_p$ with $p = 2, 3$, our data indicate that it may hold for all $p < 37$. For $p \leq 23$, we verified that $\sqrt{D}$ has a periodic NQCF for $-10000 \leq D \leq 10000$, and for $p = 29, 31$ we verified that $\sqrt{D}$ has a periodic NQCF for $-1000 \leq D \leq 1000$. To see if these results were limited to pure square roots, we also checked $\frac{P \pm \sqrt{D}}{Q}$ for $D$ on a large range and various small values of $P$ and $Q$. Because of the time required to perform the calculations, testing $P$ and $Q$ on a large range was prohibitive. In every case the quadratic irrational had a periodic NQCF. For $5 \leq p \leq 19$ we checked periodicity for $|D| \leq 10000$, $|P| \leq -2$, and $Q \in \{-2, -1, 1, 2, 3\}$. For $p = 23, 29, 31$ the values of $P$ and $Q$ checked were the same, but the values of $D$ were restricted to $[-1000, 1000]$ because of the increasingly long calculation times as $p$ grows.

For $p \geq 37$ there appear to be many square roots without a periodic NQCF. We say “appear” because our condition for proving periodicity is observing repeated values of $P_n$ and $Q_n$, so for any calculation we can only say that no period has yet been observed. The smallest case in which we have not observed periodicity is $\sqrt{-3} \in \mathbb{Q}_{37}$, for which 10,000 terms have been calculated. Although it is possible that the first period ends after more than 10,000 terms, it seems unlikely given how large $|P_n|$ and $|Q_n|$ get. For instance, $\frac{2 + \sqrt{707}}{3} \in \mathbb{Q}_{31}$ has a period starting with the third term and has a period of length 12,194. The largest values of $|P_n|$ and $|Q_n|$ in the expansion have 120 and 119 digits, respectively, while for $\sqrt{-3} \in \mathbb{Q}_{37}$ after 10,000 terms the sizes are 818 and 818 decimal digits.

For the primes, $p$, less than 100, the Table 3.1 lists the values of $D$, $-100 \leq D \leq 100$, for which no period in the NQCF of $\sqrt{D}$ was observed after 2,000 terms. Note that since there are almost exactly 100 integers between -100 and 100 with square roots in $\mathbb{Q}_p$ for $p \geq 37$, the number of values for which no period was observed—which is also given in the table—is very close to the percentage.
<table>
<thead>
<tr>
<th>(p)</th>
<th>(D)</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td>37</td>
<td>-100, -77, -3</td>
<td>3</td>
</tr>
<tr>
<td>41</td>
<td>-86, -43, -9, -4, 5, 33, 51, 73</td>
<td>8</td>
</tr>
<tr>
<td>53</td>
<td>-95, -91, -77, -66, -64, -63, -62, -59, -54, -46, -43, -38, -10, -9, -7, -1, 13, 29, 40, 42, 60, 82, 93, 97, 99</td>
<td>25</td>
</tr>
<tr>
<td>61</td>
<td>-95, -83, -76, -75, -74, -66, -65, -62, -56, -47, -34, -20, -19, -16, -13, -9, -4, -3, 13, 34, 45, 46, 48, 52, 56, 58, 66</td>
<td>27</td>
</tr>
<tr>
<td>67</td>
<td>-99, -97, -95, -94, -79, -75, -74, -69, -61, -46, -44, -43, -38, -30, -27, -20, -11, -8, -7, -5, -2, 15, 17, 19, 21, 26, 29, 73, 82, 86, 88, 93</td>
<td>32</td>
</tr>
<tr>
<td>71</td>
<td>-99, -97, -94, -92, -84, -68, -63, -52, -47, -44, -41, -39, -34, -33, -26, -23, -14, -13, 3, 5, 6, 18, 20, 24, 32, 37, 38, 43, 57, 60, 76, 77, 89, 95</td>
<td>34</td>
</tr>
<tr>
<td>73</td>
<td>-98, -92, -91, -89, -81, -77, -74, -71, -67, -61, -55, -54, -50, -41, -32, -27, -23, -19, -16, -12, -4, -3, 2, 12, 18, 19, 37, 38, 41, 54, 55, 57, 61, 65, 67, 69, 75, 76, 85, 91, 92, 97</td>
<td>42</td>
</tr>
<tr>
<td>79</td>
<td>-96, -86, -85, -82, -74, -71, -68, -66, -61, -59, -53, -47, -41, -39, -34, -28, -27, -17, -7, -6, -3, 10, 20, 22, 23, 26, 31, 32, 40, 44, 45, 46, 50, 51, 52, 55, 72, 73, 76, 89, 92, 97, 99</td>
<td>43</td>
</tr>
</tbody>
</table>

Table 3.1. \(D\) with \(|D| \leq 100, \sqrt{D} \in \mathbb{Q}_p\), and no period in the NQCF of \(\sqrt{D}\) after 2,000 terms.
3.3.2 Empirical Bounds on Remainders

Data for \( p \leq 23 \) show some predictable structure in the continued fractions for square roots. One set of data gathered to get empirical bounds on \(|P_n|\) and \(|Q_n|\) for periodicity proofs was the maximum values of \(|P_n|\) and \(|Q_n|\) that occur in the remainders of \( \sqrt{D} \) for \(|D| \leq 10000 \). This data for \(|P_n|\) and \( p \leq 19 \) is shown in Figures 3.2 and 3.3. The data for \(|Q_n|\) looks similar.

For \( p = 2, 3, 5 \) explicit bounds on \(|P_{n+1}|\) (and \(|Q_{n+1}|\) also) are visible. Namely, we have

- For \( p = 2 \), \(|P_n| \leq \frac{1}{2}|D|\) and \(|Q_n| \leq \frac{1}{2}(|D| + 1)\)
- For \( p = 3 \), \(|P_n| \leq \frac{1}{3}(|D| + 4)\) and \(|Q_n| \leq \frac{1}{3}(|D| + 1)\)
- For \( p = 5 \), \(|P_n| \leq \frac{2}{5}(|D| + 9)\) and \(|Q_n| \leq \frac{2}{5}(|D| + 2)\),

for \(|D| \leq 10000\). These same sort of lines are visible in all the graphs, but additionally there are points which do not fall on these lines and for which no bound in terms of \(|D|\) is apparent. Thus, for \( p > 5 \) there is no clear way to prove periodicity by some induction argument on the size of \(|P_n|\) and \(|Q_n|\) a bound that is a function of \(|D|\) alone. However, because of the explicit bounds for \( \mathbb{Q}_5 \), a proof of periodicity should be obtainable by induction, although it is not immediately clear how to proceed with the known recurrence relations.

Some other observations can be made regarding the structure of the continued fractions in \( \mathbb{Q}_2 \). In Figure 3.2 it is apparent that the maximum value of \(|P_n|\) lies on one of two lines, and a this also occurs for the maximum value of \(|Q_n|\). For all \(|D| \leq 10000\) the maximum values of \(|P_n|\) and \(|Q_n|\) are described by:

- if \( D \equiv 1 \pmod{16} \), \( \max |P_n| = \frac{1}{2}(|D| - \text{sgn}(D) - 2) \) and \( \max |Q_n| = \frac{1}{2}(|D| - \text{sgn}(D)) \)
Figure 3.2. Maximum values of $|P_n|$ in the NQCF for $\sqrt{D}$
Figure 3.3. Maximum values of $|P_n|$ in the NQCF for $\sqrt{D}$
• if $D \equiv 9 \pmod{16}$, $\max |P_n| = \frac{1}{4}(|D| - \text{sgn}(D) - 4)$ and $\max |Q_n| = \frac{1}{4}(|D| - \text{sgn}(D))$.

Further, the data also shows some predictability in where the period starts. Namely, if $D < 0$ then the period starts with $a_1$ if $D \equiv 9 \pmod{16}$ and with $a_3$ if $D \equiv 1 \pmod{16}$. If $D > 0$, then the period does not start with $a_2$.

### 3.3.3 Examples of a non-palindromic symmetry

The most interesting observation about NQCFs coming from quadratic irrationals is a special kind of symmetry that often occurs. While the symmetry that occurs in the period for the real numbers and SCFs is palindromic, this symmetry has the first half of the period repeated but with opposite signs on the partial denominators, which we refer to as negative symmetry. For example, in $\mathbb{Q}_{31}$

$$\sqrt{245} = \left[ \begin{array}{cccccccc} 31 & 31 & 31 & 31^2 & 31 & 31 & 31 & 31^2 \\ 11 & -10 & -7 & 2 & -115 & 10 & -7 & -2 & 115 \end{array} \right].$$

No necessary and sufficient, or even just a general sufficient, condition has been found to determine if $\sqrt{D}$ will possess negative symmetry. For $|D| \leq 1000$ in $\mathbb{Q}_2$ about 66% of the continued fractions had negative symmetry. For $\mathbb{Q}_p$ with $3 \leq p \leq 31$ we checked the percentage of continued fraction that had negative symmetry for $|D| \leq 500$, which is summarized in Table 3.2.

One mechanism that may be involved is the following. If the partial numerators are allowed to be positive or negative powers of $p$, then converting a periodic such continued fraction into an STCF will transform a period into one with negative symmetry if there are an odd number of negative powers of $p$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
</tr>
</thead>
<tbody>
<tr>
<td>%</td>
<td>53.8</td>
<td>59.1</td>
<td>53.4</td>
<td>46.2</td>
<td>45.9</td>
<td>41.5</td>
<td>37.6</td>
<td>33.1</td>
<td>32.9</td>
<td>30.5</td>
</tr>
</tbody>
</table>

Table 3.2. Percentage of square roots whose NQCF have negative symmetry
Chapter 4

Continued Fractions in $\mathbb{F}_q((t))$

In this chapter we look at analogues of ITCFs in the $t$-adic field $\mathbb{F}_q((t))$, where $\mathbb{F}_q[t]$ plays the role of $\mathbb{Z}$ and $\mathbb{F}_q[[t]]$ plays the role of $\mathbb{Z}_p$. We restrict ourselves to $\mathbb{F}_q((t))$, rather than more generally looking at the completion of $\mathbb{F}_q(t)$ with respect to some $P$-adic valuation, where $P \in \mathbb{F}_q[t]$ is irreducible, for simplicity, since $\mathbb{F}_q(t)_P$ is isomorphic to $\mathbb{F}_q((\pi_P))$, where $d = \deg P$ and $\pi_P$ is a uniformizing element. Simple continued fractions in $\mathbb{F}_q((t-1))$ with partial quotients in $\mathbb{F}_q[t]$ are the analogue of real, simple continued fractions with integral partial quotients. This case has been studied by many people, starting with Emil Artin, and has good properties that are similar to the real case, like Lagrange’s Theorem and best approximation results [Tha04]. We start by generalizing the definitions of ITCF and SRTCF classes to a field that is complete with respect to a discrete, non-archimedean, normalized valuation.

4.1 Continued Fractions in Non-archimedean Local Fields

Throughout this section, $K$ is a field that is complete with respect to a discrete, non-archimedean, normalized valuation $v$. Also, we let $\mathcal{O}$ be the ring of integers, $\mathfrak{m}$ be the unique maximal ideal, $\pi \in \mathcal{O}$ be a uniformizing element, and $\mathcal{R}$ be a set of representatives for $\mathcal{O}/\mathfrak{m}$ which includes 0. Then we can express every element $\alpha \in K^*$ uniquely as a series

$$\alpha = \sum_{k=n}^{\infty} c_k \pi^n,$$

where $c_k \in \mathcal{R}$ for $k \neq n$.

Definition 12. Let $\alpha \in \mathcal{O}^*$. A continued fraction of the form (1.1) or (1.2) is a general integral type continued fraction (GITCF) for $\alpha$ if $a_i, b_i \in \mathcal{O}$ and $v(a_i - b_i) =
$v(b_i) = e_i > 0$ for $i \geq 0$. If $\alpha \in K \setminus \mathcal{O}^*$, then the requirements are the same, except that $a_0 = 0$ and $b_0 = \pi^{e_0(\alpha)}$.

This is a generalization of ITCFs to fields complete with respect to a discrete, non-archimedean, normalized valuation. If $K = \mathbb{Q}_p$, however, the classes ITCF and GITCF are not the same, since the partial numerators and denominators are in $\mathcal{O} = \mathbb{Z}_p$, rather than restricted to $\mathbb{Z}$. Typically, we will be concerned with continued fractions whose partial numerators and denominators comes from $\mathbb{Z}$ or $\mathbb{F}_q[t]$.

These continued fractions have all the same properties as ITCFs. Here are a few that are relevant to the proofs of the convergence theorems below.

**Proposition 7.**

- $v(\alpha_n) = v(a_n) = 0$ for $n > 0$, and for $n = 0$, as well if $\alpha \in \mathcal{O}^*$
- $v(B_n) = 0$ for $n \geq 0$
- $v(A_nB_{n-1} - A_{n-1}B_n) = e_0 + \cdots e_{n-1}$ for $n > 0$
- $v(A_n/B_n - A_{n-1}/B_{n-1}) = e_0 + \cdots e_{n-1}$ for $n > 0$

The justification is exactly the same as for ITCFs. The proofs of convergence are the same as for ITCFs, where $\rho^{-v(\alpha)}$, for some $0 < \rho < 1$, is used for the absolute value, instead of $| \cdot |_p$. Thus, we have the following.

**Theorem 21.** The convergents of a GITCF for $\alpha \in K$ converge to $\alpha$.

**Theorem 22.** If a continued fraction has the properties that $a_i, b_i \in \mathcal{O}$, $v(a_i) = 0$, and $v(b_i) = e_i > 0$ for all $i \geq 0$, then all the convergents are defined and converge to a number $\alpha \in \mathcal{O}^*$. If the continued fraction has the property above for $i \geq 1$, $a_0 = 0$, $b_0 = \pi^{e_0}$, and $e_0 \neq 0$, then the convergents converge to some $\alpha \in K \setminus \mathcal{O}^*$. Furthermore, the continued fraction is a GITCF for $\alpha$. 
We can generalize the notion of SRTCFs, as well.

**Definition 13.** Let $\alpha \in K \setminus m$. A continued fraction of the form (1.1) or (1.2) is a general simple rational type continued fraction (GSRTCF) for $\alpha$ if $a_i \in K^*$, $b_i = 1$, and $v(\alpha_i - a_i) = e_i > 0$ for $i \geq 0$. If $\alpha \in m$ the requirements are the same, except that $a_0 = 0$.

The facts used in the proofs of convergence are the following.

**Proposition 8.**

- $e_i = -v(a_{i+1})$ for $i \geq 0$ and $e_{-1} = -v(a_0)$ by definition
- $v(A_i) = -(e_{-1} + \cdots + e_{i-1})$ and $v(B_{i+1}) = -(e_0 + \cdots + e_i)$ for $i \geq 0$ when $v(\alpha) \leq 0$
- $v(A_{i+1}) = -(e_1 + \cdots + e_i)$ and $v(B_{i}) = -(e_0 + \cdots + e_{i-1})$ for $i \geq 1$ when $v(\alpha) > 0$.

The justification is the same as for SRTCFs, except for $e_i = -v(a_{i+1})$, for which we represented $a_i$ as a quotient of relatively prime integers. This is easy to see, however, since $e_i = v(\alpha_i - a_i) = v(\alpha^{-1}_{i+1}) = -v(a_{i+1})$, and $v(\alpha_{i+1}) = v(a_{i+1})$ since $v(\alpha_{i+1}) < 0$ and $v(\alpha_{i+1} - a_{i+1}) > 0$, for $i \geq 0$. The convergence proofs work the same, except that $| \cdot |_p$ is replaced by $\rho^{-v(\alpha)}$, for some $0 < \rho < 1$. Thus, we have the two convergence theorems.

**Theorem 23.** The convergents of a GSRTCF for $\alpha \in K$ converge to $\alpha$.

**Theorem 24.** If a simple continued fraction has partial quotients $a_i = u_i \pi^{k_i}$ such that $u \in O^*$ and $k_i < 0$ for $i \leq 0$, then the continued fraction converges to some $\alpha \in K \setminus m$. If the condition holds for $i \geq 1$ and $a_0 = 0$ then the continued fraction converges to some $\alpha \in m$. Furthermore, the continued fraction is a GSRTCF for $\alpha$, in either case.
4.2 Rationals and Quadratic Irrationals in $\mathbb{F}_q((t))$

The question of finiteness of continued fractions for rational functions in $\mathbb{F}_q((t))$ is easily answered when the partial numerators are powers of $t$, up to a unit of $\mathbb{F}_q$, and the partial denominators are in $\mathbb{F}_q$. Suppose $\alpha = R_0/S_0 \in \mathbb{F}_q(t)$, where $R_0, S_0 \in \mathbb{F}_q[t]$. Then the remainders of a continued fraction, with partial numerators and denominators as described, are given by $\alpha_{n+1} = R_{n+1}/S_{n+1}$, where

$$
R_{n+1} = S_n
$$

$$
S_{n+1} = \frac{R_n - a_n S_n}{u_n t^{e_n}},
$$

for $u_n \in \mathbb{F}_q$ and $n \geq 0$. We know that $S_{n+1} \in \mathbb{F}_q[t]$ because $a_n$ is chosen so that $v(R_n/S_n - a_n) = e_n$. Since $e_n > 0$ and $R_n = S_{n-1}$ we have

$$
\deg S_{n+1} < \max (\deg S_{n-1}, \deg S_n),
$$

(4.1)

for $n \geq 1$, if $a_n \in \mathbb{F}_q$.

**Theorem 25.** Let $\alpha \in \mathbb{F}_q(t)$. If a GITCF for $\alpha$ has the properties that $b_n = u_n t^{e_n}$, $a_n, u_n \in \mathbb{F}_q$, and $v(\alpha_n - a_n) = e_n$, then the continued fraction is finite.

**Proof.** Suppose that the continued fraction is infinite, so that there are infinitely many $S_n$. We show that there exists a subsequence of $(\deg S_n)_{n\geq 0}$ that is infinite and strictly decreasing, which is a contradiction since $\deg S_n \geq 0$ for all $n \geq 0$.

Suppose that there are only finitely many $n$ such that $\deg S_n > \deg S_{n-1}$, and that $N$ is the last such $N$. Then we have

$$
\deg S_N \geq \deg S_{N+1} \geq \deg S_{N+2} \geq \cdots.
$$

By (4.1), we have the infinite, strictly decreasing sequence of non-negative integers

$$
\deg S_N > \deg S_{N+2} > \deg S_{N+4} > \cdots,
$$
which is a contradiction. Thus, there must be infinitely many $n$ such that $\deg S_n > \deg S_{n-1}$, which we enumerate by $N_1, N_2, \ldots$. By (4.1),

$$\deg S_{N_{k+1}} < \max (\deg S_{N_{k+1}} - 2, \deg S_{N_{k+1} - 1}) = \deg S_{N_{k+1}-2},$$

since by the definition of $N_{k+1}$ we have $\deg S_{N_{k+1}} > \deg S_{N_{k+1} - 1}$. Since

$$\deg S_{N_{k+1} - 1} < \deg S_{N_{k+1}} < \deg S_{N_{k+1} - 2}$$

we must have $N_k < N_{k+1} - 1$, which means that $\deg S_{N_{k+1} - 2} \leq \deg S_N$, and so $\deg S_{N_{k+1}} < \deg S_N$. Thus,

$$\deg S_{N_1} > \deg S_{N_2} > \deg S_{N_3} > \cdots$$

is an infinite, strictly decreasing sequence of non-negative integers, which is a contradiction. Thus, the continued fraction must be finite.

This theorem is an analogue of Theorem 19 for STCFs. The finiteness comes with less restrictions because of the fields positive characteristic, and because elements of $\mathbb{F}_q$ have degree zero. We give one example.

**Example 6.** In $\mathbb{F}_7((t))$

$$\frac{3t^3 + 2t + 1}{t^6 + t^4 + t^2 + 1} = \left[ \frac{t}{1}, \frac{t}{4}, \frac{t}{4}, \frac{t}{6}, \frac{t}{5}, \frac{2}{2}, \frac{2}{1} \right]$$

For quadratic irrationals in $\mathbb{F}_q((t))$, we will only consider GITCFs where the partial numerators are of the form $ut^n$ and the partial denominators are in $\mathbb{F}_q[t]$. We call this class of continued fractions *functional Schneider type continued fractions* (FSTCF), which is an analogue of the STCF class, except that we allow arbitrary units as factors of the partial numerators. For a quadratic irrational, $\alpha = (P_0 + \sqrt{D})/Q_0 \in \mathbb{F}_q((t))$, $P_0, Q_0, D \in \mathbb{F}_q[t]$, the same relations hold between $P_n$ and $Q_n$ in the remainders $\alpha_n = (P_n + \sqrt{D})/Q_n$ of an FSTCF for $\alpha$. Namely,

$$P_{n+1} = a_n Q_n - P_n \quad (4.2)$$
$$Q_{n+1} = \frac{D - P_{n+1}^2}{b_n Q_n} \quad (4.3)$$
The analogue of Proposition 6 holds for FSTCFs of quadratic irrationals.

**Proposition 9.** For all \( n \geq 0 \), \( P_n, Q_n \in \frac{1}{q^n} \mathbb{F}_q[t] \).

The proof is the same as for Proposition 6, replacing \( p^n \) by \( b_n = u_n t^n \), where \( u_n \in \mathbb{F}_q \). Thus, a quadratic irrational has a periodic FSTCF if and only if the sequences \( (\deg P_n)_{n \geq 0} \) and \( (\deg Q_n)_{n \geq 0} \) are bounded above, when the algorithm generating the continued fraction generates \( a_n \) and \( b_n \) solely based on \( \alpha_n \) (i.e., when the algorithm is indiscriminant).

Looking at periodicity from the standpoint of boundedness of \( \deg P_n \) and \( \deg Q_n \), the situation is significantly different from STCFs, since \( \deg \) is non-archimedean and \( | \cdot | \) is archimedean. Let us first consider the following continued fraction algorithm, which is similar to Schneider’s SCFs.

**Definition 14.** A continued fraction of the form (1.1) or (1.2) is a first functional continued fraction (FCF1) for \( \alpha \in \mathbb{F}_q((t)) \) if it an FSTCF, \( a_n \in \mathbb{F}_q \) and \( b_n = t^{e_n} \) for all \( n \geq 0 \). If \( \alpha_n \) is the \( n \)th remainder, then \( a_n \) is the unique value in \( \mathbb{F}_q \) for which \( v(\alpha_n - a_n) > 0 \), and \( e_n \) is equal to \( v(\alpha_n - a_n) \).

The continued fractions in Theorem 25 are slight generalizations of FCF1s, so the FCF1 of a rational function is finite. For an FSTCF of a quadratic irrational we have the following inequalities, when \( a_n \in \mathbb{F}_q \) for all \( n \geq 0 \),

\[
\begin{align*}
\deg P_{n+1} & \leq \max (\deg Q_n, \deg P_n) \\
\deg Q_{n+1} & \leq \max (\deg D, 2 \deg P_n) - \deg Q_n - e_n,
\end{align*}
\]

with equality when the values in the max function are unequal. One quick consequence of these inequalities is the following proposition.

**Proposition 10.** Suppose \( \alpha = P + \sqrt{D} \in \mathbb{F}_q[[t]] \) with \( P, D \in \mathbb{F}_q[t] \), and \( \deg P \leq 1 \) and \( \deg D \leq 2 \). Then an indiscriminantly generated FSTCF for \( \alpha \), with \( a_n \in \mathbb{F}_q \) for all \( n \geq 0 \), is periodic.
**Proof.** By induction we show that $\deg P_n, \deg Q_n \leq 1$ for all $n \geq 0$. This is true for $n = 0$ by the hypothesis of the proposition. Suppose that $\deg P_n, \deg Q_n \leq 1$ and consider $\deg P_{n+1}$ and $\deg Q_{n+1}$. By the inequalities we have $\deg P_{n+1} \leq \max(1,1) = 1$ and $\deg Q_{n+1} \leq 2 - 0 - e_n \leq 1$ since $e_n > 0$ and $\deg Q_{n+1} \geq 0$, by Proposition 9. Thus, since $\deg P_n$ and $\deg Q_n$ are bounded above by zero, the continued fraction is periodic. □

Here are our two examples in $\mathbb{F}_{37}[t]$:

$$\sqrt{7t + 36} = \left[ \begin{array}{c} t \\ 6 & 7 & 12 \end{array} \right]$$

$$\sqrt{30 + 29t^2} = \left[ \begin{array}{c} t^2 \\ 17 & 5 & 34 \end{array} \right]$$

It is easy to check that

$$\sqrt{a_0^2 + \frac{2a_0}{a_1}t} = \left[ \begin{array}{c} \frac{2a_0}{a_1}t \\ a_0 & a_1 & 2a_0 \end{array} \right],$$

when $p > 2$. The FCF1 does not have this form for all $D$ with $\deg D = 1$. For example, in $\mathbb{F}_3((t))$

$$1 + t + \sqrt{1 + t} = \left[ \begin{array}{c} t^2 \\ 2 & 1 & 1 & 1 & 1 & 1 \end{array} \right].$$

The example, with the smallest degree of $D$, for which we have not observed a period in the FCF1 of $\sqrt{D}$ is $D = x^3 + 2x + 1$. After calculating 100 terms, the degrees of $P_n$ and $Q_n$ are generally growing. For example, $\deg P_{20} = 6$, $\deg P_{50} = 12$, $\deg Q_{50} = 10$, and $\deg P_{100} = 22$, $\deg Q_{100} = 21$.

When trying to use the inequalities above to establish a sufficient condition for non-periodicity, by forcing unboundedness, one finds that the difficulty in predicting the values of $e_n$ presents a problem. If we force the values of $e_n$ and $\deg a_n$ to always be one, however, we can get a sufficient condition for non-periodicity.

**Proposition 11.** Let $\alpha = (P + \sqrt{D})/Q \in \mathbb{F}_q((t))$, $P, Q, D \in \mathbb{F}_q[t]$, be a quadratic irrational, and suppose it has an indiscriminantly $(a_n, b_n$ depend, deterministically,
on $\alpha_n$ alone) generated FSTCF with the properties that $\deg a_n = 1$ and $e_n = 1$ for all $n \geq 1$. If $2\deg P_n > \deg D$ and $\deg Q_n \geq \deg P_n$ for some $n \geq 1$, then the continued fraction is not periodic.

**Proof.** The proof follows by induction, showing that $\deg P_{n+k} = \deg Q_n + k$ for all $k \geq 1$. For $k = 1$, we have

$$\deg P_{n+1} = \max (\deg Q_n + 1, \deg P_n) = \deg Q_n + 1,$$

by the hypothesis that $\deg Q_n \geq \deg P_n$. We have to also show, by induction on $k$, that $\deg Q_{n+k} = \deg Q_n + k$. For $k = 1$ we know $\deg P_{n+1} > \deg P_n$, so $2\deg P_{n+1} > \deg D$ and

$$\deg Q_{n+1} = 2\deg P_{n+1} - \deg Q_n - 1 = 2(\deg Q_n + 1) - \deg Q_n - 1 = \deg Q_n + 1.$$

Now suppose that $\deg P_{n+k} = \deg Q_{n+k} = \deg Q_n + k$ and consider $\deg P_{n+k+1}$ and $\deg Q_{n+k+1}$. Then

$$\deg P_{n+k+1} = \max (\deg Q_{n+k} + 1, \deg P_{n+k}) = \max (\deg Q_n + k + 1, \deg Q_n + k) = \deg Q_n + k + 1,$$

and

$$\deg Q_{n+k+1} = 2\deg P_{n+k+1} - \deg Q_{n+k} - 1 = 2(\deg Q_n + k + 1) - (\deg Q_n + k) - 1 = \deg Q_n + k + 1,$$

since $2\deg P_{n+k+1} > \deg D$. Thus, since $\deg P_{n+k} \to \infty$, the continued fraction is not periodic. \qed

It is easy to produce such an algorithm when $q \neq 2$. For instance, if $\alpha_n = c_0 + c_1 t + c_2 t^2 + \cdots$ we could choose $a_n = c_0 + (c_1 - 1)t$ if $c_1 \neq 1$ and $a_n = c_0 + (q-1)t$ if $c_1 = 1$. If the quadratic irrational is in $\mathbb{F}_q[[t]]$ then the proposition holds for $n \geq 0$,
and one can simply choose $D$, $P_0$, and $Q_0$ appropriately, in order to construct such a non-periodic example.

Now we introduce an algorithm that uses the same modus operandi as the NQCF algorithm. That is, the algorithm constructs an FSTCF for a quadratic irrational that attempts to keep $\deg P_n$ small, with the hope that this will keep $\deg Q_n$ small as well. The impetus for the algorithm is the observation that since $\deg P_{n+1} \leq \max (\deg a_n Q_n, \deg P_n)$, with equality when the degrees are unequal, the only way for $\deg P_{n+1}$ to be less than $\deg P_n$ is for $\deg a_n Q_n = \deg P_n$ and for the leading coefficients of $a_n Q_n$ and $P_n$ to be the same. This leads one to consider algorithms where $a_n$ is chosen with $\deg a_n = \deg P_n - \deg Q_n$ when $\deg Q_n \leq \deg P_n$. Although it also seems beneficial to try to make the leading coefficients of $a_n Q_n$ and $P_n$ the same, when $\deg Q_n \leq \deg P_n$, that turns out to be problematic, and having $\deg a_n = \deg P_n - \deg Q_n$, with a couple of other conditions, turns out to be sufficient. There are a number of ways to do this, and any such algorithm will produce a periodic FSTCF for any quadratic irrational, when, additionally, $\deg b_n \geq \deg a_n$ for $n \geq 0$ and $\deg a_n = 0$ when $\deg Q_n > \deg P_n$. Before we introduce such an algorithm and prove periodicity more generally, we need the following lemma.

**Lemma 4.** Suppose $\alpha = (P + \sqrt{D})/Q \in \mathbb{F}_q((t))$, $P, Q, D \in \mathbb{F}_q[t]$ is a quadratic irrational with an FSTCF that has the properties that $\deg a_n = \deg P_n - \deg Q_n$ when $\deg Q_n \leq \deg P_n$, $\deg b_n \geq \deg a_n$ for all $n \geq 0$, and $\deg a_n = 0$ when $\deg Q_n > \deg P_n$. Then

1. If, for some $n \geq 0$, $\deg Q_n > \deg P_n$ and $2 \deg Q_n > \deg D$ then $\deg Q_{n+1} < \deg P_{n+1}$, $\deg P_{n+1} = \deg Q_n$, and $2 \deg P_{n+1} > \deg D$.

2. If, for some $n \geq 0$ and $k \geq 1$, $2 \deg P_n, \ldots, 2 \deg P_{n+k} > \deg D$ then

$$\deg P_{n+k}, \deg Q_{n+k} \leq \max (\deg P_n, \deg Q_n).$$
3. If, for some \( n \geq 0 \), \( 2 \deg P_n \leq \deg D \) and \( 2 \deg P_{n+1} > \deg D \) then \( \deg P_{n+1} \leq \deg D + \deg Q_0 - 1 \) and \( \deg Q_{n+1} \leq 2 \deg D + 3 \deg Q_0 - 3 \).

**Proof.** Throughout this lemma, we use Proposition 9, (4.2), and (4.3), without explicitly stating their use. For the first part, since \( \deg Q_n > \deg P_n \) by hypothesis, we have \( \deg a_n = 0 \) and

\[
\deg P_{n+1} = \max (\deg a_n Q_n, \deg P_n) = \deg a_n Q_n = \deg Q_n.
\]

Now since \( 2 \deg Q_n > \deg D \) we have \( 2 \deg P_{n+1} > \deg D \). Then

\[
\deg Q_{n+1} = 2 \deg P_{n+1} - \deg Q_n - \deg b_n
= \deg Q_n - \deg b_n
< \deg Q_n = \deg P_{n+1},
\]

since \( \deg b_n > 0 \).

We prove the second part by induction on \( k \). For \( k = 1 \), either \( \deg Q_n > \deg P_n \) or \( \deg Q_n \leq \deg P_n \). If \( \deg Q_n > \deg P_n \) then \( \deg P_{n+1} = \deg a_n Q_n = \deg Q_n \), since \( \deg a_n = 0 \) and \( \deg Q_{n+1} < \deg P_{n+1} = \deg Q_n \) by the first part of the lemma. If \( \deg Q_n \leq \deg P_n \) then \( \deg P_{n+1} \leq \deg P_n \), so \( \deg P_{n+1} \leq \max (\deg P_n, \deg Q_n) \). Then, since we are assuming \( 2 \deg P_{n+1} > \deg D \) we have

\[
\deg Q_{n+1} = 2 \deg P_{n+1} - \deg Q_n - \deg b_n
\leq 2 \deg P_n - \deg Q_n - \deg b_n.
\]

Since \( \deg a_n = \deg P_n - \deg Q_n \), and \( \deg b_n \geq \deg a_n \), we have \( \deg b_n \geq \deg P_n - \deg Q_n \). Then

\[
\deg Q_{n+1} \leq 2 \deg P_n - \deg Q_n - (\deg P_n - \deg Q_n) = \deg P_n.
\]

Thus, we have \( \deg P_{n+1}, \deg Q_{n+1} \leq \max (\deg P_n, \deg Q_n) \).
Now suppose that it holds for $k$ and consider $\deg P_{n+k+1}$ and $\deg Q_{n+k+1}$. Using the same argument comparing $\deg P_{n+1}$ and $\deg Q_{n+1}$ to $\max(\deg P_n, \deg Q_n)$ we have

$$\deg P_{n+k+1}, \deg Q_{n+k+1} \leq \max(\deg P_{n+k}, \deg Q_{n+k}) \leq \max(\deg P_n, \deg Q_n),$$

where the last inequality is by the induction hypothesis.

For the third part, we have

$$\deg Q_n = \deg D - \deg Q_{n-1} - \deg b_{n-1} \leq \deg D + \deg Q_0 - 1.$$ 

Since $2\deg P_{n+1} > \deg D$, $\deg P_{n+1} > \deg P_n$, so $\deg P_{n+1} = \deg a_nQ_n$. Now $\deg Q_n > \deg P_n$, since otherwise $\deg P_{n+1} \leq \deg P_n$, so $\deg a_n = 0$ and $\deg P_{n+1} = \deg Q_n$. Then

$$\deg P_{n+1} = \deg Q_n \leq \deg D - \deg Q_{n-1} - \deg b_{n-1} \leq \deg D + \deg Q_0 - 1.$$ 

Since $2\deg P_{n+1} > \deg D$ we have

$$\deg Q_{n+1} = 2\deg P_{n+1} - \deg Q_n - \deg b_n \leq 2(\deg D + \deg Q_0 - 1) + \deg Q_0 - 1 = 2\deg D + 3\deg Q_0 - 3.$$ 

We are now ready to prove periodicity for indiscriminantly $(a_n, b_n$ depend, deterministically, on $\alpha_n$ alone) generated continued fractions that satisfy the conditions of the lemma.

**Theorem 26.** Suppose $\alpha = (P + \sqrt{D})/Q \in \mathbb{F}_q((t))$, $P, Q, D \in \mathbb{F}_q[t]$ is a quadratic irrational with an indiscriminantly generated FSTCF that has the properties that
\[ \deg a_n = \deg P_n - \deg Q_n \quad \text{when} \quad \deg Q_n \leq \deg P_n, \quad \deg b_n \geq \deg a_n \quad \text{for all} \quad n \geq 0, \]

and \[ \deg a_n = 0 \quad \text{when} \quad \deg Q_n > \deg P_n. \] Then the continued fraction is periodic.

**Proof.** If after some \( N \geq 0 \) we have \( 2 \deg P_n \leq D \) for all \( n \geq N \), then

\[
\deg Q_n \leq \deg D - \deg Q_{n-1} - \deg b_n \leq \deg D + \deg Q_0 - 1,
\]

so the continued fraction would be periodic, since the sequences \((\deg P_n)_{n \geq 0}\) and \((\deg Q_n)_{n \geq 0}\) would be bounded.

We now assume that \( 2 \deg P_n > \deg D \) for some \( n \geq 0 \). Suppose \( 2 \deg P_0 > \deg D \).

If \( 2 \deg P_n > \deg D \) for all \( n \geq 0 \) then, by the second part of Lemma 4, \((\deg P_n)_{n \geq 0}\) and \((\deg Q_n)_{n \geq 0}\) are bounded above by \( \max (\deg P_0, \deg Q_0) \), and so the continued fraction is periodic.

Thus, we now assume that there is an \( n \geq 0 \) such that \( 2 \deg P_n \leq D \) and \( 2 \deg P_{n+1} > D \). We enumerate all such \( n \), by \( N_1, N_2, \ldots \), which may be a finite or infinite sequence. By the second part of Lemma 4 we have

\[
\deg P_n \leq \limsup_k \max \left( \deg P_{N_k}, \deg Q_{N_k}, \frac{\deg D}{2} \right)
\leq \max \left( \deg D + \deg Q_0 - 1, 2 \deg D + 3 \deg Q_0 - 3, \frac{\deg D}{2} \right),
\]

where the last line is by the third part of Lemma 4. Since \((\deg P_n)_{n \geq 0}\) is bounded above and

\[
\deg Q_n \leq \max (\deg D, 2 \deg P_n) - \deg Q_{n-1} - \deg b_{n-1}
\leq \max (\deg D, 2 \deg P_n) + \deg Q_0 - 1,
\]

\((\deg Q_n)_{n \geq 0}\) is bounded above, as well, and the continued fraction is periodic.

Thus, in any case, the continued fraction is periodic. \( \Box \)

Now that we know any algorithm satisfying the conditions of the theorem will produce periodic continued fractions for quadratic irrationals, we need to show that one actually exists.
Definition 15. Let $\alpha = (P + \sqrt{D})/Q \in \mathbb{F}_q[[t]]^*$, $P, Q, D \in \mathbb{F}_q[t]$ be a quadratic irrational. A continued fraction is a function field NQCF (FNQCF) for $\alpha$ if it is generated in the following way, when $\alpha_n = (P_n + \sqrt{D})/Q_n, n \geq 0$, is given:

1. if $\deg Q_n > \deg P_n$ set $a_n$ to the unique number in $\mathbb{F}_q$ for which $v(\alpha_n - a_n) = e_n > 0$; otherwise, if $\deg P_n - \deg Q_n = k \geq 0$ and
   \[
   \alpha_n = c_0 + c_1 t + c_2 t^2 + \cdots ,
   \]
   set $a_n = c_0 + \cdots + c_k t^k$ if $c_k \neq 0$ and set $a_n = c_0 + \cdots + c_{k-1} t^{k-1} + t^k$ if $c_k = 0$

2. set $e_n = v(\alpha_n - a_n)$ and $b_n = t^{e_n}$

3. then
   \[
   \alpha_{n+1} = \frac{b_n}{\alpha_n - a_n} = \frac{P_{n+1} + \sqrt{D}}{Q_{n+1}},
   \]
   where $P_{n+1}$ and $Q_{n+1}$ are given by the usual formulas.

For quadratic irrationals $\alpha \in \mathbb{F}_q((t))$ with $v(\alpha) \neq 0$, the FNQCF is generated by setting $a_0 = 0, b_0 = t^{v(\alpha)}$, and applying the algorithm above to $\alpha_1 = b_0/\alpha$ for $n \geq 1$.

If $v(\alpha) \neq 0$ then $v(\alpha_1) = 0$, and we will consider how the FNQCF of $\alpha_1$ satisfies the conditions of the theorem. The facts that $\deg a_n = \deg P_n - \deg Q_n$ when $\deg Q_n \leq \deg P_n$ and $\deg a_n = 0$ when $\deg Q_n > \deg P_n$ are clear. Since $\alpha_n$ and $a_n$ agree up through $c_{k-1} t^{k-1}$ when $k > 0$ and through $c_0$ when $k = 0$ shows that $\deg b_n \geq \deg a_n$, with equality only when $k > 1$ and $c_k = 0$. 
Appendix A

PARI/GP Code

All calculations were done using GP. The version is the following, as displayed when starting GP:

GP/PARI CALCULATOR Version 2.2.12 (beta)
i686 running cygwin (ix86 kernel) 32-bit version
compiled: Jan 3 2006, gcc-3.4.1 (cygming special)
(readline v5.0 enabled, extended help available)

Some calculations were also done using

GP/PARI CALCULATOR Version 2.3.2 (released)
i686 running linux (ix86 kernel) 32-bit version
compiled: May 15 2007, gcc-4.0.3 (Ubuntu 4.0.3-1ubuntu5)
(readline v5.1 enabled, extended help available)

The code below was modified on-the-fly to suit particular needs, so the code that was actually executed might have been different in an insignificant way, such as adding in extra print statements. The variable \texttt{prec}, the precision for \(p\)-adic arithmetic, was set at 1000 by default, but was increased in the rare cases that required more precision.

### A.1 Integral Continued Fraction Code

```c
/* Description: period length for Scheinder continued fractions */
/* */
/* Arguments: c - integer to take square root of */
/* p - prime for the p-adic field in which to take the */
/* square root */
/* */
/* Output: period length if the continued fraction is periodic, or -1 */
```
times the line in the PQ table that determined the continued fraction was not periodic

--

```plaintext
schp(c,p)=
{ local(xi=sqrt(c+O(p^prec)),a=lift(Mod(xi,p)),
    b=valuation(xi-a,p),P=0,Q=1,period=0,a0=a,b0=b,n=0,pprec=prec);

    while(period == 0,
        P = a*Q-P;
        Q = (c-P^2)/(p^b*Q);
        xi = p^b/(xi-a);
        a = lift(Mod(xi,p));
        b = valuation(xi-a,p);
        n = n+1;
        pprec = padicprec(xi,p);
        if(pprec==1, error("precision too low"));

        if((Q<0) || (P^2>c), period=-n);
        if((P==a0)&&(Q==1)&&(a==2*a0)&&(b==b0),period=n);

        period
    }
}

/*---------------------------------------------------------------------*
* Description: period length for Scheinder continued fractions where *
* partial quotients are chosen to make P_n minimal in absolute value (NQCF algorithm) *
* *
* Arguments: c - integer to take square root of *
* p - prime for the p-adic field in which to take the square root *
* n - maximum number of terms to compute *
* P,Q - the integers in xi = (P+sqrt(c))/Q *
* xi - the quadratic irrational on which to apply the alg. *
* *
* Output: period length and starting point if the first period ends after n terms, -1 otherwise *
*---------------------------------------------------------------------*/
schp2(c,p,n,P,Q)=
{ local(xi=(P+sqrt(c+O(p^prec)))/Q,a,pqtab,
    b,Pp1,Pp2,period=-1,i=0,k,pprec=prec,j);

    pqtab = listcreate(n+1);
    listput(pqtab,[P,Q]);
    a = lift(Mod(xi,p));
    Pbar = (a*Q-P)/p*(p*Q);
    k = ((P/Q)-a)/p;
    Pp1 = abs((a+floor(k*p))*Q-P);

    while(period == 0,
        P = a*Q-P;
        Q = (c-P^2)/(p^b*Q);
        xi = p^b/(xi-a);
        a = lift(Mod(xi,p));
        b = valuation(xi-a,p);
        n = n+1;
        pprec = padicprec(xi,p);
        if(pprec==1, error("precision too low"));

        if((Q<0) || (P^2>c), period=-n);
        if((P==a0)&&(Q==1)&&(a==2*a0)&&(b==b0),period=n);

        period
    )
}
```
```plaintext
Pp2 = abs((a+ceil(k)*p)*Q-P);
if(min(Pp1,Pp2)==Pp1,k=floor(k),k=ceil(k));
a = a+k*p;
b=valuation(xi-a,p);
while((period == -1)&&(i<n),
P = a*Q-P;
Q = (c-P^2)/(p^b*Q);
xi = (P+sqrt(c+O(p^prec)))/Q;
if(xi-a==0,break);
a = lift(Mod(xi,p));
Pbar = (a*Q-P)%p*Q);
k = ((P/Q)-a)/p;
Pp1 = abs((a+floor(k)*p)*Q-P);
Pp2 = abs((a+ceil(k)*p)*Q-P);
if(min(Pp1,Pp2)==Pp1,k=floor(k),k=ceil(k));
a = a+k*p;
b = valuation(xi-a,p);
if(b >= prec, print("Insufficient precision!");break);
i = i+1;
j = setsearch(Set(pqtab),[P,Q]);
if(j==0,listput(pqtab,[P,Q]),
    j=1; while(pqtab[j] != [P,Q],j=j+1);
j = j - 1;
period = i-j);
}

if(period != -1, print(c "j " period), print(-1));
}

A.2 Browkin’s Algorithms

/*---------------------------------------------------------------------*
* Description: Displays the BrowkinI continued fraction for a p-adic *
* square root to a specified number of terms and quits *
* if it becomes periodic *
* *
* Arguments: c - some integer to take the square root of *
* p - prime giving the p-adic field *
* n - number of terms to compute *
* *
* Output: BrowkinI continued fraction of c to n terms *
*---------------------------------------------------------------------*/
browkinIp(c,p,n)=
{ local(period=-1,str="[",a=sqrt(c+O(p^prec)),b,i=0,P=0,Q=1,j);
pqtab = listcreate(n+1);
listput(pqtab,[P,Q]);
while((i <= n)&&(period==-1),
```


```plaintext
i = i+1;
if(truncate(a) == 0, break);
b = padicfloor2(a,p);
if(b==-1,break);
if(a-b==0, break);
str = concat(concat(str,b),", ");
a = 1/(a-b);
P=b*Q-P;
Q=(c-P^2)/Q;
j = setsearch(Set(pqtab),[P,Q]);
if(j==0,listput(pqtab,[P,Q]),
j=1; while(pqtab[j] != [P,Q],j=j+1);
j = j - 1;
period = i-j);

str=concat(str,"\]");
if(period!=-1,print(str)); print(c" "j" "period)
}

/*---------------------------------------------------------------------*
* Description: Displays the BrowkinI PQ table for a given number of * *
* lines *
* *
* Arguments: c - integer *
* p - prime giving the p-adic field *
* n - number of lines to compute *
* *
* Output: First n lines of the BrowkinI PQ table for sqrt(c) *
*---------------------------------------------------------------------*/
browkinIPQn(c,p,n)=
{ local(xi=sqrt(c+O(p^prec)),P=0,Q=1,a,i=0);
print("n Pn Qn an");
while(i <= n,
a=padicfloor2(xi,p);
print(i" P" "Q" "a");
if(xi-a==0, break);
xi = 1/(xi-a);
P = a*Q-P;
Q = (c-P^2)/Q;
i = i+1)
}

/*---------------------------------------------------------------------*
* Description: Displays the BrowkinII continued fraction for a p-adic * *
* number to a specified number of terms *
* *---------------------------------------------------------------------*/
```
* Arguments: c - some p-adic number
  p - prime giving the p-adic field
  n - number of terms to compute

* Output: BrowkinII continued fraction of c to n terms

browkinII(c,p,n)=
{ local(str="[",a=c,b,i=0);
  b = browkins1pp(a,p);
  while(i < n, 
    if(a-b==0, break);
    str = concat(concat(str,b),", ");
    i = i+1;
    a = 1/(a-b);
    if(i%2==1,b=browkins2pp(a,p),b=browkins1pp(a,p)) ;
  );
  concat(concat(str,b),"]");
}

browkinIPQn(c,p,n)=
{ local(str="[",a=sqrt(c+O(p^prec)),b,i=0,P=0,Q=1);
  b = browkins1pp(a,p);
  print("n Pn Qn an");
  while(i < n, 
    print(i" "P" "Q" "b);
    if(a-b==0, break);
    str = concat(concat(str,b),", ");
    i = i+1;
    a = 1/(a-b);
    P = b*Q-P;
    Q = (c-P^2)/Q;
    if(i%2==1,b=browkins2pp(a,p),b=browkins1pp(a,p)) ;
  );
  concat(concat(str,b),"]");
}
/* Description: Displays the BrowkinIII continued fraction for a p-adic number to a specified number of terms
   * Arguments: c - integer
   * p - prime giving the p-adic field
   * n - number of terms to compute
   * Output: BrowkinIII continued fraction of sqrt(c) to n terms
   *---------------------------------------------------------------------*/

browkinIII(c,p,n)=
{ local(str="[",a=sqrt(c+O(p^prec)),b,i=0,P=0,Q=1);
  b = browkins1ppp(a,p,1,1);
  while(i < n,
    if(a-b==0, break);
    str = concat(concat(str,b),", ");
    i = i+1;
    a = 1/(a-b);
    P = b*Q-P;
    Q = (c-P^2)/Q;
    if(i%2==1,b=browkins2ppp(a,p,P,Q),b=browkins1ppp(a,p,P,Q))
  );
  concat(concat(str,b),"]");
}

/* Description: Displays the BrowkinIV continued fraction for a p-adic number to a specified number of terms
   * Arguments: c - integer
   * p - prime giving the p-adic field
   * n - number of terms to compute
   * Output: BrowkinIV continued fraction of sqrt(c) to n terms
   *---------------------------------------------------------------------*/

browkinIV(c,p,n)=
{ local(str="[",a=sqrt(c+O(p^prec)),b,i=0,P=0,Q=1);
  b = browkins1p4(a,p,0,1);
  while(i < n,
    if(a-b==0, break);
    str = concat(concat(str,b),", ");
    i = i+1;
    a = 1/(a-b);
    P = b*Q-P;
    Q = (c-P^2)/Q;
if(i%2==1, b = browkins2p4(a,p,P,Q), b = browkins1p4(a,p,P,Q))
);
concat(concat(str, b), "]");
}

/*---------------------------------------------------------------------*
* Description: Displays the PQ table for the BrowkinIV continued frac-
* tion of a p-adic square root to a specified number of lines
* Arguments: c - integer
* p - prime giving the p-adic field
* n - number of lines to compute
* Output: PQ table of the BrowkinIV continued fraction of sqrt(c) to n lines
---------------------------------------------------------------------*/

browkinIVPQn(c,p,n)=
{ local(str="[", a = sqrt(c+O(p^prec)), b, i=0, P=0, Q=1);
b = browkins1p4(a,p,0,1);
print("n Pn Qn an");
while(i < n,
 print(i" "P" "Q" "b);
 if(a-b==0, break);
 str = concat(concat(str, b), ", ");
 i = i+1;
 a = 1/(a-b);
P = b*Q-P;
Q = (c-P^2)/Q;
if(i%2==1, b = browkins2p4(a,p,P,Q), b = browkins1p4(a,p,P,Q))
)
}

browkinIVp(c,p,n)=
{ local(period=-1, a = sqrt(c+O(p^prec)), b, i=0, P=0, Q=1, pqtab, j);
pqtab = listcreate(n+1);
listput(pqtab,[P,Q]);
b = browkins1p4(a,p,0,1);
while((i < n)&&(period==-1),
 if(a-b==0, break);
 i = i+1;
 a = 1/(a-b);
if(truncate(a) == 0, break);
P = b*Q-P;
Q = (c-P^2)/Q;
if(i%2==1, b = browkins2p4(a,p,P,Q), b = browkins1p4(a,p,P,Q))
)
j = setsearch(Set(pqtab), [P,Q]);
if(j==0,listput(pqtab,[P,Q]),
    j=1; while(pqtab[j] != [P,Q], j=j+1);
    j = j - 1;
    period = i-j);
)

if(period == -1,print(c" has NP for "n"..............."));
}
browkinIVp2(c,p,n)=
{ local(period=-1,a=sqrt(c+O(p^prec)),b,i=0,P=0,Q=1,pqtab,j);
    pqtab = listcreate(n+1);
    listput(pqtab,[P,Q]);
    b = browkins1p4(a,p,0,1);
    while((i < n)&&(period==-1),
        if(a-b==0, break);
        i = i+1;
        a = 1/(a-b);
        P = b*Q-P;
        Q = (c-P^2)/Q;
        if(i%2==1,b=browkins2p4(a,p,P,Q),b=browkins1p4(a,p,P,Q));
        j = setsearch(Set(pqtab),[P,Q]);
        if(j==0,listput(pqtab,[P,Q]),period=i-j+2;j=j-2)
    );
    if(c%1000==1, print("...got to "c));
    period
}

/*******************************************************************/
browkins1(c,p)= /* used in Algorithm II */
{   padicfloor2(c,p)
}

browkins1p(c,p)= /* used in Algorithm II */
{   local(s1=padicfloor2(c,p));
    s1-p*sign(s1)
}

browkins2(c,p)= /* used in Algorithm II */
{   local(val=valuation(c,p),intpart=0,cp=c,addpart);
    while(val <= -1,
        addpart = lift(Mod(cp/(p^val),p));
        if(addpart > (p-1)/2, addpart=addpart-p);
```
addpart = addpart*p^val;
intpart = intpart+addpart;
cp = cp-addpart;
val = valuation(cp,p));

intpart
}
browkins2p(c,p)= /* used in Algorithm II */
{ local(s2=browkins2(c,p));
    s2-sign(s2)
}
browkins1pp(c,p)= /* used in Algorithm II */
{ browkins1(c,p)
}
browkins2pp(c,p)= /* used in Algorithm II */
{ local(s2=browkins2(c,p));
    if(valuation(c-s2,p)==0,s2,browkins2p(c,p))
}
browkins1ppp(c,p,P,Q)= /* used in Algorithm III */
{ local(s1=browkins1(c,p));
    if(sign(s1)==sign(P*Q),s1,browkins1p(c,p))
}
browkins2bar(c,p,P,Q)= /* used in Algorithm III */
{ local(s2=browkins2(c,p));
    if(sign(s2)==sign(P*Q),s2,browkins2p(c,p))
}
browkins2ppp(c,p,P,Q)= /* used in Algorithm III */
{ local(s2=browkins2(c,p),s2p=browkins2p(c,p));
    if(valuation(c-s2p,p)>0,s2p,if(valuation(c-s2,p)>0,s2p,browkins2bar(c,p,P,Q)))
}
browkins1p4(c,p,P,Q)= /* used in Algorithm IV */
{ local(s1=browkins1(c,p),slp=browkins1p(c,p),e1=abs(P/Q-s1),e2=abs(P/Q-slp));
    if(e1<e2,s1,slp)
}
```
\texttt{browkins2bar4}(c,p,P,Q) = /* used in Algorithm IV */ \
\{ local(s2=browkins2(c,p),s2p=browkins2p(c,p),e1=abs(P/Q-s2),e2=abs(P/Q-s2p)); \
  if(e1<e2,s2,s2p) \
\}

\texttt{browkins2p4}(c,p,P,Q) = /* used in Algorithm IV */ \
\{ local(s2=browkins2(c,p),s2p=browkins2p(c,p)); \
  if(\text{valuation}(c-s2p,p)>0,s2,if(\text{valuation}(c-s2,p)>0,s2p,browkins2bar4(c,p,P,Q))) \
\}

/* Does a have a non-integer p-adic square root */ 
\texttt{hasproot}(a,p) = \
\{ local(h,ap); \
  if(\text{issquare}(a), return(0)); \
  h = \text{valuation}(a,p); \
  if(h\%2 != 0, return(0)); \
  ap = a/(p^h); \
  if(p>2, if((ap^((p-1)/2))\%p == 1,1,0),if(ap\%8 == 1,1,0)) \
\}

Small changes were made to the above code that allowed us to determine exactly how many partial quotients had been calculated when a calculation terminated without finding a period.

\textbf{A.3 \ Code for Calculations in } \mathbb{F}_p((t))

\texttt{sersqrtp}(alpha,p) = \
\{ local(invec,outvec,vecsize,i,j,b,bzeroinv); \
  /* create vectors for series */ 
  invec = \text{Vec}(alpha); 
  vecsize = \text{matsize}(invec)[2]; 
  outvec = \text{vector}(vecsize); 
  /* calculate coefficients */ 
  outvec[1] = \text{lift}(\text{sqrt}(\text{Mod}(\text{invec}[1],p)))); 
  bzeroinv = \text{lift}(\text{Mod}(\text{outvec}[1],p)); 
  for(i=1,vecsize-1, 
    b = \text{lift}(\text{Mod}(2,p)^{-1})*\text{invec}[i+1]; 
    if(i\%2==0, b = b-\text{lift}(\text{Mod}(2,p)^{-1})*\text{outvec}[i/2+1]^2); 
    for(j=1,\text{floor}((i-1)/2), b = b - \text{outvec}[j+1]*\text{outvec}[i-j+1]); 
    b = bzeroinv*b; 
    outvec[i+1] = b\%p); 
  return(Ser(outvec)) \
sermodp(alpha,p) =
{ local(vec);

vec = Vec(alpha);
vec = vec%p;
return(Ser(vec));
}

serinvp(alpha,p) =
{ local(invec,outvec,vecsize,i,j,b,azeroinv);

/* create vectors for series */
invec = Vec(alpha);
vecsize = matsize(invec)[2];
outvec = vector(vecsize);

/* calculate coefficients */
azeroinv = lift(Mod(invec[1],p)^(-1));
outvec[1] = azeroinv;
for(i=1,vecsize-1,
b = 0;
   for(j=1,i, b = b - invec[j+1]*outvec[i-j+1]);
b = b*azeroinv;
   outvec[i+1] = b%p);
return(Ser(outvec))
}

sercfp(alpha,p,n) =
{ local(outmat,i=0,P=0,Q=1,a,b,rem);

rem = alpha;
outmat = matrix(2,n+2);
outmat[1,1] = 0;
a = polcoeff(rem,0);
outmat[2,1] = a;
if(truncate(rem-a)==0,print("Finite CF");break);
b = valuation(rem-a,x);
outmat[1,2] = x^b;
for(i=1,n,
   rem = serinvp((rem-a)/(x^b),p);
a = polcoeff(rem,0);
outmat[2,i+1] = a;
   if(truncate(rem-a)==0,print("Finite CF");break);
b = valuation(rem-a,x);
outmat[1,i+2] = x^b);
return(outmat)
}

A.4 Other Code

/*---------------------------------------------------------------------*
* Description: computes the Ruban continued fraction for a p-adic    *
* number                                                        *

* Arguments: a - p-adic number                                    *
* p - prime for the p-adic field in which to take the            *
* square root                                                 *
* n - maximum number of terms to compute                        *

* Output: period length and starting point if the first period ends *
* after n terms, -1 otherwise                                    *
*---------------------------------------------------------------------*/
ruban(a,p,n)=
{ local(str="[",b,i=0);
    while(i <= n,
        b = padicfloor1(a,p);
        if(a-b==0, break);
        str = concat(concat(str,b),", ");
        a = 1/(a-b);
        i = i+1
    );
    concat(concat(str,b),"]");
}
rubantest(D,p,n)=
{ local(alpha=0,i=0,enm1=0,Pn=0,Qn=1);
    while(i <= n,
        print(Pn" "Qn);
        alpha = (Pn+sqrt(D+O(p^1000)))/Qn;
        an = padicfloor1(alpha,p);
        en = valuation(an,p);
        anp = an*p^en;
        Pn1 = (anp*Qn-p^en*Pn)/p^enm1;
        Qn1 = (p^enm1+2*en*D-p^enm1*(Pn1)^2)/(p^en*Qn);
        enm1=en;
        Pn = Pn1;
        Qn = Qn1;
        i = i + 1);
}
/**
 * Description: integral part of a p-adic number assuming \{0,1,\ldots,p-1\}
 * are the digits used for the p-adic expansion
 *
 * Arguments: c - p-adic number
 * p - prime for the p-adic field in which to take the
 *
 * Output: integral part of c (part of the series with non-positive
 * powers of p)
 */

padicfloor1(c,p)=
{ local(val=valuation(c,p),intpart=0,cp=c,addpart);

    while(val <= 0,
        cpp = cp/(p^(val));
        addpart = lift(Mod(cpp,p))*p^val;
        intpart = intpart+addpart;
        cp = cp-addpart;
        val = valuation(cp,p));

    intpart
}

/**
 * Description: integral part of a p-adic number assuming \{-\frac{p-1}{2},
 * \ldots,-1,0,1,\ldots,\frac{p-1}{2}\} are the digits used for the
 * p-adic expansion
 *
 * Arguments: c - p-adic number
 * p - prime for the p-adic field in which to take the
 *
 * Output: integral part of c (part of the series with non-positive
 * powers of p)
 */

padicfloor2(c,p)=
{ local(val=valuation(c,p),intpart=0,cp=c,addpart);

    while(val <= 0,
        addpart = lift(Mod(cp/(p^val),p));
        if(addpart > (p-1)/2, addpart=addpart-p);
        addpart = addpart*p^val;
        intpart = intpart+addpart;
        cp = cp-addpart;
        val = valuation(cp,p));

    intpart
}
References


