
Politecnico di Torino

ScuDo
Scuola di Dottorato ~ Doctoral School
WHAT YOU ARE, TAKES YOU FAR

Doctoral Dissertation
Doctoral Program in Pure and Applied Mathematics ($37^{th}$cycle)

# Advances in the theory of $p$–adic continued fractions

By

Giuliano Romeo

******

**Supervisors:**
Prof. Danilo Bazzanella
Prof. Nadir Murru

2024

# Declaration

I hereby declare that, the contents and organization of this dissertation constitute my own original work and does not compromise in any way the rights of third parties, including those relating to the security of personal data.

Giuliano Romeo
2024

* This dissertation is presented in partial fulfillment of the requirements for **Ph.D. degree** in the Graduate School of Politecnico di Torino (ScuDo).

# Abstract

Continued fractions have been studied in mathematics for centuries and have been generalized in several ways for different reasons. The study of $p$–adic continued fractions has started around 1940 with a question of Mahler and the first algorithms have been defined by Ruban, Schneider and Browkin around the 1970. The main goal is to replicate, inside the field of $p$–adic numbers $\mathbb{Q}_p$, all the optimal properties that continued fractions share in the field of real numbers. Several results on continued fractions regarding convergence, finiteness, approximation and periodicity have been proved in $\mathbb{Q}_p$. However, some of the nice properties of real continued fractions do not generalize very well, due to the very different structure of $\mathbb{Q}_p$ and the different properties of the $p$–adic absolute value. The main still open problem is to find an algorithm that provides a periodic $p$–adic continued fraction for any quadratic irrational, i.e. an analogue of the famous Lagrange's Theorem. The results contained in this thesis move toward this direction. In particular, we study the convergence, the finiteness and the periodicity of many algorithms and we search for other new algorithms sharing better properties than the existent ones. We start by studying the properties of periodicity of *Browkin II*, that is the algorithm that seemingly provides more periodic representations for quadratic irrationals. We highlight that it does not share good properties of pure periodicity and, unlike continued fractions in the real field, the length of the pre-period is variable and it is not possible to predict where the period starts. Therefore, we define some new algorithms to improve these periodicity properties. In order to do that, we prove some effective characterizations for the convergence of continued fractions in $\mathbb{Q}_p$. These results provide the explicit shape of the partial quotients for defining convergent $p$–adic continued fractions, therefore they open the way for the exploration of new algorithms. We use these

results to define a new algorithm, obtained as a modification of *Browkin II*, that shares better properties of periodicity from both a theoretical and a computational point of view. Finally, we propose a novel approach to disprove Lagrange's Theorem for *Browkin-type* continued fractions, i.e. those allowing negative partial quotients, that is a well studied open problem. We prove that a necessary condition for the periodicity of $p$–adic continued fractions is the convergence of the continued fraction in $\mathbb{R}$ to the real embedding of the same quadratic irrational. We use this necessary condition to develop a probabilistic argument for the non-periodicity of *Browkin-type* continued fractions, reasoning on the expected size of the partial quotients in Euclidean absolute value. In the final section, we briefly summarize some results about other research topics, namely universal quadratic forms over number fields, linear recurrence sequences and some cryptographic methods for blockchain applications.

# Preface

This thesis is based on the main topic of my Ph. D., which is the study of continued fractions in the field of $p$–adic numbers. The whole discussion and the organization of the sections roughly follows that of my survey paper:

G. Romeo,
*Continued fractions in the field of $p$–adic numbers*, Bulletin of the American Mathematical Society **61**(2) (2024), 343-371.
DOI: https://doi.org/10.1090/bull/1819.

Parts of the original results and ideas on $p$–adic continued fractions have appeared in the following publications:

N. Murru, G. Romeo,
*A new algorithm for $p$–adic continued fractions*, Mathematics of Computation **93**(347) (2024), 1309–1331.
DOI: https://doi.org/10.1090/mcom/3890.

N. Murru, G. Romeo, G. Santilli,
*On the periodicity of an algorithm for $p$–adic continued fractions*, Annali di Matematica Pura ed Applicata **202**(6) (2023), 2971–2984.
DOI: https://doi.org/10.1007/s10231-023-01347-6.

N. Murru, G. Romeo, G. Santilli,
*Convergence conditions for $p$–adic continued fractions*, Research in Number Theory **9**(3) (2023), 66.
DOI: https://doi.org/10.1007/s40993-023-00470-w.

The section containing computational conjectures and open problems has recently become a preprint:

G. Romeo,
*Real convergence and periodicity of p–adic continued fractions*, preprint (2024), arXiv: arXiv:2410.09215.

In the final section at the end of this thesis, it is briefly summarized the content of other works not strictly connected to $p$–adic continued fractions:

G. Alecci, P. Miska, N. Murru, G. Romeo,
*On alternative definition of Lucas atoms and their p-adic valuations*, preprint (2023), arXiv: arXiv:2308.10216.

O. Chwiedziuk, M. Doležálek, E. Pěchoučková, Z. Pezlar, O. Prakash, G. Romeo, A. Růžičková, M. Zindulka,
*Representing rational integers by generalized quadratic forms over quadratic fields*, preprint (2024), arXiv: arXiv:2403.07171.

A. J. Di Scala, A. Gangemi, G. Romeo, G. Vernetti,
*Special subsets of addresses for blockchains using the secp256k1 curve*, Mathematics, **10**(15):2746 (2022).
DOI: https://doi.org/10.3390/math10152746.

V. Kala, J. Krásenský, G. Romeo,
*Universality criterion sets for quadratic forms over number fields*, preprint (2024), arXiv: arXiv:2410.22507.

# Contents

# Chapter 1

# Introduction

Continued fractions are objects of the form

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \ddots}}, \tag{1.1}$$

and they have a long history in mathematics. Their study begins more than 2000 years ago with the division algorithm, defined by Euclid in his famous "Elements", around 300 BC. However, the first main developments and modern formalization of the basic theory of continued fractions is due to Euler in 1744 [29]. Since then, continued fractions have been extensively explored, mainly due to their excellent properties of approximations of real numbers. The first proof of irrationality of $\pi$, that has been carried out by Lambert in 1761 [48], exploits a particular continued fraction expansion for $\tan(x)$. In 1844, Liouville [52] used continued fractions to provide the first example of a transcendental number. Liouville proved that algebraic numbers do not admit infinitely many "too good" approximations (Liouville's inequality), and used continued fractions to construct some real numbers that are approximated "too well" to be algebraic. Before Liouville, the existence of numbers that are not algebraic was not known for sure. In fact, Cantor's argument on the countability of algebraic numbers has been proposed later on in 1874 [18]. Moreover, although $\pi$ and $e$ were conjectured to be transcendental numbers, it was proved only few years later by Hermite in 1873 [37], for the

transcendence of $e$, and by Lindemann in 1882 [51], for the transcendence of $\pi$. In the last two centuries, continued fractions have been among the most efficient tools to create new transcendental numbers, through a generalization of Liouville approach. In this sense, a particular attention should be given to the pioneering works of Baker in 1962 [4] and Adamczewski and Bugeaud in 2005 [2] and the many subsequent improvements.

A real number has a finite continued fraction if and only if it is a rational number, as an easy consequence of the finiteness of the Euclidean division algorithm. Instead, infinite periodic continued fractions in $\mathbb{R}$ represent algebraic irrational numbers that are quadratic over $\mathbb{Q}$. In fact, by requiring the periodicity, a continued fraction satisfies a polynomial relation of degree 2, which was already known by Euler. In 1776, Lagrange [47] proved that also the converse holds, i.e. every real quadratic irrational can be expressed as a periodic continued fractions. This result is surprising for several reasons, that can be also dated back to the ancient Greece. Indeed, it is likely that the first to prove the irrationality of $\sqrt{2}$ was a Pythagorean, Hippasus of Metapontum. Legend says that for this discovery Hippasus has been sentenced to death by Pythagora, and has been drowned, offshore in Crotone's sea. The reason was that Pythagora could not stand the idea of the existence of incommensurable numbers, that are not representable by means of integers. In this sense, Lagrange's Theorem gives for the first time (around 2000 years after Hippasus' sacrifice) a very elegant expression to irrational numbers, even if just to quadratic ones, that uses only positive integer numbers (for example, the expansion of $\sqrt{2}$ is $[1,\overline{2}]$). In order to get an analogue of Lagrange's Theorem for algebraic irrationalities of degree higher than two, a multidimensional generalization of continued fraction has been defined. Motivated by a question of Hermite [38], Jacobi [41] introduced a continued fraction algorithm with the purpose of providing periodic representations for cubic irrationals, in the spirit of Lagrange's Theorem. Later on, Perron [62] generalized Jacobi's approach in order to handle algebraic irrationalities of any degree. However, as it sometimes happens in mathematics, all the theory of continued fractions does not generalize so easily to higher dimensions. In fact, it is still not known if Jacobi's algorithm becomes periodic for every real cubic irrational and, in

general, Hermite's problem for multidimensional continued fractions is still open.

Because of all these optimal properties that we have mentioned up to now, continued fractions have been studied and employed in various areas of mathematics and there exist several generalizations of the classical theory of continued fractions. The main topic of this thesis is the study of continued fractions defined over the field of $p$–adic numbers $\mathbb{Q}_p$.

In 1940, Mahler [54] raised the problem of defining continued fractions over $\mathbb{Q}_p$. The $p$–adic numbers have been introduced in 1897 by Hensel [36], who took insipiration from the work of Kummer on ideal numbers [44, 45]. In fact, Kummer implicitly used the $p$–adic valuation of prime ideals appearing in the ideal factorization of integers over cyclotomic fields. The original idea of Hensel was to provide a tool to obtain some "local" information near the prime $p$, in analogy with Laurent series in powers of the irreducible monomials $(X-\alpha)$, that are used to obtain information "around the point $\alpha$". The field of $p$–adic numbers is constructed as the completion of the field of rational numbers $\mathbb{Q}$ with respect to the $p$–adic absolute value. The completion is the smallest field containing $\mathbb{Q}$ in which all Cauchy sequences are convergent. Besides the standard Euclidean one, the $p$–adic absolute values are, up to equivalences, the only non-trivial absolute values over $\mathbb{Q}$ (Ostrowski's Theorem). Therefore, the field of $p$–adic numbers $\mathbb{Q}_p$ are the only non-trivial completions of $\mathbb{Q}$ different from $\mathbb{R}$.

The $p$–adic approach turns out to be striking in many senses. Perhaps, the most important applications lie in the the so-called *local-global principle*, originally introduced by Hasse [34]. The *local-global principle* is the idea of obtaining global information (for example, over $\mathbb{Q}$) by looking only at local information (over $\mathbb{R}$ and $\mathbb{Q}_p$). For instance, an equation that has a solution in $\mathbb{Q}$ (globally) clearly has a solution in $\mathbb{R}$ and in every $\mathbb{Q}_p$ (locally), but the converse is false: an equation that has a real root (or a $p$–adic root) not necessarily has a rational root. However, in some specific cases, it is possible to recover a solution over $\mathbb{Q}$ by having solutions over $\mathbb{R}$ and over $\mathbb{Q}_p$ for all

$p$. One of the first major result in this direction is the Hasse-Minkowski Theorem, stating that a quadratic form has a root in $\mathbb{Q}$ if and only if it has a root in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all $p$ (see, for example, [35, 72]). The actual result concerns any number field (and in general any global field) and its completions. Hasse-Minkowski Theorem and *local-global* principle suggest that, sometimes, the study of mathematical objects only inside the field of real numbers can be "not enough". For all these reasons, and many others, the field of $p$–adic numbers is nowadays largely studied in the whole mathematics.

The problem of defining a continued fraction in $\mathbb{Q}_p$ sharing all the optimal properties enjoyed by classical continued fractions is still open. In particular, it is not known an algorithm that provides periodic representations for every $p$–adic quadratic irrational. Hence, $p$–adic continued fractions miss, up to now, an analogue of Lagrange's Theorem. This is one of the main great goal I kept in mind when facing the research problems in this area, and it is one of the central focus of this thesis.

The main issue is that in $\mathbb{Q}_p$ there is not an intuitive satisfying definition for the integer part of a $p$–adic number, as we have for real numbers. There are at least two very natural definitions, due to Schneider [73] and Ruban [69], both around 1970. The two algorithms try to replicate the standard algorithm for real continued fractions in two different senses. In fact, for some reasons of $p$–adic convergence that we discuss more thoroughly in the next sections, a "classical" continued fraction, meaning that we have all numerators equal to 1 and the partial quotients are integer, can never converge to a $p$–adic number. Schneider's algorithm overcomes this problem by allowing non-unitary numerators, and the partial quotients are integers. Ruban's algorithm, instead, has unitary denominators, but the partial quotients are rational numbers, with powers of the prime $p$ appearing at the denominator. Ruban's and Schneider's continued fractions are not finite for every rational number, but they can also be infinite periodic [17, 49]. This is very annoying, since we miss one of the first and most important properties of continued fractions in $\mathbb{R}$. Moreover, the two algorithms do not provide a periodic continued fraction for every $p$–adic quadratic irrational. In fact, the analogues of Lagrange's Theorem

have been disproved in [74] for Schneider's algorithm and in [22] for Ruban's algorithm.

In 1978, Browkin [15] came out with the definition of a new $p$–adic continued fractions algorithm (we call it *Browkin I*) that terminates if and only if the input is a rational number. This algorithm is really similar to Ruban's one, but it allows to have also negative numbers as partial quotients. The problem of understanding if Browkin's continued fractions are always periodic for $p$–adic quadratic irrationals is still open. Trying to find a way to prove or disprove Lagrange's Theorem for Browkin's continued fraction has taken some energies out of me in the last 3 years. For the moment it seems to me, for my humble opinion and knowledge, a hard problem, that needs some fresh novel technique to be tackled. However, although a proof has not been provided yet, I believe Lagrange's Theorem to fail also for Browkin's algorithm. In 2000, more than 20 years after his first algorithm, Browkin [16] proposed a second algorithm (we call it *Browkin II*) that allows to have integer partial quotients for half of the steps, and for the other half it keeps rational partial quotients with powers of $p$ at the denominator. This choice is possible due to a less restrictive convergence condition that Browkin proved in [16]. This second algorithm computationally appears to outperform the first algorithm in the number of periodic continued fractions provided for quadratic irrational numbers. For example, see Chapter 7, that is based on the computational analysis we carried out in [55]. In particular, in Figure 7.1, it is possible to see how much better *Browkin II* behaves compared with *Browkin I*. But again, this is only heuristic and experimental, since no quadratic irrational has been proved yet to have non-periodic *Browkin I* or *Browkin II* continued fractions.

This is roughly the starting point of my research in this field.

In [56], we studied the properties of periodicity of *Browkin II* from a theoretical point of view, in order to better understand its behaviour. A famous result for real continued fractions, proved by Galois [30], states that the continued fraction of $\alpha$ is purely periodic if and only if $|\alpha| > 1$ and $-1 < \overline{\alpha} < 0$, where $|\cdot|$ is the Euclidean absolute value and $\overline{\alpha}$ is the conjugate

over $\mathbb{Q}$ of the quadratic irrational $\alpha$. Another famous result provides a nice form for the continued fractions of pure square roots of integers. In fact, for $D > 0$ non-square integer, the continued fraction of $\sqrt{D}$ is

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

where the $a_n$ are positive integers and the sequence $a_1, \ldots, a_n$ is palindromic. For *Browkin I*, some very similar results have been proved by Bedocchi in [8, 9], and our main goal in [56] has been to generalize them also to *Browkin II*, for which very few remarks were done before. The results of Bedocchi, and in general all the results regarding the periodicity, are stated in Chapter 6. The best analogue of Galois' and Bedocchi's theorems that we were able to obtain is Theorem 6.2.10, where the condition on the $p$–adic absolute value of $\alpha$ is only necessary for the pure periodicity, but not sufficient, and we have many counterexamples. Moreover, in Theorem 6.2.17 we proved that the pre-period of periodic *Browkin II* continued fractions of square roots of integers can have a period of length 1 or even. This result does not seem improvable, since we observed periods of many even lengths. Therefore, the two results that hold in the real framework and for *Browkin I*, fail to hold for *Browkin II*. Notice that both Bedocchi's and our results are proved under the hypothesis of periodicity, that can not be removed. Therefore, these properties of periodicity hold "whenever the continued fraction is periodic". This is in big contrast with continued fractions in $\mathbb{R}$, where, for example in the two results that we have recalled, this hypothesis is not required as the periodicity is much better understood.

In [57], we started searching for further possible generalizations of *Browkin II*. We proved with the constructive Example 4.3.1 in Chapter 4, that a generalization where one partial quotient has negative valuation and two partial quotients have null valuation, not necessarily converge without a stronger hypothesis. In fact, it is not hard to see, and we show it at the begin of Chapter 4, that a continued fraction converges in $\mathbb{Q}_p$ if and only if the sequence of valuations of consecutive denominators of convergents tends to $-\infty$. One of our main results in [57] is the explicit characterization of

the strict decrease of this sequence, in terms of the valuation of the partial quotients, that is much easier to handle. This characterization is stated in Theorem 4.2.1 where we prove that having one negative partial quotient each two steps is a necessary and sufficient the strict decrease of the sequence of denominators, that guarantees the convergence. Instead, if we want to have one partial quotient with negative valuation each $r$ steps, with $r \geq 3$, we need to add some extra hypotheses on the valuations of some products of partial quotients. For the case $r = 3$, it is Theorem 4.3.2, where we add only one hypothesis to obtain the convergence of a "3-steps" algorithm. For this case, in the same paper we introduced two new algorithms that fulfill the hypotheses of Theorem 4.3.2 and they are defined in Chapter 3 as Algorithm (3.8) and Algorithm (3.9). We prove, in Theorem 5.2.1, that one of them provides a finite continued fraction for all rational numbers. However, their periodicity properties do not seem, experimentally, to improve those of *Browkin II*. Also for any $r \geq 4$, we proved some sufficient conditions for the convergence of a "$r$-steps" algorithm, that are contained in Theorem 4.3.6. For bigger $r$, the hypotheses of Theorem 4.3.6 become more difficult to fulfill, and probably not leading to an improvement of the performance, therefore we did not define any algorithm for $r \geq 4$.

The convergence results proved in [57] paved the way for the exploration of new possible algorithms for $p$–adic continued fractions. In particular, Theorem 4.2.1 has been practically used in some recent works by Yasutomi [79] and by Deng and Wang [26], in order to easily prove the $p$–adic convergence of their algorithms. We also used Theorem 4.2.1 in [55], in order to define a new algorithm, Algorithm (3.10) in Chapter 6, that is a slight modification of *Browkin II*. As we explain at the end of Section 6.2, the main obstruction that we had to deal with in [56] for obtaining results on the periodicity of *Browkin II*, is the presence of the *sign* function in (3.6). In the new algorithm introduced in [55], the *sign* function is not anymore required, thanks to our more general convergence results of [57]. For this new algorithm, finite continued fractions characterize rational numbers. Moreover, both a necessary and a sufficient conditions for the pure periodicity hold, therefore obtaining a proper analogue of Galois' Theorem and Bedocchi's Theorem, that is Theorem 6.3.1.

In Proposition 6.3.3 we also proved that $p$–adic square roots of integers, that have a periodic continued fraction, have always pre-period 1, as it is for real continued fractions. Finally, this new algorithm improves also experimentally the properties of *Browkin II*, and the results are listed in Chapter 7. In particular, in Figure 7.1 it is possible to see a comparison of the number of periodic continued fractions for $p$–adic square roots of integers with *Browkin I*, *Browkin II* and the new algorithm (detected within a fixed number of steps, as no quadratic irrational has been proved to have non-periodic continued fraction with these three algorithms). The SageMath code developed for Chapter 7, which is based on the computational section of [55], is publicly available[1] and contains also the implementation of all the main algorithms presented in Chapter 3.

The final Chapter 8 collects some conclusions, open problems and future directions that we are trying or have tried to follow, mainly to prove the non-periodicity of Browkin's algorithms. The core idea is contained in Conjecture 8.1.4, saying that the $p$–adic continued fraction of a quadratic irrational obtained by *Browkin I*, *Browkin II* or our Algorithm (3.10) becomes eventually periodic if and only if the continued fraction converges in $\mathbb{R}$ to the "same" quadratic irrational. One implication is true by a known result of convergence of periodic continued fractions. Therefore, if the continued fraction is periodic, it converges to a root of the same polynomial both in $\mathbb{R}$ and in $\mathbb{Q}_p$. However, when the $p$–adic continued fraction of a quadratic irrational $\alpha$ does not show a period for a lot of steps, it seems to be convergent in $\mathbb{R}$ very neetly, but toward something really different than the image of $\alpha$ inside $\mathbb{R}$. Proving that it is actually convergent to something different from $\alpha$ would be a counterexample to Lagrange's Theorem for Browkin-type algorithms, that is not known at the present time. In the second part of Chapter 8, we develop a probabilistic argument for the size of convergents, under the assumption of uniform distribution of the $p$–adic digits of irrational numbers. The assumption of uniform distribution is reasonable, and connected to several hard and ancient conjectures on the so-called normal numbers. Under this hypothesis, we prove that the expected value of the size of the partial quotients

[1] https://github.com/giulianoromeont/p-adic-continued-fractions

increases linearly with the prime $p$. Therefore, especially for large values of $p$, the denominators $B_n$ tend to be really big, since they grow esponentially in the partial quotients. Hence, the convergents are not expected to oscillate too much after several steps. We state it as Conjecture 8.2.10 at the end of the thesis, saying that the sequence of denominators $|B_n|$ of Browkin-type continued fractions tends to $+\infty$ with probability 1. These reasonings have been recently included in [66].

The thesis is organized as follows.

In Chapter 2 we recall some notation and known facts for the classical theory of continued fractions in $\mathbb{R}$ and for the field of $p$–adic numbers $\mathbb{Q}_p$.

In Chapter 3, we describe the various algorithms that have been defined over the years, underlining their motivations and their main properties, together with their issues.

In Chapter 4, we discuss the $p$–adic convergence of a continued fraction, which is the very first requirement for the definition of an algorithm.

In Chapter 5, we present the properties of the expansions of rational numbers that, as already mentioned, are not always finite in the field of $p$–adic numbers.

Chapter 6 contains the results related to the periodicity of $p$–adic continued fractions and the main developments towards a $p$–adic analogue of Lagrange's Theorem.

In Chapter 7, we show some experimental computations on the properties of periodicity of the main algorithms.

In Chapter 8, we investigate the main open problems and summarize some possible strategies.

Finally, Chapter 9 summarizes the content of other works, in [3, 23, 27, 42], that I have developed during my Ph. D. together with other collaborators and are not based on the study of $p$–adic continued fractions.

# Chapter 2

# Preliminaries and notation

## 2.1 Continued fractions

In this section, we provide a short introduction to the theory of continued fractions. Some good sources on the topic are [43, 58].

We call *continued fraction* an object of the form

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \ddots}}, \tag{2.1}$$

and we denote it by

$$\begin{bmatrix} b_1 & b_2 & \dots & \\ a_0 & a_1 & a_2 & \dots \end{bmatrix},$$

where the coefficients $a_n$ and $b_n$ are elements in a field and the expansion can be either finite or infinite. If $b_n = 1$ for all $n \in \mathbb{N}$, the continued fraction is called *simple*, that is

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}},$$

and we denote it by $[a_0, a_1, a_2, \ldots]$. The coefficients $a_0, a_1, a_2 \ldots$ are called *partial quotients*. For all $n \in \mathbb{N}$, the rational number

$$\frac{A_n}{B_n} = \left[\begin{array}{ccccc} b_1 & \ldots & b_{n-1} & b_n & \\ a_0 & a_1 & \ldots & a_{n-1} & a_n \end{array}\right] = a_0 + \cfrac{b_1}{a_1 + \ddots + \cfrac{b_{n-1}}{a_{n-1} + \cfrac{b_n}{a_n}}},$$

corresponding to the continued fraction stopped at the $n$-th term, is called $n$-th *convergent* of the continued fraction. The $A_n$'s are called *partial numerators* and the $B_n$'s are called *partial denominators*. The sequences $\{A_n\}_{n\in\mathbb{N}}$ and $\{B_n\}_{n\in\mathbb{N}}$ satisfy the recursions

$$\begin{cases} A_0 = a_0, \\ A_1 = a_1 a_0 + b_1, \\ A_n = a_n A_{n-1} + b_n A_{n-2}, \quad n \geq 2, \end{cases} \qquad \begin{cases} B_0 = 1, \\ B_1 = a_1, \\ B_n = a_n B_{n-1} + b_n B_{n-2}, \quad n \geq 2. \end{cases} \tag{2.2}$$

The partial numerators and denominators of the convergents can be represented also using the following matrix form. For all $n \in \mathbb{N}$,

$$\begin{pmatrix} A_n & A_{n-1} \\ B_n & B_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 1 & 0 \\ 0 & b_n \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}. \tag{2.3}$$

Furthermore, for an infinite continued fraction representing an element $\alpha$, we introduce the sequence of *complete quotients* $\{\alpha_n\}_{n\in\mathbb{N}}$ defined, for all $n \in \mathbb{N}$, as

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

starting from $\alpha_0 = \alpha$. In this way, in fact,

$$\alpha_n = a_n + \frac{b_{n+1}}{\alpha_{n+1}}.$$

We say that an infinite continued fraction is *periodic* (or *eventually periodic*) if and only if there exists $h \in \mathbb{N}$ and $k \geq 1$ such that $a_{n+k} = a_n$ and $b_{n+k} = b_n$ for all $n \geq h$. In this case we call *period length* and *pre-period length*, respec-

tively, the least $k$ and $h$ for which this happens (or just *period* and *pre-period* where there is no risk of ambiguity). If $h = 0$, the continued fraction is said *purely periodic* and it means that the period starts from the first partial quotient, without a pre-period. We denote a periodic continued fraction by $[a_0, \dots, a_{h-1}, \overline{a_h, \dots, a_{h+k-1}}]$, where $a_0, \dots, a_{h-1}$ is the pre-periodic part and $\overline{a_h, \dots, a_{h+k-1}}$ is the periodic part.

The standard algorithm to express a real number $\alpha$ through a simple continued fraction $[a_0, a_1, \dots]$ is the following, with $\alpha_0 = \alpha$:

$$\begin{cases} a_n = \lfloor \alpha_n \rfloor \\ \alpha_{n+1} = \frac{1}{\alpha_n - a_n}, \end{cases} \tag{2.4}$$

where $\lfloor \alpha_n \rfloor$ denotes the integer part of $\alpha$, that is the greatest integer $a_n \leq \alpha_n$. If $\alpha_n = a_n$ for some $n \in \mathbb{N}$, then the algorithm terminates and the continued fraction is finite. A finite continued fraction $[a_0, \dots, a_n]$, with $a_n \geq 2$, can be equivalently represented as $[a_0, \dots, a_n - 1, 1]$.

Finally, we briefly recall some important results about continued fractions in $\mathbb{R}$, that we would like to emulate for continued fractions in $\mathbb{Q}_p$. Continued fractions with positive integer partial quotients always converge to some real number, and the approximation provided by the convergents is the best possible (without increasing the denominator of the rational number). More details on the convergence in $\mathbb{R}$ are given in the dedicated Chapter 4. Moreover, In the field of real numbers, continued fractions completely characterize rational numbers and quadratic irrationals. A real number $\alpha \in \mathbb{R}$ is rational if and only if its continued fractions is finite. The latter is an easy consequence of the finiteness of the Euclidean division algorithm in $\mathbb{Z}$. More details are given in Chapter 5. A real number $\alpha \in \mathbb{R}$ is a quadratic irrational, i.e. root of an irreducible rational polynomial of degree 2, if and only if its continued fraction is eventually periodic. The latter is the famous Lagrange's Theorem. More results on the periodicity, together with some comments on the strategies for the proofs, are given at the begin of Chapter 6.

## 2.2 The field of $p$–adic numbers $\mathbb{Q}_p$

In this section, we introduce the field of $p$–adic numbers $\mathbb{Q}_p$ and recall the main properties that are useful for our discussion. For an extensive source on the theory of $p$–adic numbers, see [31].

First, we recall some basic definitions and properties of valuations and absolute values over a field.

**Definition 2.2.1.** *Let $K$ be a field. A valuation over $K$ is a function $v : K \to \mathbb{R} \cup \{\infty\}$ such that*

*i)* $v(x) = \infty$ *if and only if* $x = 0$,

*ii)* $v(xy) = v(x) + v(y)$ *for all* $x, y \in K$,

*iii)* $v(x+y) \geq \min\{v(x), v(y)\}$.

**Definition 2.2.2.** *Let $K$ be a field. An absolute value over $K$ is a function $|\cdot| : K \to \mathbb{R}_+$ such that*

*i)* $|x| = 0$ *if and only if* $x = 0$,

*ii)* $|xy| = |x||y|$ *for all* $x, y \in K$,

*iii)* $|x+y| \leq |x| + |y|$ *for all* $x, y \in K$.

*If the following further condition, stronger than iii), holds:*

*iv)* $|x+y| \leq \max\{|x|, |y|\}$, *for all* $x, y \in K$,

*then the the absolute value $|\cdot|$ is said non-archimedean. Otherwise, it is said archimedean.*

In the following, let $p$ be a prime number. In the next definitions, we introduce the $p$–adic valuation and the $p$–adic absolute value over $\mathbb{Q}$.

**Definition 2.2.3.** *The $p$–adic valuation over $\mathbb{Q}$ is the function $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ defined as follows: for any non-zero $x \in \mathbb{Q}$,*

$$x = \frac{a}{b} p^e, \quad p \nmid ab,$$

*then $v_p(x) = e$. Moreover, we set $v_p(0) = \infty$.*

**Definition 2.2.4.** *The $p$–adic absolute value over $\mathbb{Q}$ is the function $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_+$ defined as follows: for any non-zero $x \in \mathbb{Q}$,*

$$|x|_p = p^{-v_p(x)},$$

*where $v_p(x)$ is the $p$–adic valuation of $x$, and $|0|_p = 0$.*

**Remark 2.2.5.** *It is not hard to see that the $p$–adic valuation is a valuation and that the $p$–adic absolute value is a non-archimedean absolute value, in the sense of Definition 2.2.1 and Definition 2.2.2.*

**Definition 2.2.6.** *Let $|\cdot|_1$ and $|\cdot|_2$ two absolute values over a field $K$. Then we say that $|\cdot|_1$ and $|\cdot|_2$ are equivalent if and only if they induce the same topology over $K$.*

In the following theorem, we see that the standard Euclidean absolute value and the $p$–adic absolute values are, up to equivalences, the only non-trivial absolute values that is possible to define over $\mathbb{Q}$.

**Theorem 2.2.7** (Ostrowski)**.** *Let $|\cdot|$ be a non-trivial absolute value over $\mathbb{Q}$. Then $|\cdot|$ is either equivalent to the Euclidean absolute value or to the $p$–adic absolute value*

**Proposition 2.2.8.** *The field $\mathbb{Q}$ of rational numbers is not complete with respect to any of its non-trivial absolute values.*

The field of $p$–adic numbers $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the $p$–adic absolute value, exactly as $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the Euclidean absolute value. Therefore, $\mathbb{Q}_p$ is the smallest field containing $\mathbb{Q}$ where all Cauchy sequences with respect to $|\cdot|_p$ are convergent. Moreover, $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ with respect to the $p$–adic absolute value. From Ostrowski's theorem, the fields $\mathbb{Q}_p$ are the only non-trivial completions of $\mathbb{Q}$ besides $\mathbb{R}$.

The field of $p$–adic numbers can be proved to be exactly the set of all the finite-tailed series in powers of $p$, that is:

$$\mathbb{Q}_p = \left\{ \sum_{n=-r}^{+\infty} c_n p^n \;\middle|\; r \in \mathbb{Z},\ c_n \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

Moreover, the $p$–adic valuation $v_p(\cdot)$ and the $p$–adic absolute value $|\cdot|_p$ can be extended uniquely from $\mathbb{Q}$ to $\mathbb{Q}_p$.

We also define the set of $p$–adic integers as the set of $p$–adic numbers with non-negative valuation, i.e.

$$\mathbb{Z}_p = \left\{ \sum_{n=0}^{+\infty} a_n p^n \;\middle|\; a_n \in \mathbb{Z}/p\mathbb{Z} \right\}.$$

It is a local ring with unique maximal ideal

$$p\mathbb{Z}_p = \left\{ \sum_{n=1}^{+\infty} a_n p^n \;\middle|\; a_n \in \mathbb{Z}/p\mathbb{Z} \right\},$$

and residue field

$$\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p,$$

that is the finite field of order $p$.

The following is an important property of the convergence in $\mathbb{Q}_p$ that we are going to use in the next sections, and that holds in general for every non-archimedean absolute value.

**Proposition 2.2.9.** *Let $\mathbb{K}$ be a field with a non-archimedean absolute value $|\ |$. A sequence $\{x_n\}$ in $\mathbb{K}$ is a Cauchy sequence if and only if $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$.*

**Remark 2.2.10.** *Notice that Proposition 2.2.9 does not hold in the archimedean setting. In fact, if we consider the harmonic series $\sum_{n=0}^{+\infty} \frac{1}{n}$, then the sequence of partial sums $s_k = \sum_{n=0}^{k} \frac{1}{n}$ does not converge for $k \to +\infty$, as this series is notoriously divergent, and hence is not a Cauchy sequence. However,*

$$\lim_{k\to\infty} |s_{k+1} - s_k| = \lim_{k\to\infty} \frac{1}{k+1} = 0,$$

*i.e. the difference of two consecutive terms tends to $0$. The other implication of Proposition 2.2.9 is of course true also in the archimedean setting, i.e. for any Cauchy sequence that limit tends to $0$.*

Finally, we see how to express rationals and quadratic irrationals inside $\mathbb{Q}_p$, i.e. as a formal series in powers of the prime $p$. Understanding the shape of rationals and quadratic irrationals in $\mathbb{Q}_p$ is important in order to generalize the results of classical continued fractions in the $p$–adic framework. For more detailed results on $p$–adic rational numbers, see the paper of Conrad [24]. For Hensel's Lemma and $p$–adic quadratic irrationals, see Chapter 4 of [31].

Rational numbers have a precise shape inside $\mathbb{Q}_p$, as stated in the next theorem.

**Theorem 2.2.11.** *Let $a \in \mathbb{Q}_p$ be a $p$–adic number. Then $a$ is rational if and only if its $p$–adic expansion*

$$a = a_{-r}\frac{1}{p^r} + \ldots + a_{-1}\frac{1}{p} + a_0 + a_1 p + a_2 p^2 + \ldots$$

*is either finite or eventually periodic.*

From Theorem 2.2.11, we know that the elements in $\mathbb{Q}_p \backslash \mathbb{Q}$ correspond exactly to the infinite and not periodic $p$–adic series. Later on, we are interested in generalizing the results of periodicity that hold in $\mathbb{R}$. In particular, we would like to have Lagrange's Theorem, hence a periodic continued fraction for all $p$–adic quadratic irrational. A $p$–adic quadratic irrational is an element of $\mathbb{Q}_p$ that is the root of a polynomial in $\mathbb{Q}[x]$ of degree 2, irreducible over $\mathbb{Q}$. In several results, we handle square roots $\sqrt{D}$, $D \in \mathbb{Z}$. When $x^2 - D$ splits in $\mathbb{Q}_p$, then it has two roots. In the case of the standard representatives in $\{0, \ldots, p-1\}$, we choose the root that in its $p$–adic expansion has the smaller first representative. In the case of representatives in $\{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\}$ we take the one with positive first representative. We denote the other root by $-\sqrt{D}$. More details are given at the begin of Chapter 6, where we deal with periodic continued fractions and quadratic irrationals.

It is not hard to see that a necessary condition for $\sqrt{D}$ to lie in $\mathbb{Q}_p$ is that $D$ is a quadratic residue modulo $p$. In fact, let

$$\sqrt{D} = a_0 + a_1 p + \ldots,$$

then, squaring both sides we obtain $D = a_0^2 + p(\ldots)$, so that $D \equiv a_0^2 \mod p$. Therefore, if $D$ is not a quadratic residue modulo $p$, then the latter equation is not solvable and $\sqrt{D} \notin \mathbb{Q}_p$. Conversely, if $D$ is a quadratic residue modulo $p$, this means that $X^2 - D$ has a solution in $\mathbb{Z}/p\mathbb{Z}$. It turns out that this condition is also sufficient for $\sqrt{D}$ to lie in $\mathbb{Q}_p$, thanks to the famous Hensel's Lemma.

**Theorem 2.2.12** (Hensel's Lemma)**.** *Let $F(X) = a_0 + a_1 X + \ldots a_n X^n$ a polynomial with coefficients in $\mathbb{Z}_p$. Let us suppose that there is a p–adic integer $\alpha_1 \in \mathbb{Z}_p$ such that:*

$$F(\alpha_1) \equiv 0 \mod p\mathbb{Z}_p, \quad F'(\alpha_1) \not\equiv 0 \mod p\mathbb{Z}_p,$$

*where $F'(X)$ represents the formal derivative of $F(X)$. Then there exists a unique p–adic integer $\alpha \in \mathbb{Z}_p$ such that:*

$$\alpha \equiv \alpha_1 \mod p\mathbb{Z}_p, \quad \text{with} \quad F(\alpha) = 0.$$

Basically, from Hensel's Lemma, if a quadratic equation has a solution $\alpha$ in $\mathbb{Z}/p\mathbb{Z}$, then it can be "lifted" uniquely to a solution in $\mathbb{Z}/p^2\mathbb{Z}$, and then to a solution in $\mathbb{Z}/p^3\mathbb{Z}$ and this process can be continued infinitely, in order to compute the expansion of $\alpha$ in $\mathbb{Q}_p$. From Hensel's Lemma, we obtain the following result on the squares that lie in $\mathbb{Z}_p^*$.

**Corollary 2.2.13.** *Let $b \in \mathbb{Z}_p^*$ a p–adic unit. If exists $\alpha_1 \in \mathbb{Z}_p$ such that $\alpha_1^2 \equiv b \mod p\mathbb{Z}_p$, then $b$ is the square of an element of $\mathbb{Z}_p^*$.*

In order to extend Corollary 2.2.13 to all $p$–adic numbers, we notice that each $\alpha \in \mathbb{Q}_p$ can be written as $\alpha = p^{v_p(\alpha)}\alpha'$, with $\alpha' \in \mathbb{Z}_p^*$. Then $\alpha$ is a square if and only if the valuation $v_p(\alpha)$ is even and $\alpha'$ is a square.

**Corollary 2.2.14.** *Let $\alpha \in \mathbb{Q}_p$. Then $\alpha$ is a square if and only if it can be written as $\alpha = p^{2n}y^2$, where $n \in \mathbb{Z}$ and $y \in \mathbb{Z}_p^*$ is a p–adic unit.*

In the latter results, we have considered only square roots, i.e. the solutions of the irreducible polynomial $X^2 - D$. The exact same construction can be carried out to for a general quadratic irrational, i.e. for solutions in $\mathbb{Q}_p$ of a generic irreducible polynomial of degree 2.

# Chapter 3

# Main definitions of $p$–adic continued fractions

In this chapter we present the main definitions for $p$–adic continued fractions that have appeared in literature. A first attempt is of course trying to emulate the standard algorithm (2.4) for real continued fractions. The problem is that the definition of the integer part of a $p$–adic number $\alpha \in \mathbb{Q}_p$ is not uniquely determined. In $\mathbb{R}$, the integer part of a real number $\alpha$ is defined as the unique integer $a$ less than $\alpha$ for which $|\alpha - a| < 1$. However, for example in $\mathbb{Z}_p$, there are infinitely many integers such that this happens, since there are infinitely many $a \in \mathbb{Z}$ such that $p$ divides $\alpha - a$.

We start by presenting the approach of Schneider [73]. Schneider's continued fraction is not simple but, as in the classical case, it employs only integers. Then we present Ruban's [69] and Browkin's [15, 16] approach, that attempted to construct a simple continued fraction by defining an $p$–adic analogue of the integer part in $\mathbb{R}$. However, in this case, the partial quotients can be either integer or rationals. Finally, we discuss the new algorithms that have been defined in the latest years with the purpose of improving Schneider's, Ruban's and Browkin's $p$–adic continued fraction.

## 3.1 Schneider's definition

The first definition that we are going to analyze is due to T. Schneider [73] in 1969, and it works for all $p$–adic integers. The $p$–adic integers are the elements $\alpha \in \mathbb{Q}_p$ with $v_p(\alpha) \geq 0$. Let us observe that, for $\alpha \in \mathbb{Z}_p$, all the integers $a$ satisfying $0 \leq |\alpha - a|_p < 1$ are congruent modulo $p$. Therefore, it is meaningful to define the partial quotients as the unique representatives of $a$ modulo $p$ that lie inside $\{0, \dots, p-1\}$. Schneider followed this approach to provide a non-simple continued fraction expansion

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \ddots}}, \tag{3.1}$$

for all $p$–adic integers. For $\alpha_0 \in \mathbb{Z}_p$, with expansion

$$\alpha_0 = \sum_{i=0}^{+\infty} c_i p^i, \qquad c_i \in \{0, \dots, p-1\},$$

Schneider's algorithm works as follows. The first partial quotient is $a_0 = c_0$. Then, for all $n \in \mathbb{N}$,

$$\begin{cases} e_{n+1} = v_p(\alpha_n - a_n) \\ b_{n+1} = p^{e_{n+1}} \\ \alpha_{n+1} = \dfrac{b_{n+1}}{\alpha_n - a_n} \\ a_{n+1} = c_0^{(n+1)}, \end{cases} \tag{3.2}$$

where $c_0^{(n+1)}$ denotes the first term of the expansion of

$$\alpha_{n+1} = \sum_{i=0}^{+\infty} c_i^{(n+1)} p^i,$$

which by construction has zero valuation, i.e. it is a unit in $\mathbb{Z}_p$.

**Example 3.1.1.** *Let us give an idea of how Schneider's algorithm* (3.2) *works to provide the* 5*–adic continued fraction of* $\frac{2}{7}$*. In* $\mathbb{Q}_5$*,*

$$\frac{2}{7} = 1+2\cdot 5+5^2+\ldots,$$

*hence* $a_0 = 1$ *and* $e_1 = v_p(\alpha_0 - a_0) = v_p(2\cdot 5+5^2+\ldots) = 1$*. The next complete quotient is then*

$$\alpha_1 = \frac{p^{e_1}}{\alpha_0 - a_0} = \frac{5}{2\cdot 5+5^2+\ldots} = \frac{1}{2+5+\ldots} = 3+3\cdot 5+4\cdot 5^2+\ldots.$$

*Hence,* $a_1 = 3$ *and the algorithm goes on as before. The expansion becomes eventually periodic with* $b_n = 5$ *for all* $n \in \mathbb{N}$ *and* $[a_0, a_1, \ldots] = [1,3,2,3,\overline{4}]$*.*

## 3.2 Ruban's definition

In 1970, A. A. Ruban [69] defined an algorithm very similar to the standard algorithm in $\mathbb{R}$, using an analogue of the integer part for a $p$–adic number. For any $p$–adic number $\alpha = \sum_{i=-r}^{+\infty} c_i p^i \in \mathbb{Q}_p$, $c_i \in \{0,\ldots,p-1\}$, the floor function used by Ruban is

$$\lfloor \alpha \rfloor_p = \sum_{i=-r}^{0} c_i p^i,$$

and $\lfloor \alpha \rfloor_p = 0$ if $r < 0$. Notice that in this case $\lfloor \alpha \rfloor_p$ is, in general, a rational number. Ruban's continued fractions are simple and the coefficients of the expansion can be computed iteratively by the following algorithm, starting with $\alpha_0 = \alpha$.

$$\begin{cases} a_n = \lfloor \alpha_n \rfloor_p \\ \alpha_{n+1} = \frac{1}{\alpha_n - a_n}. \end{cases} \tag{3.3}$$

If at some point $\alpha_n = a_n$, then the algorithm stops and $\alpha = [a_0, \ldots, a_n]$, i.e. $\alpha$ has finite Ruban's continued fraction.

**Remark 3.2.1.** *The choice of this floor function is, somehow, natural. In fact, in the series* $\sum_{i=-r}^{+\infty} c_i p^i$*, the positive powers of* $p$ *have fractional* $p$*–adic*

*absolute value and the floor function $\lfloor\cdot\rfloor_p$ takes the part that has integral absolute value.*

**Example 3.2.2.** *Let us compute Ruban's expansion of $\alpha_0 = -\frac{2}{5}$ in $\mathbb{Q}_7$. The 7–adic expansion of $\alpha_0$ is*

$$\alpha_0 = 1 + 4\cdot 7 + 5\cdot 7^2 + \ldots,$$

*so that $a_0 = \lfloor\alpha_0\rfloor_p = 1$ and*

$$\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{1}{-\frac{2}{5} - 1} = -\frac{5}{7} = 2\cdot 7^{-1} + 6 + 6\cdot 7 + \ldots.$$

*The second partial quotient is then*

$$a_1 = \lfloor\alpha_1\rfloor_p = \frac{2}{7} + 6 = \frac{44}{7},$$

*and we compute the third complete quotient as*

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{1}{-\frac{5}{7} - \frac{44}{7}} = -\frac{1}{7} = 6\cdot 7^{-1} + 6 + 6\cdot 7 + \ldots.$$

*Then*

$$a_2 = \lfloor\alpha_2\rfloor_p = \frac{48}{7},$$

*and we find*

$$\alpha_3 = \frac{1}{\alpha_2 - a_2} = \frac{1}{-\frac{1}{7} - \frac{48}{7}} = -\frac{1}{7} = \alpha_2.$$

*We have found a repetition on the complete quotients, $\alpha_3 = \alpha_2$, therefore the continued fraction repeats from this point onward. It means that*

$$-\frac{2}{5} = \left[1, \frac{44}{7}, \overline{\frac{48}{7}}\right],$$

*hence $-\frac{2}{5}$ has a periodic Ruban's continued fraction in $\mathbb{Q}_7$.*

## 3.3 Browkin's definitions

In 1978, J. Browkin [15] defined an algorithm that is a slight modification of Ruban's algorithm. The only difference is that, in Browkin's approach, the representatives of $\mathbb{Z}/p\mathbb{Z}$ are chosen in $\{-\frac{p-1}{2},\dots,\frac{p-1}{2}\}$ instead of $\{0,\dots,p-1\}$. This small variation is fundamental because Browkin's algorithm produces a finite continued fraction for each rational number, while Ruban's algorithm can also be periodic over the rationals (more details on the expansion of rational numbers are given in Chapter 5). Given $\alpha=\sum_{i=-r}^{+\infty} c_i p^i \in \mathbb{Q}_p$, with $c_i \in \{-\frac{p-1}{2},\dots,\frac{p-1}{2}\}$, Browkin defines the floor function $s:\mathbb{Q}_p \to \mathbb{Q}$ as

$$s(\alpha)=\sum_{i=-r}^{0} c_i p^i, \tag{3.4}$$

and $s(\alpha)=0$ if $r<0$. Browkin's first algorithm, that we call *Browkin I*, work as follows. At the first step $\alpha_0=\alpha$ and, for all $n\geq 0$,

$$\begin{cases} a_n = s(\alpha_n) \\ \alpha_{n+1}=\frac{1}{\alpha_n - a_n}. \end{cases} \tag{3.5}$$

If at some point $\alpha_n=a_n$, then the algorithm stops and $\alpha=[a_0,\dots,a_n]$, i.e. $\alpha$ has finite *Browkin I* continued fraction.

**Example 3.3.1.** *Let us compute Browkin I continued fraction of $\alpha_0=-\frac{2}{5}$ in $\mathbb{Q}_7$ and let us compare with Ruban's expansion obtained in Example 3.2.2. For Browkin's algorithm, we have to consider the 7–adic expansion with representatives in $\{-3,\dots,3\}$, hence:*

$$\alpha_0 = 1-3\cdot 7-7^2+\dots.$$

*Also in this case the first partial quotient is $a_0=s(\alpha_0)=1$ and then*

$$\alpha_1=\frac{1}{\alpha_0-a_0}=\frac{1}{-\frac{2}{5}-1}=-\frac{5}{7}=2\cdot 7^{-1}-1\dots.$$

*The second partial quotient is then*

$$a_1 = s(\alpha_1) = \frac{2}{7} - 1 = -\frac{5}{7} = \alpha_1.$$

*Therefore,*

$$-\frac{2}{5} = \left[1, -\frac{5}{7}\right],$$

*hence* $-\frac{2}{5}$ *has a finite Browkin I continued fraction. The difference with Ruban's expansion of Example 3.2.2, which is periodic, relies only on the choice of the representatives in* $\{-3, \ldots, 3\}$ *instead of* $\{0, \ldots, 6\}$.

In 2000, more than 20 years after the first algorithm, Browkin [16] defined another floor function, that is similar to the first function $s$, but excluding the zero term. For $\alpha = \sum_{i=-r}^{+\infty} c_i p^i \in \mathbb{Q}_p$, with $c_i \in \{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\}$, the second floor function is the function $t : \mathbb{Q}_p \to \mathbb{Q}$, such that

$$t(\alpha) = \sum_{i=-r}^{-1} c_i p^i,$$

and $t(\alpha) = 0$ if $r \leq 0$. The second algorithm, that we call *Browkin II*, works on an input $\alpha$ as follows. At the first step $\alpha_0 = \alpha$ and, for all $n \geq 0$,

$$\begin{cases} a_n = s(\alpha_n) & \text{if } n \text{ even} \\ a_n = t(\alpha_n) & \text{if } n \text{ odd and } v_p(\alpha_n - t(\alpha_n)) = 0 \\ a_n = t(\alpha_n) - sign(t(\alpha_n)) & \text{if } n \text{ odd and } v_p(\alpha_n - t(\alpha_n)) \neq 0 \\ \alpha_{n+1} = \frac{1}{\alpha_n - a_n}. \end{cases} \tag{3.6}$$

If at some point $\alpha_n = a_n$, then the algorithm stops and $\alpha = [a_0, \ldots, a_n]$, i.e. $\alpha$ has finite *Browkin II* continued fraction. The result of the alternation is that in *Browkin II* all the even partial quotients are integers by construction and all the odd partial quotients are rationals (see Example 3.3.2 below). The use of the *sign* function is due to the convergence condition of Proposition 4.1.4, proved by Browkin in [16].

**Example 3.3.2.** *Let us consider* $\alpha_0 = \frac{22}{7} \in \mathbb{Q}_5$ *and let us compute its Browkin II expansion. The* 5*–adic expansion of* $\alpha_0$ *is*

$$\alpha_0 = 1 - 1 \cdot 5 + 1 \cdot 5^2 + \ldots,$$

*so that* $a_0 = s(\alpha_0) = 1$ *and*

$$\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{1}{\frac{22}{7} - 1} = \frac{7}{15} = -1 \cdot 5^{-1} - 1 + 2 \cdot 5 + \ldots.$$

*Now we apply the function* $t$*, thus obtaining* $b_1 = t(\alpha_1) = -\frac{1}{5}$ *and*

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{3}{2} = -1 - 2 \cdot 5 - 2 \cdot 5^2 + \ldots.$$

*At the next step we have* $a_2 = s(\alpha_2) = -1$ *and* $\alpha_3 = \frac{2}{5}$*. At this point, since* $v_p(\alpha_3 - t(\alpha_3)) > 0$*, then we use the sign function, obtaining:*

$$a_3 = t(\alpha_3) - sign(t(\alpha_3)) = \frac{2}{5} - 1 = -\frac{3}{5}.$$

*Therefore* $\alpha_4 = s(\alpha_4) = b_4 = 1$ *and the expansion is* $\frac{22}{7} = \left[1, -\frac{1}{5}, -1, -\frac{3}{5}, 1\right]$.

## 3.4 Further algorithms and improvements

From several experimental computations, it has been observed that *Browkin II* produces more periodic expansions for quadratic irrationals than *Browkin I*, hence getting closer to a $p$–adic analogue of Lagrange's Theorem (see, Chapter 7). For this reason, *Browkin II* has been taken as a starting point for the definition of some new algorithms with the aim of improving furthermore the properties of periodicity. In [6], it is studied a variant of *Browkin II* in which the representatives are taken in $\{0, \ldots, p-1\}$ instead of $\{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\}$. This choice improves the properties of approximation of *Browkin II* and, unexpectedly, does not compromise the finiteness of the continued fraction expansions of rational numbers. In [57], we proposed a 3-steps generalization of *Browkin II* relying on the convergence condition of Theorem 4.3.2 in Section 4. In order to satisfy that convergence condition, a new integer part is defined,

which acts on elements of $\mathbb{Z}_p$. For $\alpha = \sum_{i=0}^{+\infty} c_i p^i \in \mathbb{Z}_p$, with $c_i \in \{-\frac{p-1}{2}, \dots, \frac{p-1}{2}\}$, the new integer part is

$$u(\alpha) = \begin{cases} +1 & \text{if } c_0 \in \left\{+2, \dots, \frac{p-1}{2}\right\} \cup \{-1\} \\ -1 & \text{if } c_0 \in \left\{-\frac{p-1}{2}, \dots, -2\right\} \cup \{+1\} \\ 0 & \text{if } c_0 = 0. \end{cases} \tag{3.7}$$

In the same paper, we defined two new algorithms by exploiting the three integer parts $s, t, u$ in three different steps. On input $\alpha_0 \in \mathbb{Q}$ the two algorithms work as follows, for all $n \in \mathbb{N}$:

$$\begin{cases} a_n = s(\alpha_n) & \text{if } n \equiv 0 \bmod 3 \\ a_n = t(\alpha_n) & \text{if } n \equiv 1 \bmod 3 \text{ and } v_p(\alpha_n - t(\alpha_n)) = 0 \\ a_n = t(\alpha_n) - sign(t(\alpha_n)) & \text{if } n \equiv 1 \bmod 3 \text{ and } v_p(\alpha_n - t(\alpha_n)) \neq 0 \\ a_n = u(\alpha_n) & \text{if } n \equiv 2 \bmod 3 \\ \alpha_{n+1} = \frac{1}{\alpha_n - a_n}. \end{cases} \tag{3.8}$$

$$\begin{cases} a_n = s(\alpha_n) & \text{if } n \equiv 0 \bmod 3 \\ a_n = t(\alpha_n) & \text{if } n \equiv 1 \bmod 3 \text{ and } v_p(\alpha_n - t(\alpha_n)) = 0 \\ a_n = t(\alpha_n) - sign(t(\alpha_n)) & \text{if } n \equiv 1 \bmod 3 \text{ and } v_p(\alpha_n - t(\alpha_n)) \neq 0 \\ a_n = s(\alpha_n) - u(\alpha_n) & \text{if } n \equiv 2 \bmod 3 \\ \alpha_{n+1} = \frac{1}{\alpha_n - a_n}. \end{cases} \tag{3.9}$$

If at some point $\alpha_n = a_n$, then the algorithm stops and $\alpha = [a_0, \dots, a_n]$, i.e. $\alpha$ has a finite continued fraction. For Algorithm (3.9), we proved (Theorem 5.2.1 in Chapter 5) that all rational numbers have a finite continued fraction, hence becoming more interesting than the other one. Notice that, by construction of Algorithm (3.9) and (3.8), the function $u$ applies only to $p$–adic units, hence it is never zero. Finally, in [55], we proposed a variant of *Browkin II* without

the use of the *sign* function. For all $\alpha_0 \in \mathbb{Q}_p$, the algorithm works as follows:

$$\begin{cases} a_n = s(\alpha_n) & \text{if } n \text{ even} \\ a_n = t(\alpha_n) & \text{if } n \text{ odd} \\ \alpha_{n+1} = \frac{1}{\alpha_n - a_n}. \end{cases} \tag{3.10}$$

If at some point $\alpha_n = a_n$, then the algorithm stops and $\alpha = [a_0, \ldots, a_n]$, i.e. $\alpha$ has a finite continued fraction. This choice turns out to improve the periodicity properties of Browkin's second algorithm both from a theoretical and an experimental point of view. For the theoretical results see Chapter 6, for the experimental simulations see Chapter 7. Our algorithm (3.10) has been recently object of study by Deng and Wang in [26] and by Yasutomi in [79]. They independently defined some algorithms following the same core idea. They introduced two modified floor functions $\tilde{s}$ and $\tilde{t}$ in order to minimize the Euclidean absolute value of $\alpha - \tilde{s}(\alpha)$ and $\alpha - \tilde{t}(\alpha)$, without decreasing its $p$–adic valuation, therefore without compromising the $p$–adic convergence. The two functions are defined as

$$\begin{aligned} \tilde{s}(\alpha) &= s(\alpha) + np, \\ \tilde{t}(\alpha) &= t(\alpha) + m, \end{aligned}$$

where $n, m$ are the integers minimizing, respectively,

$$\begin{aligned} &|\alpha - s(\alpha) - np|, \\ &|\alpha - t(\alpha) + m|. \end{aligned}$$

The important weakness of these functions is that they work only over fields $K$ that can be embedded in both $\mathbb{Q}_p$ and $\mathbb{R}$. In fact, they can not be defined over all $p$–adic numbers, where the Euclidean norm has not an interpretation in general. However, the relevant case for periodic $p$–adic continued fractions is a field $K = \mathbb{Q}[x]/(f(x))$, where $f(x)$ is a polynomial of degree 2 that is irreducible over $\mathbb{Q}$ and that splits both in $\mathbb{R}$ and $\mathbb{Q}_p$. Therefore, given such

field $K$, for all $\alpha_0 \in K$, the algorithms introduced in [26] and [79] work as follows:

$$\begin{cases} a_n = \tilde{s}(\alpha_n) & \text{if } n \text{ even} \\ a_n = \tilde{t}(\alpha_n) & \text{if } n \text{ odd} \\ \alpha_{n+1} = \frac{1}{\alpha_n - a_n}. \end{cases} \tag{3.11}$$

In [26], Deng and Wang also introduced a 3-steps algorithm, exploiting the same convergence conditions introduced in [57] that ensures the convergence of Algorithms (3.8) and (3.9). This algorithm again uses the functions $\tilde{s}$ and $\tilde{t}$, therefore it works only for fields $K$ having an embedding both into $\mathbb{Q}_p$ and into $\mathbb{R}$. For all $\alpha_0 \in K$, it works as follows:

$$\begin{cases} a_n = \tilde{s}(\alpha_n) & \text{if } n \equiv 0 \bmod 3 \\ a_n = \tilde{t}(\alpha_n) & \text{if } n \equiv 1 \bmod 3 \\ a_n = \tilde{t}(\alpha_n) & \text{if } n \equiv 2 \bmod 3 \\ \alpha_{n+1} = \frac{1}{\alpha_n - a_n}. \end{cases} \tag{3.12}$$

In this case, because of the presence of two consecutive uses of the function $\tilde{t}$, some of the partial quotients can be zero, and they overcome this problem by using the formula

$$[\ldots, a_{n-1}, a_n, 0, a_{n+1}, a_{n+2}, \ldots] = [\ldots, a_{n-1}, a_n + a_{n+1}, a_{n+2}, \ldots].$$

In the latter, all partial quotients are non-zero, since there can not be two consecutive null partial quotients.

However, although all these algorithms improve on several different aspects the known methods to generate $p$–adic continued fractions, they experimentally seem still far from an analogue of Lagrange's Theorem and, in general, from a satisfactory algorithm reproducing the same properties of classical continued fractions in $\mathbb{R}$.

Very recently, in [21], the definition of $p$–adic continued fractions has been generalized also to number fields, addressing some questions similar to Rosen [67, 68] in the archimedean setting. The authors gave a general definition of $\mathfrak{P}$–adic continued fractions for a prime ideal $\mathfrak{P}$ of the ring of integers $\mathcal{O}_K$ of a number field $K$. Moreover, they investigated their finiteness and periodicity properties, focusing on a general number field $K$ and obtaining some more effective results for the quadratic case. In [19], the construction of [21] has been generalized to quaternion algebras over $\mathbb{Q}$ ramified at $p$, hence including all the classical $p$–adic framework.

# Chapter 4

# Convergence of continued fractions in $\mathbb{Q}_p$

In this section we study the convergence of $p$–adic continued fractions. An infinite continued fraction $[a_0, a_1, \ldots]$ converges to an element $\alpha$ if the sequence of its convergents does, i.e. if

$$\lim_{n \to +\infty} \frac{A_n}{B_n} = \alpha. \tag{4.1}$$

In the field of real numbers, every continued fraction with positive integral partial quotients converges to an $\alpha \in \mathbb{R}$, but we are going to see that this is not always the case in $\mathbb{Q}_p$. In particular, for general real partial quotients (not necessarily integers), the following more precise result holds.

**Theorem 4.0.1** ([75]). *Let $\{a_n\}_{n \in \mathbb{R}}$ be a sequence of real numbers. Then, the continued fraction $[a_0, a_1, \ldots]$ converges if and only if $\sum_{n=0}^{+\infty} a_n = +\infty$, and this happens if and only if the sequence $B_n$ of partial denominators is unbounded.*

In the field of $p$–adic numbers, we require (4.1) to hold in the $p$–adic topology, hence with respect to the $p$–adic norm. In Section 2.2, we have seen that the field of $p$–adic numbers is complete with respect to the $p$–adic absolute value $|\cdot|_p$. Therefore, a sequence is convergent in $\mathbb{Q}_p$ if and only if it

is a Cauchy sequence. Then, a continued fraction

$$a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \ddots}},$$

converges to a $p$–adic number if and only if the sequence of the convergents $\{\frac{A_n}{B_n}\}_{n\in\mathbb{N}}$ is a Cauchy sequence with respect to $|\cdot|_p$. By Proposition 2.2.9, for a non-archimedean absolute value this is equivalent to require that

$$\lim_{n\to+\infty} \left|\frac{A_{n+1}}{B_{n+1}} - \frac{A_n}{B_n}\right|_p = 0.$$

The latter quantity can be written as

$$\left|\frac{A_{n+1}}{B_{n+1}} - \frac{A_n}{B_n}\right|_p = \left|\frac{(-1)^n}{B_n B_{n+1}}\right|_p = p^{v_p(B_n B_{n+1})}, \tag{4.2}$$

so that the continued fraction $[a_0, a_1, \ldots]$ converges to an element of $\mathbb{Q}_p$ if and only if

$$\lim_{n\to+\infty} v_p(B_n B_{n+1}) = -\infty.$$

In this chapter, we delve into the understanding of when the latter happens. This is, in fact, the minimum requirement in order to define meaningful continued fractions in the field of $p$–adic numbers, since, otherwise, a continued fraction would not represent any element of $\mathbb{Q}_p$.

## 4.1 Convergence of the main algorithms

In this section, we focus on simple continued fractions and we see why the main algorithms defined in Chapter 3 always represent $p$–adic numbers.

**Remark 4.1.1.** *In [15], Browkin proved that, for Browkin I,*

$$\begin{aligned} v_p(A_n) &= v_p(a_0) + v_p(a_1) + \ldots + v_p(a_n), \\ v_p(B_n) &= v_p(a_1) + v_p(a_2) + \ldots + v_p(a_n), \end{aligned} \tag{4.3}$$

*or, equivalently,*

$$\begin{aligned} |A_n|_p &= |a_0|_p |a_1|_p \dots |a_n|_p, \\ |B_n|_p &= |a_1|_p |a_2|_p \dots |a_n|_p. \end{aligned} \tag{4.4}$$

*The proof is done by induction on $n$. Using a similar argument, it is not hard to see that a sufficient condition for these equations to hold is having $v_p(a_{n+1}B_n) < v_p(B_{n-1})$ for all $n \in \mathbb{N}$.*

The $p$–adic convergence strictly depends on the $p$–adic valuation of the partial quotients, regardless of the representatives of $\mathbb{Z}/p\mathbb{Z}$ that are used. Therefore, the next proposition proves the convergence for both Ruban's and Browkin's continued fractions.

**Proposition 4.1.2** ([15])**.** *Let an infinite sequence $a_0, a_1, \dots \in \mathbb{Z}[\frac{1}{p}]$ such that for all $n \in \mathbb{N}$, $v_p(a_n) < 0$. Then the continued fraction $[a_0, a_1, \dots]$ is convergent to a $p$–adic number.*

*Proof.* We want to prove that, for all $n \in \mathbb{N}$, $v_p(B_{n+1}) < v_p(B_n)$, so that the sequence $v_p(B_n)$, for $n \to +\infty$, decreases to $-\infty$. We prove it by induction on $n$. For $n = 0$ and $n = 1$,

$$\begin{aligned} v_p(B_1) &= v_p(a_1) < 0 = v_p(1) = v_p(B_0), \\ v_p(B_2) &= v_p(a_2a_1 + 1) = v_p(a_2a_1) = v_p(a_2) + v_p(a_1) < v_p(a_1). \end{aligned}$$

Then, let us suppose by inductive hypothesis that $v_p(B_n) < v_p(B_{n-1})$. This means that the valuation of $B_{n+1}$ is

$$v_p(B_{n+1}) = v_p(a_{n+1}B_n + B_{n-1}) = v_p(a_{n+1}B_n) = v_p(a_{n+1}) + v_p(B_n) < v_p(B_n),$$

and this proves the inductive step. Hence, the continued fraction $[a_0, a_1, \dots]$ converges in $\mathbb{Q}_p$. □

**Remark 4.1.3.** *Proposition 4.1.2 and all the convergence results in this section contain conditions that hold for all $n$. However, the results do not change if these conditions hold for all $n \geq n_0 \in \mathbb{N}$.*

In his second paper [16], Browkin noticed that the condition of Proposition 4.1.2 can be lightened by allowing partial quotients to have null valuation at half steps. In fact, the convergence of *Browkin II* relies on the following proposition.

**Proposition 4.1.4** ([16])**.** *Let an infinite sequence $a_0, a_1, \ldots \in \mathbb{Z}[\frac{1}{p}]$ such that for all $n \in \mathbb{N}$:*

$$\begin{cases} v_p(a_{2n}) = 0 \\ v_p(a_{2n+1}) < 0. \end{cases} \tag{4.5}$$

*Then the continued fraction $[a_0, a_1, \ldots]$ is convergent to a $p$–adic number.*

*Proof.* Let us prove, by induction, that $B_n \neq 0$ and $v_p(B_n) \leq v_p(B_{n-1})$, for all $n \geq 0$, and that the equality holds if and only if $n$ is even. The base of the induction is true since $B_0 = 1$ and $B_1 = a_1$, so that

$$v_p(B_0) = 0 > v_p(a_1) = v_p(B_1),$$

and $B_1 \neq 0$. Now, let us suppose that

$$B_{n-1} \neq 0, \quad v_p(B_{n-1}) \leq v_p(B_{n-2}), \text{ for } n \geq 2,$$

and that the equality holds for $n$ odd. Then, for $n$ even,

$$v_p(a_n B_{n-1}) = v_p(a_n) + v_p(B_{n-1}) = v_p(B_{n-1}) < v_p(B_{n-2}),$$

and, for $n$ odd,

$$v_p(a_n B_{n-1}) = v_p(a_n) + v_p(B_{n-1}) < v_p(B_{n-1}) = v_p(B_{n-2}).$$

In both cases, $v_p(a_n B_{n-1}) < v_p(B_{n-2})$ and this implies that

$$v_p(B_n) = v_p(a_n B_{n-1} + B_{n-2}) = v_p(a_n B_{n-1}) < v_p(B_{n-2}).$$

We have obtained, by induction, that $v_p(B_n) < 0$, so $B_n \neq 0$, and that $v_p(B_{n+2}) < v_p(B_n)$ for all $n \in \mathbb{N}$. It follows that the sequence $v_p(B_n B_{n+1})$

is strictly decreasing and the continued fraction $[a_0, a_1, \ldots]$ converges with respect to the $p$–adic absolute value. □

## 4.2 Sufficient conditions for convergence

In this section, we present our contribution to the convergence of $p$–adic continued fractions. Let us recall that a continued fraction is convergent in $\mathbb{Q}_p$ if and only if

$$\lim_{n \to +\infty} v_p(B_n B_{n+1}) = -\infty.$$

In both Browkin's proofs of Proposition 4.1.2 and Proposition 4.1.4, the sequence $\{v_p(B_n B_{n+1})\}_{n \in \mathbb{N}}$ diverges to $-\infty$ because it is a strictly decreasing sequence of integers. In [57], we effectively characterized the strict decrease of this sequence in terms of the partial quotients, hence giving a practical method to define $p$–adically convergent algorithms. In particular, the main result is the following, that generalizes Proposition 4.1.2 and Proposition 4.1.4 and allows to define several new algorithms.

**Theorem 4.2.1** ([57]). *Let $a_0, a_1, \ldots \in \mathbb{Z}\left[\frac{1}{p}\right]$. Then, the sequence of valuations of partial denominators $\{v_p(B_n B_{n+1})\}_{n \in \mathbb{N}}$ is strictly decreasing if and only if $v_p(a_n a_{n+1}) < 0$ for all $n \in \mathbb{N}$.*
*In particular, the latter is a sufficient condition for the convergence of the continued fraction $[a_0, a_1, \ldots]$ to a $p$–adic number.*

The rest of this section is devoted to provide a proof of this result.
Let us notice that requiring the sequence $\{v_p(B_n B_{n+1})\}_{n \in \mathbb{N}}$ strictly decreasing is equivalent to ask that $v_p(B_{n+1}) < v_p(B_{n-1})$ for all $n \geq 1$. In fact, for all $n \in \mathbb{N}$,

$$v_p(B_{n-1}) + v_p(B_n) = v_p(B_{n-1} B_n) > v_p(B_n B_{n+1}) = v_p(B_n) + v_p(B_{n+1}),$$

happens if and only if $v_p(B_{n+1}) < v_p(B_{n-1})$. In the following lemmas, we characterize this condition in terms of the valuations of the partial quotients.

**Lemma 4.2.2.** *For all $n \geq 1$, if $v_p(B_{n+1}) < v_p(B_{n-1})$, then*

$$v_p(B_{n+1}) \leq v_p(B_n).$$

*Proof.* If $v_p(a_{n+1}B_n) < v_p(B_{n-1})$, then

$$v_p(B_{n+1}) = v_p(a_{n+1}B_n) = v_p(a_{n+1}) + v_p(B_n) \leq v_p(B_n),$$

since $v_p(a_{n+1}) \leq 0$. Instead, if $v_p(a_{n+1}B_n) \geq v_p(B_{n-1})$,

$$v_p(B_{n+1}) \geq \min\{v_p(a_{n+1}B_n), v_p(B_{n-1})\} = v_p(B_{n-1}),$$

but it is a contradiction with the hypothesis of $v_p(B_{n+1}) < v_p(B_{n-1})$, hence this second case can not occur. □

For sake of completeness, we include the next lemma, which is basically the technique that has already been used in [15] and [16].

**Lemma 4.2.3.** *For all $n \geq 1$, $v_p(B_{n+1}) < v_p(B_{n-1})$ if and only if*

$$v_p(a_{n+1}B_n) < v_p(B_{n-1}).$$

*Proof.* If $v_p(B_{n+1}) < v_p(B_{n-1})$ and $v_p(a_{n+1}B_n) \geq v_p(B_{n-1})$, then

$$v_p(B_{n+1}) \geq \min\{v_p(a_{n+1}B_n), v_p(B_{n-1})\} = v_p(B_{n-1}),$$

but this contradicts the hypothesis. Conversely, if $v_p(a_{n+1}B_n) < v_p(B_{n-1})$, then

$$v_p(B_{n+1}) = v_p(a_{n+1}B_n) < v_p(B_{n-1}),$$

and the claim is proved. □

Using the results of Lemma 4.2.2 and Lemma 4.2.3, we prove the characterization of the strict decrease of the sequence $\{v_p(B_nB_{n+1})\}_{n\in\mathbb{N}}$.

**Theorem 4.2.4.** *The following conditions are equivalent:*

*i)* $v_p(a_{n+1}B_n) < v_p(B_{n-1})$, *for all* $n \geq 1$,

*ii)* $v_p(a_na_{n+1}) < 0$, *for all* $n \geq 1$.

*Proof.* *i)* $\Rightarrow$ *ii)*
Let us suppose that $v_p(a_{n+1}B_n) < v_p(B_{n-1})$ for all $n \geq 1$.

If $v_p(a_{n+1}) < 0$, then $v_p(a_{n+1}a_n) = v_p(a_{n+1}) + v_p(a_n) < 0$ and the claim is proved. Therefore, let us assume $v_p(a_{n+1}) = 0$ and we prove that $v_p(a_n) < 0$. Since $v_p(a_{n+1}) = 0$ and

$$v_p(a_{n+1}B_n) < v_p(B_{n-1}),$$

then $v_p(B_n) < v_p(B_{n-1})$. The latter means that:

$$v_p(B_n) = v_p(a_nB_{n-1} + B_{n-2}) < v_p(B_{n-1}).$$

Moreover, $v_p(B_n) = v_p(a_nB_{n-1})$ because otherwise $v_p(B_n) \geq v_p(B_{n-2})$ and this would lead to a contradiction, by Lemma 4.2.3. Hence, we have obtained that

$$v_p(B_n) = v_p(a_nB_{n-1}) = v_p(a_n) + v_p(B_{n-1}) < v_p(B_{n-1}),$$

and the last inequality implies $v_p(a_n) < 0$ and this concludes the proof.
$ii) \Rightarrow i)$
Conversely, let us suppose that $v_p(a_na_{n+1}) < 0$ for all $n \geq 1$. We prove the claim by induction on $n$.
**Base step:**
By hypothesis, we have that $v_p(a_1a_2) < 0$ and $v_p(a_2a_3) < 0$. Hence, for $n = 1$ and $n = 2$, we have that:

$$\begin{aligned} &v_p(a_2B_1) = v_p(a_2a_1) < 0 = v(1) = v(B_0), \\ &v_p(a_3B_2) = v_p(a_3a_2a_1 + a_3) = v_p(a_3a_2a_1) = v_p(a_3a_2) + v_p(a_1) < \\ &\qquad < v_p(a_1) = v_p(B_1). \end{aligned}$$

**Induction step:**
Let us suppose that the thesis is true until a step $n \geq 2$ and we show it for $n+1$. From $v_p(a_{n+2}a_{n+1}) < 0$ we get that either $v_p(a_{n+2}) < 0$ or $v_p(a_{n+1}) < 0$ (or both).
**Case $v_p(a_{n+2}) < 0$:**
In this case, using the inductive hypothesis and Lemma 4.2.2 we get that

$v_p(B_{n+1}) \leq v_p(B_n)$, hence:

$$v_p(a_{n+2}B_{n+1}) = v_p(a_{n+2}) + v_p(B_{n+1}) < v_p(B_{n+1}) \leq v_p(B_n).$$

**Case $v_p(a_{n+1}) < 0$:**
In this case we have

$$a_{n+2}B_{n+1} = a_{n+2}\left(a_{n+1}B_n + B_{n-1}\right),$$

therefore

$$v_p\left(a_{n+2}B_{n+1}\right) \leq v_p\left(a_{n+1}B_n + B_{n-1}\right).$$

The inductive hypothesis ensures that $v_p\left(a_{n+1}B_n\right) < v_p(B_{n-1})$, so

$$v_p\left(a_{n+2}B_{n+1}\right) \leq v_p\left(a_{n+1}B_n\right) < v_p(B_n),$$

and this concludes the proof. □

Therefore, we easily obtain the following corollary, fully characterizing the strict decrease of the sequence of denominators.

**Corollary 4.2.5.** *The sequence $\{v_p(B_nB_{n+1})\}_{n\in\mathbb{N}}$ is strictly decreasing if and only if $v_p(a_na_{n+1}) < 0$ for all $n \in \mathbb{N}$.*

This corollary, in particular, concludes the proof of Theorem 4.2.1 since the strict decreasing of $\{v_p(B_nB_{n+1})\}_{n\in\mathbb{N}}$ implies the convergence of the correspondent continued fraction.

## 4.3 Other convergence conditions

In Theorem 4.2.1, we have characterized the strict decrease of the sequence $\{v_p(B_nB_{n+1})\}_{n\in\mathbb{N}}$, which provides a sufficient condition for the $p$–adic convergence of a continued fraction. However, in general, an integer sequence that diverges to $-\infty$ is not necessarily strictly decreasing. Thus, in this section we examine the convergence of continued fractions for which the condition of Theorem 4.2.1 is not fulfilled, therefore admitting also consecutive partial

quotients with null $p$–adic valuation. The first attempt we make is to generalize the "2 steps" construction of *Browkin II*'s Proposition 4.1.4 into 3 or more steps. For example, it is reasonable to wonder if it is possible to define an algorithm that produces the partial quotients such that, for all $n \in \mathbb{N}$,

$$\begin{cases} v_p(a_{3n+1}) < 0 \\ v_p(a_{3n+2}) = 0 \\ v_p(a_{3n+3}) = 0. \end{cases} \tag{4.6}$$

It is not hard to see that this construction does not satisfy the hypothesis of Theorem 4.2.1, since $v_p(a_{3n+2}a_{3n+3}) = 0$. In the following constructive example we see that, for a sequence of partial quotients defined as in (4.6), the convergence is not guaranteed in general. Therefore, an analogue of Proposition 4.1.2 and Proposition 4.1.4 fails. In particular, without a stronger hypothesis, we may construct, for every prime $p$, a suitable continued fraction that does not converge to any $p$–adic number.

**Example 4.3.1.** *Let $p$ be an odd prime. We want to show that there exists a sequence $a_0, a_1, \ldots \in \mathbb{Q}_p$ with, for all $n \in \mathbb{N}$,*

$$\begin{cases} v_p(a_{3n+1}) < 0 \\ v_p(a_{3n+2}) = 0 \\ v_p(a_{3n+3}) = 0, \end{cases}$$

*such that the sequence $v_p(B_nB_{n+1})$ does not diverge to $-\infty$. Let us define $a_1 = \frac{1}{p}$. The first denominators of the convergents are*

$$\begin{aligned} B_0 &= 1, \\ B_1 &= a_1 = \frac{1}{p}, \\ B_2 &= a_2B_1 + B_0 = \frac{a_2 + p}{p}, \\ B_3 &= a_3B_2 + B_1 = \frac{(a_3a_2 + 1) + a_3p}{p}. \end{aligned}$$

*Their valuations are*

$$\begin{aligned} v_p(B_0) &= v_p(1) = 0, \\ v_p(B_1) &= v_p\left(\frac{1}{p}\right) = -1, \\ v_p(B_2) &= v_p\left(\frac{a_2 + p}{p}\right) = -1, \\ v_p(B_3) &= v_p\left(\frac{(a_3 a_2 + 1) + a_3 p}{p}\right). \end{aligned}$$

*Let us choose suitable $a_2$ and $a_3$ such that $a_3 a_2 + 1 = p$ (for example, $a_2 = 2$ and $a_3 = \frac{p-1}{2}$). Then*

$$v_p(B_3) = v_p\left(\frac{a_3 p + p}{p}\right) = v_p(a_3 + 1) \geq 0.$$

*At this point, for a generic $n \in \mathbb{N}$ for which*

$$v_p(B_{3n+1}) = -1,\ v_p(B_{3n+2}) = -1,\ v_p(B_{3n+3}) \geq 0,$$

*we are going to show that there exists a choice for the partial quotients such that*

$$v_p(B_{3(n+1)+1}) = -1,\ v_p(B_{3(n+1)+2}) = -1,\ v_p(B_{3(n+1)+3}) \geq 0.$$

*We can write*

$$\begin{aligned} B_{3n+1} &= \frac{c_1}{p}, && \text{with } v_p(c_1) = 0, \\ B_{3n+2} &= \frac{c_2}{p}, && \text{with } v_p(c_2) = 0, \\ B_{3n+3} &= c_3, && \text{with } v_p(c_3) \geq 0. \end{aligned}$$

*We have two cases:*

- *In the case that $v_p(c_3 + c_2) = 0$, we choose $a_{3n+4} = \frac{1}{p}$. Therefore,*

$$B_{3n+4} = a_{3n+4} B_{3n+3} + B_{3n+2} = \frac{c_3 + c_2}{p}.$$

*Its valuation is*

$$v_p(B_{3n+4}) = v_p(c_3 + c_2) - v_p(p) = -1,$$

*so that we can write* $B_{3n+4} = \frac{c_4}{p}$, *with* $v_p(c_4) = 0$. *Subsequently,*

$$B_{3n+5} = a_{3n+5}B_{3n+4} + B_{3n+3} = a_{3n+5}\frac{c_4}{p} + c_3 = \frac{a_{3n+5}c_4 + c_3 p}{p},$$

*so that* $v_p(B_{3n+5}) = -1$. *It means that* $B_{3n+5} = \frac{c_5}{p}$, *with* $v_p(c_5) = 0$. *At the following step,*

$$B_{3n+6} = a_{3n+6}B_{3n+5} + B_{3n+4} = \frac{a_{3n+6}c_5 + c_4}{p}.$$

*Notice that* $c_4$ *and* $c_5$ *are arbitrary nonzero elements and we can choose a suitable* $a_{3n+6}$ *such that*

$$a_{3n+6}c_5 + c_4 \equiv 0 \bmod p.$$

*We obtain that* $p$ *divides* $a_{3n+6}c_5 + c_4$ *and so* $v_p(B_{3n+6}) \geq 0$. *In this case we have obtained that, starting from*

$$v_p(B_{3n+1}) = -1,\ v_p(B_{3n+2}) = -1,\ v_p(B_{3n+3}) \geq 0,$$

*then*

$$v_p(B_{3(n+1)+1}) = -1,\ v_p(B_{3(n+1)+2}) = -1,\ v_p(B_{3(n+1)+3}) \geq 0.$$

- *Let us examine also the case* $v_p(c_3 + c_2) > 0$. *Here we choose* $a_{3n+4} = \frac{2}{p}$. *Since* $v_p(c_2) = 0$ *and* $v_p(c_3 + c_2) > 0$, *necessarily also* $v_p(c_3) = 0$. *The next denominator is*

$$B_{3n+4} = a_{3n+4}B_{3n+3} + B_{3n+2} = \frac{2c_3 + c_2}{p}.$$

*Notice that since $p$ divides $c_3 + c_2$ but does not divide $c_3$, it can not divide $2c_3 + c_2$. In this way $v_p(2c_3 + c_2) = 0$ and*

$$v_p(B_{3n+4}) = v_p(2c_3 + c_2) - v_p(p) = -1.$$

*Then we get*

$$v_p(B_{3n+5}) = v_p(a_{3n+5}B_{3n+4} + B_{3n+3}) = -1,$$

*and so we can write*

$$\begin{aligned} B_{3n+4} &= \frac{c_4}{p}, && \text{with } v_p(a_4) = 0, \\ B_{3n+5} &= \frac{c_5}{p}, && \text{with } v_p(a_5) = 0. \end{aligned}$$

*At the next step we have*

$$B_{3n+6} = a_{3n+6}B_{3n+5} + B_{3n+4} = \frac{a_{3n+6}c_5 + c_4}{p}.$$

*As before, we choose $a_{3n+6}$ such*

$$a_{3n+6}c_5 + c_4 \equiv 0 \bmod p.$$

*In this way we get $v_p(B_{3n+6}) \geq 0$. Hence, also in this second case we have obtained that*

$$v_p(B_{3(n+1)+1}) = -1,\ v_p(B_{3(n+1)+2}) = -1,\ v_p(B_{3(n+1)+3}) \geq 0.$$

*We have just constructed a sequence of denominators $B_n$ such that the sequence of valuations $v_p(B_nB_{n+1}) = v_p(B_n) + v_p(B_{n+1})$ can not diverge to $-\infty$. In fact, in particular, $v_p(B_n) \geq -1$ for all $n \in \mathbb{N}$ and the $p$–adic continued fraction is not convergent.*

In the last example we showed that an algorithm generating the partial quotients as in (4.6) does not ensure the $p$–adic convergence of the correspondent continued fraction. However, with the addition of one constraint to the two partial quotients having null valuation, it is possible to avoid the growth

of the valuation of the denominators. In this way we succeed to obtain the convergence of a $p$–adic continued fraction with only one partial quotient with negative valuation each three steps, as defined in (4.6).

**Theorem 4.3.2.** *Let $a_0, a_1, \ldots \in \mathbb{Q}_p$ such that, for all $n \in \mathbb{N}$:*

$$\begin{cases} v_p(a_{3n+1}) < 0 \\ v_p(a_{3n+2}) = 0 \\ v_p(a_{3n+3}) = 0. \end{cases}$$

*If $v_p(a_{3n+3}a_{3n+2}+1) = 0$ for all $n \in \mathbb{N}$, then,*

$$v_p(B_{3n-2}) = v_p(B_{3n-1}) = v_p(B_{3n}) > v_p(B_{3n+1}).$$

*Proof.* Let us prove the claim by induction on $n$.
**Base step**:

$$\begin{aligned} &v_p(B_0) = v_p(1) = 0, \\ &v_p(B_1) = a_1 < 0, \\ &v_p(B_2) = v_p(a_2a_1+1) = v_p(a_2) + v_p(a_1) = v_p(a_1) = v_p(B_1), \\ &v_p(B_3) = v_p(a_3B_2 + B_1) = v_p((a_3a_2+1)B_1 + a_3B_0) \\ &\qquad = v_p((a_3a_2+1)B_1) = v_p(B_1) = v_p(B_2), \\ &v_p(B_4) = v_p(a_4B_3 + B_2) = v_p(a_4) + v_p(B_3) < v_p(B_3) = \\ &\qquad = v_p(B_1) = v_p(B_2), \end{aligned}$$

where we employed the fact that $v_p(a_4) < 0$ and $v_p(a_3a_2+1) = 0$.
**Induction step:**
Let us suppose that:

$$v_p(B_{3n-2}) = v_p(B_{3n-1}) = v_p(B_{3n}) > v_p(B_{3n+1}).$$

In fact, the valuation of $B_{3n+1}$ is:

$$v_p(B_{3n+1}) = v_p(a_{3n+1}B_{3n} + B_{3n-1}) = v_p(a_{3n+1}) + v_p(B_{3n}) < v_p(B_{3n}),$$

since, by induction hypothesis, $v_p(B_{3n}) = v_p(B_{3n-1})$ and $v_p(a_{3n+1}) < 0$. Recalling that $v_p(a_{3n+4}) < 0$ and $v_p(a_{3n+3}a_{3n+2}+1) = 0$, at the following steps we obtain:

$$\begin{aligned}
v_p(B_{3n+2}) &= v_p(a_{3n+2}B_{3n+1} + B_{3n}) = v_p(a_{3n+2}) + v_p(B_{3n+1}) = \\
&= v_p(B_{3n+1}) < v_p(B_{3n}), \\
v_p(B_{3n+3}) &= v_p(a_{3n+3}B_{3n+2} + B_{3n+1}) = \\
&= v_p((a_{3n+3}a_{3n+2}+1)B_{3n+1} + a_{3n+3}B_{3n}) = \\
&= v_p((a_{3n+3}a_{3n+2}+1)B_{3n+1}) = v_p(B_{3n+1}) = \\
&= v_p(B_{3n+2}) < v_p(B_{3n}), \\
v_p(B_{3n+4}) &= v_p(a_{3n+4}B_{3n+3} + B_{3n+2}) = v_p(a_{3n+4}) + v_p(B_{3n+3}) < \\
&< v_p(B_{3n+3}) = v_p(B_{3n+1}) = v_p(B_{3n+2}).
\end{aligned}$$

Hence, we have obtained that

$$v_p(B_{3n+4}) < v_p(B_{3n+3}) = v_p(B_{3n+2}) = v_p(B_{3n+1}) < v_p(B_{3n}),$$

and this proves the claim. □

Theorem 4.3.2 easily leads to the following corollary, achieving the convergence of a $p$–adic continued fraction generating the partial quotients as in (4.6).

**Corollary 4.3.3.** *Let $a_0, a_1, \ldots$ as in Theorem 4.3.2. Then the continued fraction $[a_0, a_1, \ldots]$ is convergent to a $p$–adic number.*

*Proof.* We have seen that the continued fraction $[a_0, a_1, \ldots]$ converges to a $p$–adic number if and only if

$$\lim_{n \to +\infty} v_p(B_n B_{n+1}) = -\infty.$$

Notice that, for all $n \in \mathbb{N}$,

$$v_p(B_{3n}B_{3n+1}) > v_p(B_{3n+1}B_{3n+2}),$$

since $v_p(B_{3n+1}) < v_p(B_{3n})$ and $v_p(B_{3n+1}) = v_p(B_{3n+2})$. Then

$$v_p(B_{3n+1}B_{3n+2}) = v_p(B_{3n+2}B_{3n+3}),$$

since all the three valuations are equal. Moreover,

$$v_p(B_{3n+2}B_{3n+3}) > v_p(B_{3n+3}B_{3n+4}),$$

since $v_p(B_{3n+4}) < v_p(B_{3n+3})$ and $v_p(B_{3n+3}) = v_p(B_{3n+2})$. So, the sequence $v_p(B_nB_{n+1})$ is decreasing and divergent. □

In the next Section 4.4, we define an algorithm satisfying all the hypotheses of Theorem 4.3.2, hence obtaining the convergence of a $p$–adic continued fraction where the valuation of the partial quotients satisfy (4.6). It is natural to wonder whether this approach can be extended to $n$ steps, i.e. by obtaining the convergence of a continued fraction with 1 partial quotient with negative valuation each $n$ steps, and with all the others having zero valuation. Also in this case the answer is positive, but it is necessary to add more constraints. On this purpose, we introduce the following notation for a family of sequences.

Let $n, m \in \mathbb{N}$, with $m \geq 2$. Starting from an infinite sequence of partial quotients $\{a_n\}_{n\in\mathbb{N}}$, we define recursively the family of sequences $U_m^{(n)}$ as

$$U_m^{(0)} = 1, \quad U_m^{(1)} = a_m, \quad U_m^{(n+1)} = a_{m+n}U_m^{(n)} + U_m^{(n-1)}. \tag{4.7}$$

**Lemma 4.3.4.** *For every $n \geq 2$, the partial denominators $B_n$ of the continued fraction $[a_0, a_1, \ldots]$ can be obtained as:*

$$B_n = U_2^{(n-1)}B_1 + U_3^{(n-2)}B_0,$$

*where the sequences $U_m^{(n)}$ are defined as in (4.7).*

*Proof.* Let us prove the claim by induction on $n$. For $n=2$ and $n=3$ the base step is true since

$$B_2 = a_2 B_1 + B_0 = U_2^{(1)} B_1 + U_3^{(0)} B_0,$$
$$B_3 = a_3 B_2 + B_1 = (a_3 a_2 + 1) B_1 + a_3 B_0 = U_2^{(2)} B_1 + U_3^{(1)} B_0.$$

Now, let us suppose that the claim holds at the steps $n$ and $n+1$, that is:

$$B_n = U_2^{(n-1)} B_1 + U_3^{(n-2)} B_0,$$
$$B_{n+1} = U_2^{(n)} B_1 + U_3^{(n-1)} B_0.$$

We are going to show that it is true also for $B_{n+2}$. In fact:

$$\begin{aligned} B_{n+2} &= a_{n+2} B_{n+1} + B_n = \\ &= a_{n+2}(U_2^{(n)} B_1 + U_3^{(n-1)} B_0) + (U_2^{(n-1)} B_1 + U_3^{(n-2)} B_0) = \\ &= (a_{n+2} U_2^{(n)} + U_2^{(n-1)}) B_1 + (a_{n+2} U_3^{(n-1)} + U_3^{(n-2)}) B_0 = \\ &= U_2^{(n+1)} B_1 + U_3^{(n)} B_0. \end{aligned}$$

It follows that the thesis is true for all $n \geq 2$. □

**Remark 4.3.5.** *Notice that Lemma 4.3.4 holds also starting from a generic step $k$. It means that, for all $k \in \mathbb{N}$ and $n \geq 2$,*

$$B_{k+n} = U_{k+2}^{(n-1)} B_{k+1} + U_{k+3}^{(n-2)} B_k,$$

*and the proof is similar to the case $k=0$ seen in Lemma 4.3.4.*

**Theorem 4.3.6.** *Let us consider $r \in \mathbb{N}^+$ and $a_0, a_1, \ldots \in \mathbb{Q}_p$ such that, for all $n \in \mathbb{N}$:*

$$\begin{cases} v_p(a_{rn+1}) < 0 \\ v_p(a_{rn+i}) = 0, \ \forall i \in \{2, \ldots, r\}. \end{cases}.$$

*Moreover let us suppose that, for all* $n \in \mathbb{N}$,

$$v_p(U^{(i)}_{rn+2}) = 0 \text{ for all } i \in \{2, \dots, r-1\} \text{ and for } r \geq 3,$$
$$v_p(U^{(i)}_{rn+3}) = 0 \text{ for all } i \in \{2, \dots, r-2\} \text{ and for } r \geq 4,$$

*where the sequences* $U^{(n)}_m$ *are defined as in* (4.7). *Then we have, for all* $n \in \mathbb{N}$,

$$v_p(B_{rn+1}) = v_p(B_{rn+2}) = \dots = v_p(B_{rn+r}) > v_p(B_{rn+r+1}).$$

*Proof.* Let us prove the claim by induction on $n$.
**Base step:**
We prove the thesis for $n = 0$. The valuation of the first denominator is:

$$v_p(B_1) = v_p(a_1) < 0.$$

By Lemma 4.3.4, for $i \in \{2, \dots, r\}$,

$$v_p(B_i) = v_p(U_2^{(i-1)} B_1 + U_3^{(i-2)} B_0) = v_p(U_2^{(i-1)} B_1) = v_p(a_2 B_1) = v_p(B_1).$$

At the following step, since $v_p(a_{r+1}) < 0$, we get:

$$v_p(B_{r+1}) = v_p(a_{r+1} B_r + B_{r-1}) = v_p(a_{r+1}) + v_p(B_r) < v_p(B_r).$$

Hence, the claim is true for $n = 0$.
**Induction step:**
Let us suppose that the thesis holds for a generic $n \in \mathbb{N}$, that is:

$$v_p(B_{rn+1}) = v_p(B_{rn+2}) = \dots = v_p(B_{rn+r}) > v_p(B_{rn+r+1}).$$

We want to prove the claim for $n+1$. Here we use Remark 4.3.5 with $k = r(n+1)$. Now, for $i \in \{2, \dots, r\}$,

$$\begin{aligned} v_p(B_{r(n+1)+i}) &= v_p(U^{(i-1)}_{r(n+1)+2} B_{r(n+1)+1} + U^{(i-2)}_{r(n+1)+3} B_{r(n+1)}) = \\ &= v_p(U^{(i-1)}_{r(n+1)+2} B_{r(n+1)+1}) = \\ &= v_p(U^{(i-1)}_{r(n+1)+2}) + v_p(B_{r(n+1)+1}) = v_p(B_{r(n+1)+1}). \end{aligned}$$

At the following step, since $v_p(a_{r(n+2)+1}) < 0$, then:

$$\begin{aligned} v_p(B_{r(n+2)+1}) &= v_p(a_{r(n+2)+1}B_{r(n+2)} + B_{r(n+2)-1}) = \\ &= v_p(a_{r(n+2)+1}B_{r(n+2)}) < v_p(B_{r(n+2)}). \end{aligned}$$

The induction is then complete and the claim holds for all $n \in \mathbb{N}$. □

**Corollary 4.3.7.** *Let $r \in \mathbb{N}^+$ and $a_0, a_1, \ldots$ as in Theorem 4.3.6. Then the continued fraction $[a_0, a_1, \ldots]$ is convergent to a $p$–adic number.*

*Proof.* The continued fraction $[a_0, a_1, \ldots]$ converges in $\mathbb{Q}_p$ if and only if

$$\lim_{n \to +\infty} v_p(B_n B_{n+1}) = -\infty.$$

By Theorem 4.3.6 we have that, for all $n \in \mathbb{N}$,

$$v_p(B_{rn+1}B_{rn+2}) = \ldots = v_p(B_{rn+r-1}B_{rn+r}) > v_p(B_{rn+r}B_{rn+r+1}),$$

so that the sequence $v_p(B_n B_{n+1})$ is decreasing and divergent to $-\infty$. □

By Corollary 4.3.7, we obtain the convergence of a $p$–adic continued fractions algorithm generating the partial quotients as

$$\begin{cases} v_p(a_{rn+1}) < 0 \\ v_p(a_{rn+2}) = 0 \\ v_p(a_{rn+3}) = 0 \\ \ldots \\ v_p(a_{rn+r}) = 0. \end{cases} \tag{4.8}$$

With a construction similar to Example 4.3.1, it can be proved that the conditions of Theorem 4.3.6 are also necessary for the $p$–adic convergence.

## 4.4 Some new algorithms

In this section, we define some new algorithms by exploiting the convergence results of the previous section. In particular, Algorithm (3.8) and Algorithm

(3.9) have been described in [57] and they are based on the results of Theorem 4.3.2, while Algorithm (3.10) has appeared in [55] and it relies on Theorem 4.2.1. We start by defining the two algorithms fulfilling the convergence condition of Theorem 4.3.2. In order to do that, we introduce a third function $u$ to use in combination with the functions $s$ and $t$. For any $p$–adic integer $\alpha = \sum_{n=0}^{+\infty} c_n p^n \in \mathbb{Z}_p$, with $c_i \in \{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\}$, we introduce the new floor function

$$u : \mathbb{Q}_p \to \{-1, 0, +1\},$$

defined as

$$u(\alpha) = \begin{cases} +1 & \text{if } c_0 \in \left\{+2, \ldots, \dfrac{p-1}{2}\right\} \cup \{-1\} \\ -1 & \text{if } c_0 \in \left\{-\dfrac{p-1}{2}, \ldots, -2\right\} \cup \{+1\} \\ 0 & \text{if } c_0 = 0. \end{cases}$$

Therefore, exploiting all the three floor functions $s$, $t$ and $u$, we define the following two novel algorithms, anticipated in Section 3.4.

**Definition 4.4.1** (First new algorithm)**.** *On input $\alpha_0 = \alpha$, for $n \geq 0$, the first new algorithm works as follows:*

$$\begin{cases} a_n = s(\alpha_n) & \text{if } n \equiv 0 \bmod 3 \\ a_n = t(\alpha_n) & \text{if } n \equiv 1 \bmod 3 \text{ and } v_p(\alpha_n - t(\alpha_n)) = 0 \\ a_n = t(\alpha_n) - sign(t(\alpha_n)) & \text{if } n \equiv 1 \bmod 3 \text{ and } v_p(\alpha_n - t(\alpha_n)) \neq 0 \\ a_n = u(\alpha_n) & \text{if } n \equiv 2 \bmod 3 \\ \alpha_{n+1} = \frac{1}{\alpha_n - a_n}. \end{cases}$$

**Definition 4.4.2** (Second new algorithm)**.** *On input $\alpha_0 = \alpha$, for $n \geq 0$, the second new algorithm works as follows:*

$$\begin{cases} a_n = s(\alpha_n) & \text{if } n \equiv 0 \bmod 3 \\ a_n = t(\alpha_n) & \text{if } n \equiv 1 \bmod 3 \text{ and } v_p(\alpha_n - t(\alpha_n)) = 0 \\ a_n = t(\alpha_n) - sign(t(\alpha_n)) & \text{if } n \equiv 1 \bmod 3 \text{ and } v_p(\alpha_n - t(\alpha_n)) \neq 0 \\ a_n = s(\alpha_n) - u(\alpha_n) & \text{if } n \equiv 2 \bmod 3 \\ \alpha_{n+1} = \frac{1}{\alpha_n - a_n}. \end{cases}$$

**Remark 4.4.3.** *The choice of the third function $u$ is a little tricky. In fact, the function $t$ takes all the negative powers, leaving out the zero term. The function $u$ acts on a $p$–adic number with zero valuation, but it has to leave out another $p$–adic number with zero valuation, otherwise the third partial quotient would not have null valuation. Clearly, the choice of this function can be done in several ways. In fact, there are a lot of manners to separate the zero term $a_0 \in \{-\frac{p-1}{2}, \dots, \frac{p-1}{2}\}$ in two nonzero parts. It would be interesting to analyze also other options different from these two proposals.*

Both of the algorithms in Definition 4.4.1 and Definition 4.4.2 produce a sequence of partial quotients $a_0, a_1, \dots \in \mathbb{Q}_p$ such that, for all $n \in \mathbb{N}$,

$$\begin{cases} v_p(a_{3n+1}) < 0 \\ v_p(a_{3n+2}) = 0 \\ v_p(a_{3n}) = 0. \end{cases}$$

We prove that also the additional condition required by Theorem 4.3.2 for the $p$–adic convergence, i.e.

$$v_p(a_{3n+2}a_{3n+3} + 1) = 0,$$

is satisfied for all $n \in \mathbb{N}$ by both algorithm.

**Proposition 4.4.4.** *Let $\alpha \in \mathbb{Q}_p$. Then the partial quotients generated by Algorithm* (3.8) *in Definition 4.4.1 and by Algorithm* (3.9) *in Definition 4.4.2 satisfy the convergence conditions of Theorem 4.3.2.*

*Proof.* To prove the claim, we have to show that, for all $n \in \mathbb{N}$

$$v_p(a_{3n+2}a_{3n+3}+1) = 0,$$

holds for the sequences of partial quotients generated by the two algorithms. We prove it only for Algorithm (3.9) in Definition 4.4.2, the other proof is similar. First we notice that, by construction,

$$v_p(a_{3n+2}a_{3n+3}) = v_p(a_{3n+2}) + v(a_{3n+3}) = 0,$$

so that $v_p(a_{3n+2}a_{3n+3}+1) \geq \min\{v_p(a_{3n+2}a_{3n+3}), v_p(1)\} = 0$. Let us show that the case $v_p(a_{3n+2}a_{3n+3}+1) > 0$ can not occur. For all $n \in \mathbb{N}$,

$$\alpha_{3n+2} = \frac{1}{\alpha_{3n+1} - t(\alpha_{3n+1})} = c_0 + c_1 p + c_2 p^2 + \dots.$$

and

$$\begin{aligned} a_{3n+2} &= s(\alpha_{3n+2}) - u(\alpha_{3n+2}) = c_0 \mp 1, \\ a_{3n+3} &= s(\alpha_{3n+3}) = s\Big(\frac{1}{\alpha_{3n+2} - a_{3n+2}}\Big) = (c_0 - a_{3n+2})^{-1} = \pm 1. \end{aligned}$$

Therefore, the condition $v_p(a_{3n+2}a_{3n+3}+1) = 0$ is satisfied if and only if

$$a_{3n+2}(c_0 - a_{3n+2})^{-1} \equiv (\pm 1)(c_0 \mp 1) \equiv -1 \bmod p$$

is not fulfilled. However, the latter would imply that $c_0 \equiv 0 \bmod p$, but this cannot happen, due to the constraints in the algorithm when using the function $t$. □

However, Algorithms (3.8) and (3.9) do not seem to improve the periodicity properties of *Browkin II*. This result, together with the characterization that we proved in Theorem 4.2.1, suggests that a good $p$–adic continued fraction algorithm should not be too far from the approach of *Browkin I* or *Browkin II*. Moreover, as we see in Section 6.2, which is devoted to periodicity, although *Browkin II* is periodic on more quadratic irrationals than *Browkin I*, it shows more important problems on other theoretical aspects. In order to solve

some of these issues, in [55] we defined the following algorithm, that is a modification of *Browkin II* where the *sign* function is not used. It is Algorithm (3.10), preliminarly presented in Section 3.4, and it works as follows, for any $\alpha_0 \in \mathbb{Q}_p$:

$$\begin{cases} a_n = s(\alpha_n) & \text{if } n \text{ even} \\ a_n = t(\alpha_n) & \text{if } n \text{ odd} \\ \alpha_{n+1} = \frac{1}{\alpha_n - a_n}. \end{cases}$$

In *Browkin II*, the *sign* function is necessary in order to generate the even partial quotients always with zero valuations and hence to satisfy the condition of Browkin's Proposition 4.1.4. Otherwise, without the use of the *sign* function, it might happen that

$$v_p(\alpha_n - t(\alpha_n)) > 0,$$

for some odd $n \in \mathbb{N}$. This implies that

$$v_p(a_{n+1}) = v_p(s(\alpha_{n+1})) < 0,$$

with $n+1$ even, and the hypothesis of Proposition 4.1.4 would not be satisfied. However, in Theorem 4.2.1, the convergence condition of Proposition 4.1.4 has been lightened, always guaranteeing also the $p$–adic convergence of Algorithm (3.10). In fact, our result in Theorem 4.2.1 only requires that one out of two consecutive partial quotients has negative valuation and, unlike *Browkin II*, it gives no further restriction on the behaviour of the second one.

# Chapter 5

# The $p$–adic continued fraction of rational numbers

In this chapter, we analyze the $p$–adic continued fraction expansions of rational numbers. In the field of real numbers, the rational numbers are characterized by finite continued fractions. This is a natural consequence of the finiteness of the Euclidean division algorithm in $\mathbb{Z}$. In fact, for all $a, b \in \mathbb{Z}$, $b \neq 0$, the simple continued fraction of $\frac{a}{b}$ is obtained by iterating

$$\frac{a}{b} = \frac{bq+r}{b} = q + \frac{r}{b} = q + \frac{1}{\frac{b}{r}}, \tag{5.1}$$

where $q = \lfloor \frac{a}{b} \rfloor$ and $|r| < |b|$. An attempt of replicating the Euclidean algorithm for $p$–adic numbers can be found in [28, 46]. Our goal is to have also in $\mathbb{Q}_p$ a continued fractions algorithm that terminates in a finite number of steps for all $\alpha \in \mathbb{Q}$, i.e. every $\alpha$ rational can be represented as a finite $p$–adic continued fraction.

In the first section, we are going to discuss the properties of the continued fraction expansions of rational numbers obtained by the main known algorithms. Then, in the second section we provide the proofs of finiteness for our new continued fraction algorithms. In particular, we prove that Algorithm (3.8) and (3.10) terminate in a finite number of step when the input is a $p$–adic rational.

## 5.1 Rational numbers by means of the known algorithms

For Schneider's continued fractions, Bundschuh [17] proved that rational numbers have not always a finite expansion, but they can also be periodic. In [39], the authors gave a combinatorial characterization of some non-terminating expansions. Very recently, Pejkovic [60] proved a criterion for determining whether the Schneider's continued fraction of a rational number terminates.

**Theorem 5.1.1** ([60]). *Let $\alpha = \frac{a}{b} \in \mathbb{Q}$. Schneider's continued fraction of $\alpha$ either terminates or a period is detected within $O(\log^2 \max\{|a|, |b|\})$ steps.*

For Ruban's continued fractions, Laohakosol [49] proved the following, which is the analogue of Bundschuh's result.

**Theorem 5.1.2** ([49]). *A $p$–adic number is rational if and only if either its Ruban's continued fraction terminates or it is eventually periodic with all partial quotients equal to $p - \frac{1}{p}$ from a certain point onward.*

**Remark 5.1.3.** *A $p$–adic number that has a finite Ruban's continued fraction is, by construction, rational and positive. Therefore, negative numbers can not have a finite Ruban's continued fraction. For example,*

$$-p = (p-1)p + (p-1)p^2 + \ldots = \cfrac{1}{\frac{p-1}{p} + (p-1) + \cfrac{1}{\frac{p-1}{p} + (p-1) + \ddots}},$$

*that is, $-p = \left[\overline{p - \frac{1}{p}}\right]$. In the proof of Theorem 5.1.2, Laohakosol showed that all the continued fractions of rational numbers that are not finite, eventually have $-p$ as complete quotient.*

A proof of the characterization of rational numbers through this algorithm can be found also in [76]. Ruban's continued fractions have been deepened in more details by Capuano, Veneziano and Zannier [22]. In particular, they provided an effective algorithm that determines in a finite number of steps

whether the continued fraction of a rational number terminates or not. In the non-terminating case, a negative complete quotient appears in the expansion of $\alpha = \frac{a}{b}$ in at most $\max\{2, \frac{\log b}{\log p}\}$ steps. Then, they proved the following result that, giving a rational number $\alpha$, establishes how its Ruban's continued fraction changes when varying the prime $p$.

**Proposition 5.1.4** ([22]). *Let $\alpha \in \mathbb{Q}$. Then:*

*i) If $\alpha < 0$, then for every prime number $p$, Ruban's continued fraction of $\alpha$ does not terminate;*

*ii) If $\alpha \geq 0$ and $\alpha \in \mathbb{Z}$, there are only finitely many prime numbers $p$ such that Ruban's continued fraction of $\alpha$ does not terminate;*

*iii) If $\alpha \geq 0$ and $\alpha \notin \mathbb{Z}$, there are only finitely many prime numbers $p$ such that Ruban's continued fraction of $\alpha$ terminates.*

The first definition of $p$–adic continued fractions with the important property of terminating for every rational number is Browkin's first algorithm (3.5). This result is caused by the different choice of the representatives in $\{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\}$ instead of $\{0, \ldots, p-1\}$ (which is, in fact, the only difference between Ruban's and Browkin's algorithm). In this case, the Euclidean absolute value of the partial quotients satisfies the following inequality:

$$|s(\alpha)| = \left| \sum_{n=-r}^{0} c_n p^n \right| \leq \frac{p-1}{2} \left| \sum_{n=-r}^{0} p^n \right| < \frac{p}{2}. \tag{5.2}$$

In the following we provide the proofs for the finiteness of the algorithms presented in [15] and [16] when processing a rational number. We start by proving it for *Browkin I.*

**Theorem 5.1.5** ([15]). *For all $\alpha \in \mathbb{Q}$, Browkin I stops in a finite number of steps.*

*Proof.* Let us notice that in *Browkin I*, for all $n > 0$, $v(\alpha_n) < 0$. Therefore, we can write

$$\alpha_n = \frac{N_n}{p^l D_n}, \quad \text{with } (N_n, D_n) = 1, \quad p \nmid N_n D_n, \quad l \geq 1,$$
$$\alpha_{n+1} = \frac{N_{n+1}}{p^k D_{n+1}}, \quad \text{with } (N_{n+1}, D_{n+1}) = 1, \quad p \nmid N_{n+1} D_{n+1}, \quad k \geq 1.$$

We write the partial quotients as $a_n = \frac{c_n}{p^l}$, with $p \nmid c_n$. Exploiting the fact that $\alpha_{n+1} = \frac{1}{\alpha_n - a_n}$ for all $n \geq 0$, we obtain that

$$N_{n+1}(N_n - c_n D_n) = p^{k+l} D_n D_{n+1}, \quad \text{for all } n \in \mathbb{N}.$$

In this equality all quantities are integers and $(pD_{n+1}, N_{n+1}) = 1$, hence

$$|N_{n+1}| = |D_n|, \quad |(N_n - c_n D_n)| = p^{k+l} |D_{n+1}|.$$

Therefore we can obtain the following inequalities:

$$|D_{n+1}| \leq \frac{|N_n| + |c_n||D_n|}{p^{k+l}} < \frac{|N_n|}{2} + \frac{|D_n|}{2},$$
$$|N_{n+1}| + 2|D_{n+1}| < |D_n| + (|N_n| + |D_n|) < |N_n| + 2|D_n|.$$

The latter inequality means that $\{|N_n| + 2|D_n|\}_{n \in \mathbb{N}}$ is a strictly decreasing sequence of natural numbers and, hence, it is finite. Therefore $\alpha$ has a finite continued fraction and the proof is complete. □

Some results about the complexity of *Browkin I* continued fractions for rational numbers can be found in [12]. The finiteness of Browkin's second algorithm (3.6) over $\mathbb{Q}$ is less straightforward, hence Browkin left it open in [16] as a conjecture. Most recently, more than 20 years after Browkin's second paper [16], Barbero, Cerruti and Murru [5] proved this conjecture by providing an inequality similar to (5.2) also for the second floor function $t$. For the odd partial quotients $a_{2n+1}$, resulting from the use of the function $t$ eventually adjusted with the *sign* function,

$$|a_{2n+1}| \leq 1 - \frac{1}{p^l}, \tag{5.3}$$

where $l = -v_p(\alpha_{2n+1})$. after the definition of this algorithm.

**Theorem 5.1.6** ([5]). *For all $\alpha \in \mathbb{Q}$, Browkin II stops in a finite number of steps.*

*Proof.* Let $\alpha \in \mathbb{Q}$. Then, the valuation of the complete quotients is, by construction,

$$v_p(\alpha_{2k+1}) < 0, \qquad v_p(\alpha_{2k}) = 0,$$

for all $k \geq 1$. Therefore, we can write:

$$\begin{aligned}
\alpha_{2n} &= \frac{N_{2n}}{D_{2n}}, && \text{with } (N_{2n+2}, D_{2n+2}) = 1, \ \ p \nmid N_{2n} D_{2n}, \\
\alpha_{2n+1} &= \frac{N_{2n+1}}{D_{2n+1} p^l}, && \text{with } (N_{2n+1}, D_{2n+1}) = 1, \ \ p \nmid N_{2n+1} D_{2n+1}, \ \ l \geq 1, \\
\alpha_{2n+2} &= \frac{N_{2n+2}}{D_{2n+2}}, && \text{with } (N_{2n+2}, D_{2n+2}) = 1, \ \ p \nmid N_{2n+2} D_{2n+2}.
\end{aligned}$$

Using the formula $\alpha_{k+1} = \frac{1}{\alpha_k - a_k}$ for $k = 2n, 2n+1$, we obtain

$$\begin{aligned}
N_{2n+1}(N_{2n} - c_{2n} D_{2n}) &= p^l D_{2n+1} D_{2n}, \\
N_{2n+2}(N_{2n+1} - c_{2n+1} D_{2n+1}) &= p^l D_{2n+2} D_{2n+1}.
\end{aligned}$$

Since $(N_n, pD_n) = 1$ for all $n \in \mathbb{N}$, then

$$|N_{2n+2}| = |D_{2n+1}|, \quad |N_{2n+1}| = |D_{2n}|,$$

and

$$\begin{aligned}
|D_{2n+1}| p^l &= |N_{2n} - c_{2n} D_{2n}|, \\
|D_{2n+2}| p^l &= |N_{2n+1} - c_{2n+1} D_{2n+1}|.
\end{aligned}$$

Now we notice that, by (5.2) and (5.3),

$$\begin{aligned}
|c_{2n}| &= |a_{2n}| < \frac{p}{2}, \\
|c_{2n+1}| &= p^l a_{2n+1} \leq p^l \left(1 - \frac{1}{p^l}\right).
\end{aligned}$$

Hence, it follows that:

$$|D_{2n+1}| \leq \frac{1}{p^l}\left(|N_{2n}| + \frac{p}{2}|D_{2n}|\right), \tag{5.4}$$

$$|D_{2n+2}| \leq \frac{1}{p^l}|N_{2n+1}| + \left(1 - \frac{1}{p^l}\right)|D_{2n+1}|. \tag{5.5}$$

We substitute $|D_{2n+1}| = |N_{2n+2}|$ into (5.5) in order to obtain:

$$|N_{2n+2}| + p^l|D_{2n+2}| \leq |N_{2n+1}| + p^l|D_{2n+1}|.$$

Using also (5.4) for $|D_{2n+1}|$ in the latter expression, and substituting $|D_{2n+2}| = |N_{2n+3}|$ and $|D_{2n}| = |N_{2n+1}|$, we get:

$$|N_{2n+2}| + p^l|N_{2n+3}| < \left(\frac{p}{2} + 1\right)|N_{2n+1}| + |N_{2n}|.$$

Since, for $l \geq 1$ and $p$ odd, $p^l > \frac{p}{2} + 1$, then

$$\left(\frac{p}{2} + 1\right)|N_{2n+3}| + |N_{2n+2}| < \left(\frac{p}{2} + 1\right)|N_{2n+1}| + |N_{2n}|,$$

that is

$$(p+2)|N_{2n+3}| + 2|N_{2n+2}| < (p+2)|N_{2n+1}| + 2|N_{2n}|$$

Since the sequence $\{(p+2)|N_{2n+1}| + 2|N_{2n}|\}_{n\in\mathbb{N}}$ is a strictly decreasing sequence of natural numbers, then it is finite and $\alpha$ has a finite continued fraction. □

## 5.2 Finiteness of the new algorithms

In this section we prove that the continued fraction expansions provided by Algorithm (3.9) and (3.10) are finite when the input is a rational number.

**Theorem 5.2.1.** *For $\alpha_0 \in \mathbb{Q}$, Algorithm* (3.9) *of Definition 4.4.2 stops in a finite number of steps.*

*Proof.* Let us consider $\alpha \in \mathbb{Q}$. By construction we have,

$$v_p(\alpha_{3k+1}) < 0,\ v_p(\alpha_{3k+2}) = v_p(\alpha_{3k+3}) = 0,$$

so that we can write

$$\begin{aligned}
\alpha_{3k+1} &= \frac{N_{3k+1}}{D_{3k+1}p^l}, && \text{with } (N_{3k+1}, D_{3k+1}) = 1,\ \ p \not| N_{3k+1}D_{3k+1},\ \ l \geq 1,\\
\alpha_{3k+2} &= \frac{N_{3k+2}}{D_{3k+2}}, && \text{with } (N_{3k+2}, D_{3k+2}) = 1,\ \ p \not| N_{3k+2}D_{3k+2},\\
\alpha_{3k+3} &= \frac{N_{3k+3}}{D_{3k+3}}, && \text{with } (N_{3k+3}, D_{3k+3}) = 1,\ \ p \not| N_{3k+3}D_{3k+3}.
\end{aligned}$$

Let us notice that for this algorithm, for all $n \in \mathbb{N}$, the partial quotients are such that $a_{3n+2} \in \{-\frac{p-1}{2}+1, \ldots, -1, 1, \ldots, \frac{p-1}{2}-1\}$ and $a_{3n+3} = \pm 1$, so that

$$|a_{3n+2}| \leq \frac{p-3}{2}, \quad |a_{3n+3}| = 1.$$

Since $v_p(a_{3n+1}) < 0$, we can write

$$a_{3n+1} = \frac{c_{3n+1}}{p^l},\ \text{with } v_p(c_{3n+1}) = 0,\ l \geq 1.$$

The partial quotients $a_{3n+1}$ are generated by the function $t$ and it has been shown in [5] that

$$|c_{3n+1}| \leq p^l \left(1 - \frac{1}{p^l}\right).$$

For the sake of simplicity, we also write $c_{3k+2} = a_{3k+2}$ and $c_{3k+3} = a_{3k+3}$, so that the coefficients $c_n$ always have zero valuation.
Exploiting $\alpha_{k+1} = \frac{1}{\alpha_k - a_k}$, we get

$$\begin{aligned}
N_{3k+1}(N_{3k} - c_{3k}D_{3k}) &= p^l D_{3k}D_{3k+1},\\
N_{3k+2}(N_{3k+1} - c_{3k+1}D_{3k+1}) &= p^l D_{3k+1}D_{3k+2},\\
N_{3k+3}(N_{3k+2} - c_{3k+2}D_{3k+2}) &= D_{3k+2}D_{3k+3}.
\end{aligned}$$

Since $(|N_n|, p|D_n|) = 1$ for all $n \in \mathbb{N}$, then

$$|N_{3k+1}| = |D_{3k}|,\ |N_{3k+2}| = |D_{3k+1}|,\ |N_{3k+3}| = |D_{3k+2}|,$$

and

$$\begin{aligned}
|D_{3k+1}| &= \frac{|N_{3k} - c_{3k}D_{3k}|}{p^l} \leq \frac{|N_{3k}| + |c_{3k}D_{3k}|}{p^l} = \frac{1}{p^l}|N_{3k}| + \frac{1}{p^l}|D_{3k}|, \\
|D_{3k+2}| &= \frac{|N_{3k+1} - c_{3k+1}D_{3k+1}|}{p^l} \leq \frac{1}{p^l}|N_{3k+1}| + \left(1 - \frac{1}{p^l}\right)|D_{3k+1}|, \\
|D_{3k+3}| &= |N_{3k+2} - c_{3k+2}D_{3k+2}| \leq |N_{3k+2}| + \left(\frac{p-3}{2}\right)|D_{3k+2}|.
\end{aligned}$$

By using the formulas above, we may write:

$$\begin{aligned}
&|N_{3k+3}| + |D_{3k+3}| \leq |D_{3k+1}| + \frac{p-1}{2}|D_{3k+2}| \leq \\
&\leq |D_{3k+1}| + \frac{p-1}{2}\left(\frac{1}{p^l}|N_{3k+1}| + \frac{p^l-1}{p^l}|D_{3k+1}|\right) = \\
&= \frac{p-1}{2p^l}|N_{3k+1}| + \frac{p^{l+1}+p^l-p+1}{2p^l}|D_{3k+1}| \leq \\
&\leq \frac{p-1}{2p^l}|D_{3k}| + \frac{p^{l+1}+p^l-p+1}{2p^l} \cdot \left(\frac{1}{p^l}|N_{3k}| + \frac{1}{p^l}|D_{3k}|\right) = \\
&= \left(\frac{p^{l+1}+p^l-p+1}{2p^{2l}}\right)|N_{3k}| + \left(\frac{2p^{l+1}-p+1}{2p^{2l}}\right)|D_{3k}|.
\end{aligned}$$

We have that $2p^{l+1} - p + 1 < 2p^{2l}$, since $p^{2l} \geq p^l$ for every $l \geq 1$ and consequently we also have $p^{l+1} + p^l - p + 1 < 2p^{2l}$. Thus, we obtain, for all $k \in \mathbb{N}$, that

$$|N_{3k+3}| + |D_{3k+3}| < |N_{3k}| + |D_{3k}|.$$

Since the sequence $\{|N_{3n}| + |D_{3n}|\}_{n\in\mathbb{N}}$ is a strictly decreasing sequence of natural numbers, then it is finite and $\alpha$ has a finite continued fraction. $\square$

Before proving the finiteness of Algorithm (3.10) over $\mathbb{Q}$, we need the following lemma, providing a bound on the Euclidean norm of the floor function $t$, obtained with a similar technique of (5.2) for the function $s$.

**Lemma 5.2.2** ([56]). *Let* $\alpha = \sum_{n=-r}^{+\infty} c_n p^n \in \mathbb{Q}_p$, *with* $r \in \mathbb{Z}$ *and* $c_n \in \{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\}$ *for all* $n \in \mathbb{N}$. *Then*

$$\left|t(\alpha)\right| < \frac{1}{2},$$

*where* $|\cdot|$ *is the Euclidean norm.*

*Proof.* If $r \leq 0$ then $|t(\alpha)| = 0 < \frac{1}{2}$ and the claim holds. When $r > 0$, then

$$t(\alpha) = t\Big(\sum_{n=-r}^{+\infty} c_n p^n\Big) = \sum_{n=-r}^{-1} c_n p^n,$$

and we have

$$\begin{aligned}\left|t(\alpha)\right| = \left|\sum_{n=-r}^{-1} c_n p^n\right| \leq \frac{p-1}{2}\left|\sum_{n=-r}^{-1} p^n\right| = \\ = \frac{1}{2}\cdot\frac{(p-1)(1+p+\ldots+p^{r-1})}{p^r} = \\ = \frac{1}{2}\cdot\frac{p^r-1}{p^r} < \frac{1}{2},\end{aligned}$$

and the thesis follows. □

**Theorem 5.2.3.** *For* $\alpha_0 \in \mathbb{Q}$, *Algorithm* (3.10) *stops in a finite number of steps.*

*Proof.* By the construction we have that, for all $n > 0$,

$$\begin{aligned}v_p(\alpha_{2n}) &\leq 0,\\ v_p(\alpha_{2n+1}) &< 0,\\ v_p(\alpha_{2n+2}) &\leq 0.\end{aligned}$$

Hence, the complete quotients have the form

$$\begin{aligned}
\alpha_{2n} &= \frac{N_{2n}}{D_{2n}p^j}, && \text{with } (N_{2n+2}, D_{2n+2}) = 1, \;\; p \not| N_{2n+2}D_{2n+2}, \;\; j \geq 0,\\
\alpha_{2n+1} &= \frac{N_{2n+1}}{D_{2n+1}p^k}, && \text{with } (N_{2n+1}, D_{2n+1}) = 1, \;\; p \not| N_{2n+1}D_{2n+1}, \;\; k \geq 1,\\
\alpha_{2n+2} &= \frac{N_{2n+2}}{D_{2n+2}p^l}, && \text{with } (N_{2n+2}, D_{2n+2}) = 1, \;\; p \not| N_{3n+1}D_{3n+1}, \;\; l \geq 0.
\end{aligned}$$

The partial quotients satisfy, for all $n \in \mathbb{N}$,

$$|a_{2n}| = \left|\frac{c_{2n}}{p^j}\right| < \frac{p}{2}, \qquad |a_{2n+1}| = \left|\frac{c_{2n+1}}{p^k}\right| < \frac{1}{2},$$

for some $j \geq 0$, $k \geq 1$ and $v_p(c_{2n}) = v_p(c_{2n+1}) = 0$. Using the formula $\alpha_{k+1} = \frac{1}{\alpha_k - a_k}$ for $k = 2n, 2n+1$, we obtain

$$\begin{aligned}
N_{2n+1}(N_{2n} - c_{2n}D_{2n}) &= p^{j+k}D_{2n+1}D_{2n},\\
N_{2n+2}(N_{2n+1} - c_{2n+1}D_{2n+1}) &= p^{k+l}D_{2n+2}D_{2n+1}.
\end{aligned}$$

Since $(N_n, pD_n) = 1$ for all $n \in \mathbb{N}$, then

$$|N_{2n+2}| = |D_{2n+1}|, \quad |N_{2n+1}| = |D_{2n}|,$$

and

$$\begin{aligned}
|D_{2n+1}|p^{k+j} &= |N_{2n} - c_{2n}D_{2n}|,\\
|D_{2n+2}|p^{k+l} &= |N_{2n+1} - c_{2n+1}D_{2n+1}|.
\end{aligned}$$

Therefore,

$$\begin{aligned}
|D_{2n+1}| &\leq \frac{|N_{2n}| + |c_{2n}||D_{2n}|}{p^{k+j}} = \frac{|N_{2n}|}{p^{k+j}} + \frac{|c_{2n}|}{p^j} \cdot \frac{1}{p^k}|D_{2n}| < \frac{|N_{2n}|}{p^{k+j}} + \frac{1}{2p^{k-1}}|D_{2n}|,\\
|D_{2n+2}| &\leq \frac{|N_{2n+1}| + |c_{2n+1}||D_{2n+1}|}{p^{k+l}} = \frac{|N_{2n+1}|}{p^{k+l}} + \frac{|c_{2n+1}|}{p^k} \cdot \frac{1}{p^l}|D_{2n+1}| <\\
&< \frac{|N_{2n+1}|}{p^{k+l}} + \frac{1}{2} \cdot \frac{1}{p^l}|D_{2n+1}| = \frac{|N_{2n+1}|}{p^{k+l}} + \frac{1}{2p^l}|D_{2n+1}|,
\end{aligned}$$

so that, since $k \geq 1$ and $j, l \geq 0$,

$$|D_{2n+1}| < \frac{|N_{2n}|}{p} + \frac{|D_{2n}|}{2}, \quad |D_{2n+2}| < \frac{|N_{2n+1}|}{p} + \frac{|D_{2n+1}|}{2}.$$

By using the above formulas we can write:

$$\begin{aligned} |N_{2n+2}| + p|D_{2n+2}| &< |D_{2n+1}| + p\left(\frac{|N_{2n+1}|}{p} + \frac{|D_{2n+1}|}{2}\right) = \\ &= |N_{2n+1}| + \left(\frac{p}{2} + 1\right)|D_{2n+1}| < \\ &< |D_{2n}| + \left(\frac{p}{2} + 1\right)\left(\frac{|N_{2n}|}{p} + \frac{|D_{2n}|}{2}\right) = \\ &= \left(\frac{1}{p} + \frac{1}{2}\right)|N_{2n}| + \left(\frac{p}{4} + \frac{1}{2} + 1\right)|D_{2n}|. \end{aligned}$$

The coefficient of $|N_{2n}|$ is clearly less or equal 1 and the coefficient of $|D_{2n}|$ is less or equal $p$ if and only if $p \geq \frac{p+6}{4}$, that is, if and only if $p \geq 2$. We can conclude that, for all $n \in \mathbb{N}$,

$$|N_{2n+2}| + p|D_{2n+2}| < |N_{2n}| + p|D_{2n}|.$$

The sequence $\{|N_{2n}| + p|D_{2n}|\}_{n \in \mathbb{N}}$ is then a strictly decreasing sequence of natural numbers and, hence, it is finite. Therefore $\alpha$ has a finite continued fraction and the thesis follows. □

# Chapter 6

# Periodicity of $p$–adic continued fractions

The continued fraction expansion of a real number is eventually periodic if and only if it is a quadratic irrational number, by Lagrange's Theorem [47]. Also for $p$–adic continued fractions, periodicity is often related to quadratic irrationals. In fact, a periodic continued fraction can be regarded as the root of a quadratic polynomial. However, we have seen in Chapter 5 that periodic $p$–adic continued fractions can correspond also to rational numbers. On the other hand, none of the existent algorithms has been proved to produce a periodic continued fractions for all quadratic irrationals in $\mathbb{Q}_p$. Therefore, none of the two implications of Lagrange's Theorem is true in general for $p$–adic continued fractions. The latter is one of the most challenging open problems in this research field. This section is devoted to the main results regarding the periodicity of $p$–adic continued fractions up to the most recent developments.

**Remark 6.0.1.** *Periodic continued fractions, when not representing a rational number, converge to some irrational number $\alpha \in \mathbb{Q}_p$ that is quadratic over $\mathbb{Q}$, i.e. it is a root of an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree 2. We denote by $\overline{\alpha}$ the conjugate of $\alpha$, that is the other root of $f(x)$ over $\mathbb{Q}$. Moreover, when we write $\sqrt{D}$ as a root of $x^2 - D$ over $\mathbb{Q}_p$, it must be clear which of the two roots we are meaning. In the case of standard representatives in $\{0, \ldots, p-1\}$, we choose the root that in its p–adic expansion has the smaller*

*first representative, while in the case of representatives in* $\{-\frac{p-1}{2},\dots,\frac{p-1}{2}\}$ *we take the one with positive first representative. We denote the other root by* $-\sqrt{D}$*. In general, we deal with quadratic irrationals* $\alpha$ *having an embedding both in* $\mathbb{R}$ *and* $\mathbb{Q}_p$*, so that we often denote with* $\alpha$ *both the real number and its p–adic counterpart, using a slight abuse of notation.*

Let $\alpha_0 = \frac{P_0+\sqrt{D}}{Q_0} \in \mathbb{Q}_p$, where $D$ is a non-square integer that is a quadratic residue modulo $p$ and $P_0, Q_0 \in \mathbb{Q}$. For all $n \in \mathbb{N}$, the complete quotients of the continued fraction expansion of $\alpha$ can be written as

$$\alpha_n = \frac{P_n + \sqrt{D}}{Q_n}, \tag{6.1}$$

where $P_n, Q_n \in \mathbb{Q}$. Similarly as in the real framework, the sequences $P_n$ and $Q_n$, for all $n \in \mathbb{N}$ can be computed recursively, starting from $P_0$ and $Q_0$, by

$$P_{n+1} = a_n Q_n - P_n, \qquad Q_{n+1} = \frac{D - P_{n+1}^2}{Q_n},$$

where $a_n$ is the $n$-th partial quotient of $\alpha_0$.

Before turning our attention to the periodicity of $p$–adic continued fractions, we list some of the most important and classical results for continued fractions in $\mathbb{R}$, that we aim to generalize in $\mathbb{Q}_p$. The following is a famous result of Galois [30] characterizing purely periodic continued fractions.

**Theorem 6.0.2** (Galois' Theorem)**.** *The continued fraction expansion of a quadratic irrational* $\alpha \in \mathbb{R}$ *is purely periodic if and only if it is reduced, that is* $\alpha > 1$ *and its conjugate* $-1 < \overline{\alpha} < 0$*.*

The idea for proving Galois' Theorem is that the conditions on

$$\alpha = \frac{P_0 + \sqrt{D}}{Q_0},$$

and its conjugate

$$\overline{\alpha} = \frac{P_0 - \sqrt{D}}{Q_0},$$

imply that

$$\begin{aligned} 0 < & P_0 < \sqrt{D}, \\ \sqrt{D} - P_0 < & Q_0 < \sqrt{D} + P_0. \end{aligned}$$

The latter inequalities establish that there are only finitely many *reduced* complete quotients $\alpha_n$, satisfying the hypotheses of Galois' Theorem. Moreover, the property of being *reduced* is inherited by all the subsequent complete quotients. Hence, there is a repetition $\alpha_n = \alpha_{n+k}$, $k \geq 1$, and the expansion is periodic from that point onward.

One of the classical techniques to prove Lagrange's Theorem in $\mathbb{R}$ consists in showing that the expansion of any quadratic irrational, not necessarily *reduced*, eventually reaches a *reduced* complete quotients, hence it starts to be periodic at some point.

Another question that we examine in the $p$–adic framework is the length of the periods for $\sqrt{D}$, $D > 0$. In $\mathbb{R}$, the continued fraction expansion of a "pure" square root is

$$\sqrt{D} = [a_0, \overline{a_1, \ldots, a_k, 2a_0}], \tag{6.2}$$

where $a_1, \ldots, a_n$ is palindromic. In order to verify (6.2), it is sufficient to notice that $\sqrt{D} + \lfloor \sqrt{D} \rfloor$ is reduced, hence purely periodic by Galois' Theorem.

## 6.1 Periodicity of Ruban's and Schneider's algorithms

One of the first works on the periodicity of $p$–adic continued fractions is due to Bundschuh [17]. Bundschuh studied Schneider's continued fractions and suggested that Lagrange's Theorem fails for this algorithm through some numerical computations, although did not prove it. Some years later, de Weger [78] proved the following condition for the non-periodicity of Schneider's continued fractions.

**Proposition 6.1.1** ([78]). *Let $P_n$ and $Q_n$ as in* (6.1). *Then, if for some $n \in \mathbb{N}$ the signs of $P_n$ and $Q_n$ are different and $P_{n+1}^2 > D$, Schneider's continued fraction of $\sqrt{D} \in \mathbb{Z}_p$ is not periodic. In particular, $\sqrt{D} \in \mathbb{Z}_p$ is never periodic for $D < 0$.*

In [77], the same author approached the periodicity of $p$–adic continued fractions from another point of view, i.e. by associating a sequence of *approximation lattices* to every $p$–adic number. In the spirit of Lagrange's Theorem, de Weger proved that the sequence of approximation lattices attached to $\alpha \in \mathbb{Z}_p$ becomes periodic if and only if $\alpha$ is a quadratic irrational. However, this method is not effective for the construction of a periodic continued fraction for a given $p$–adic quadratic irrational. Few years later, Tilborghs [74] determined an algorithm to detect the non-periodicity of Schneider's continued fraction in a finite number of steps. Becker [7] then showed the following result on the length of the pre-periods.

**Proposition 6.1.2** ([7]). *Let $\alpha \in \mathbb{Z}_p$ be quadratic over $\mathbb{Q}$ with periodic Schneider's continued fraction. Then, if $p$ does not divide the discriminant of $\alpha$, the pre-period length is at most* 1.

A fairly complete survey on the periodicity of Schneider's continued fractions is contained in [63]. More recently, this algorithm has been studied also from other points of view and in more generality in [32, 33, 40].

For Ruban's algorithm, using an argument similar to de Weger, Ooto [59] showed that not all quadratic irrationals in $\mathbb{Q}_p$ have a periodic Ruban's continued fraction. In particular, Ooto proved the following result, giving some sufficient conditions to have a non-periodic $p$–adic continued fraction.

**Proposition 6.1.3** ([59]). *Let $\alpha = \sqrt{D} \in \mathbb{Q}_p$ and the sequences $P_n, Q_n$ as in* (6.1) *for some $n \in \mathbb{N}$, $P_n Q_n \leq 0$ and $P_{n+1}^2 > D$, then the Ruban's continued fraction of $\alpha$ is not periodic.*

In the proof of Proposition 6.1.3, the author showed that, in these hypotheses, the sequence $P_n$ has strictly increasing absolute value from some point onward, hence it can not be periodic. From Proposition 6.1.3 it easily follows that, for example, $\sqrt{D}$ can not have a periodic continued fraction if $D < 0$.

In fact, in this case, $P_0Q_0 = 0$ and $P_1 \geq 0 > D$ (in analogy to Proposition 6.1.1 for Schneider's algorithm).

In [22], Capuano, Veneziano and Zannier made a more extensive analysis of Ruban's algorithm. In particular, they provided an effective criterion for determining in a finite number of step whether the expansion of a quadratic irrational becomes periodic. They proved the following result.

**Theorem 6.1.4** ([22]). *Let $\alpha \in \mathbb{Q}_p$ be a quadratic irrational over $\mathbb{Q}$. Then, Ruban's continued fraction of $\alpha$ is periodic if and only if there exists a unique real embedding $j : \mathbb{Q}(\alpha) \to \mathbb{R}$ such that the image of each complete quotient $\alpha_n$ under the map $j$ is positive. Moreover, there exists an effectively computable constant $N_\alpha$ with the property that, either exists $n \leq N_\alpha$ such that $\alpha_n$ does not have a positive real embedding, therefore the expansion is not periodic, or $\alpha_{n_1} = \alpha_{n_2}$ for $n_1 < n_2 \leq N_\alpha$, hence the expansion is periodic.*

In the following, we try to illustrate the general idea behind the proof of Theorem 6.1.4. If a $p$–adic number

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

has got a purely periodic expansion with Ruban's algorithm, then $\alpha = \alpha_k$ for some $k$, hence

$$\alpha = \frac{\alpha_k A_{k-1} + A_{k-2}}{\alpha_k B_{k-1} + B_{k-2}} = \frac{\alpha A_{k-1} + A_{k-2}}{\alpha B_{k-1} + B_{k-2}},$$

and it is a root of the polynomial

$$B_{k-1}\alpha^2 - (A_{k-1} - B_{k-2})\alpha - A_{k-2} = 0.$$

Since all the partial quotients in Ruban's expansion are positive, then the numerators $A_n$ and the denominators $B_n$ are positive for all $n \in \mathbb{N}$. Therefore, if $\alpha$ has a periodic expansion, then

$$\alpha\overline{\alpha} = -\frac{A_{k-1}}{B_k} < 0. \tag{6.3}$$

If $\alpha$ is purely periodic, then all its complete quotients $\alpha_n$ are purely periodic and hence satisfy (6.3). However, this means that

$$\alpha_n \overline{\alpha}_n = \frac{P_n^2 - D}{Q_n^2} < 0, \tag{6.4}$$

for all $n \in \mathbb{N}$. It is not hard to see that (6.4) gives a bound on both $P_n$ and $Q_n$ (depending only on $D$). Therefore, there are only finitely many different complete quotients $\alpha_n$ for a $p$–adic number $\alpha$ having a purely periodic expansion. Now there are two cases:

a) all complete quotients $\alpha_n$ satisfy $\alpha_n \overline{\alpha}_n < 0$, and then we have a repetition within a known bound depending only on the size of $D$,

b) before getting a repetition, we encounter a complete quotient $\alpha_n$ such that $\alpha_n \overline{\alpha}_n \geq 0$, and therefore the expansion of $\alpha$ can not be periodic.

This gives an effective practical criterion for determining the periodicity, or non-periodicity, of Ruban's continued fractions.

In the next section, we are going to see that a similar technique is not applicable for Browkin's algorithms. In fact, since Browkin's partial quotients can also be negative, then (6.3) is not a necessary condition for the periodicity. This is one of the main reasons why the problem of determining if an analogue of Lagrange's Theorem holds or fails is still unsolved.

## 6.2 Periodicity of Browkin's algorithms

In this section, we arise the problem of the periodicity of Browkin's algorithms. Unlike Ruban's and Schneider's case, it is not known whether or not Browkin's continued fractions are periodic for every quadratic irrational and, in general, there is not an effective characterization for the periodicity. However, some numerical simulations suggest that this is not always the case (see, for example, [5, 6, 15, 16, 20, 55]). As we have seen in Section 5.1, for these two algorithms finite continued fractions characterize rational numbers. Therefore, all periodic continued fractions correspond to irrational elements that are quadratic over

$\mathbb{Q}$. The first systematic study of the periodicity of *Browkin I* has been performed by Bedocchi, in a series of papers between 1988 and 1993 [8–11]. The first result concerns purely periodic continued fractions and it is the analogue of Galois' Theorem for classical continued fractions.

**Theorem 6.2.1** ([8]). *Let $\alpha \in \mathbb{Q}_p$ having a periodic Browkin I continued fraction expansion. Then the continued fraction is purely periodic if and only if*

$$|\alpha|_p > 1, \quad |\overline{\alpha}|_p < 1.$$

Theorem 6.2.1 is the analogue of Galois' Theorem 6.0.2 for classical continued fractions and it is similar both in the statement and in the proof. However, notice that the hypothesis of starting from a periodic continued fraction can not be removed. This is in contrast with Galois' Theorem, where the conditions on the norms of $\alpha$ and $\overline{\alpha}$ are also sufficient for obtaining periodicity. Moreover, Bedocchi characterized the possible lengths of the pre-periods for periodic *Browkin I* continued fractions.

**Proposition 6.2.2** ([8]). *Let $D \in \mathbb{Z}$ such that $\sqrt{D} \in \mathbb{Q}_p$, if the Browkin I expansion of $\sqrt{D}$ is periodic, then the pre-period is*

$$\begin{cases} 2 & D \not\equiv 4 \mod 8 \text{ when } p = 2 \\ 3 & \text{otherwise.} \end{cases}$$

Then, Bedocchi focused on the possible lengths of the periods for square roots of integers. We collect all the results in the next proposition.

**Proposition 6.2.3** ([9–11]). *For the algorithm Browkin I, the following statements are true.*

1. *There are no square roots of integers that are periodic with period of length 1;*
2. *For every odd integer $d$, there are only finitely many square roots of integers that are periodic with period of length $d$;*
3. *There exist infinitely many square roots of integers that are periodic with period of length 2, 4 and 6.*

In view of the results of Proposition 6.2.3, Bedocchi left the following conjecture.

**Conjecture 6.2.4** (Bedocchi's Conjecture). *For all even $h \in \mathbb{N}$, there exist infinitely many square roots of integers that are periodic with Browkin I and have a period of length $h$.*

This conjecture is still open. However, for all the lengths that are powers of 2, Bedocchi's Conjecture has been proved by Capuano, Murru and Terracini in [20].

**Theorem 6.2.5** ([20]). *For every $n, k \geq 1$, there are infinitely many $D \in \mathbb{Z}$, with $p \nmid D$, such that the Browkin I expansion of $p^k\sqrt{D}$ is periodic with period of length $2^n$.*

The proof of Theorem 6.2.5 exploits a new definition of a particular class of Browkin's continued fractions, that we introduce in the next definition.

**Definition 6.2.6** ([20]). *Let $[a_0, \ldots, a_{t-1}]$ be a finite Browkin I continued fraction and let us denote by $\tilde{n} = \frac{n}{p^{v_p(n)}}$ the part of $n$ that is coprime to $p$. Then, $[a_0, \ldots, a_{t-1}]$ is nice if:*

*i)* $|a_0|_p > 1$ *and* $|a_0| < \frac{p}{4}$;

*ii)* $\left|\frac{A_{t-1}}{A_{t-2}}\right| > \frac{4}{p}$;

*iii) there exists an integer $q$ such that $\tilde{B}_{t-1}|q|\tilde{B}_{t-1}^2$ and the class of $q$ modulo $\tilde{A}_{t-1}^2$ belongs to the multiplicative subgroup generated by the class of $p$.*

The authors proved the following result for *nice* Browkin's continued fractions.

**Theorem 6.2.7** ([20]). *Let $[a_0, \ldots, a_{t-1}]$ be a nice Browkin's continued fraction. Then there are infinitely many Browkin's partial quotients $a_t$ such that the continued fraction*

$$[a_0, \overline{a_1, \ldots, a_{t-1}, a_t, a_{t-1}, \ldots, a_1, 2a_0}]$$

*converges to a quadratic irrational number of the form $\frac{1}{p^e\sqrt{D}}$, for some $D \in \mathbb{Z}$ not a perfect square.*

Basically, using Theorem 6.2.7, starting with a *nice* sequence $[a_0, a_1, \ldots, a_{t-1}]$ it is possible to provide an infinite family of integers $D$ such that the Browkin's continued fraction of $p^e\sqrt{D}$ is periodic with period $2t$. They left the following conjecture, together with other problems about *nice* continued fractions.

**Conjecture 6.2.8** ([20]). *For every $t \geq 1$ there exists a nice Browkin's continued fraction of length $t$, except when $t = 1$ and $p = 3$.*

By Theorem 6.2.7, solving the latter conjecture implies the existence of infinitely many square roots of integers that have periodic *Browkin I* expansion with period $2t$, for any $t$. Thus, it would give a positive answer to Bedocchi's Conjecture.

Moreover, in the same paper, the authors deepened other aspects of the periodicity of *Browkin I*. The aim was to use an argument similar to that of Capuano, Veneziano and Zannier [22], that we examined at the end of section 6.1), in order to prove a criterion for the periodicity of *Browkin I* expansions. Unfortunately, as already pointed out, Theorem 6.1.4 strongly depends on the fact that Ruban's continued fractions have only positive partial quotients. Therefore, reasoning as in [22], it is possible to obtain some results on the periodicity and on the length of the period for Browkin's continued fractions, only by assuming that (6.3) holds for a sufficiently large number of complete quotients. In fact, unlike for Ruban's expansions, condition (6.3) is not implied by the periodicity. For these reasons, there is not an "easy" way to prove non-periodicity in *Browkin I* up to now. In particular, no quadratic irrational has been proved to have non-periodic *Browkin I* continued fraction, although it is largely believed to fail Lagrange's Theorem (see, for example, the experimental computations in [55]).

In [1], the authors followed another approach to find periodic $p$–adic continued fractions for all the square roots of integers in $\mathbb{Q}_p$, without focusing on a specific algorithm. They used Rédei rational functions [64] to construct a periodic continued fraction converging to $\sqrt{D}$ simultaneously in the real

and the $p$–adic field. It is possible to notice that, for any integer $z$,

$$\sqrt{D} = z + (\sqrt{D} - z) = z + \frac{1}{\frac{1}{\sqrt{D}-z}} = z + \frac{1}{\frac{\sqrt{D}+z}{D-z^2}} =$$
$$= z + \frac{1}{\frac{2z}{D-z^2} + \frac{\sqrt{D}-z}{D-z^2}} = z + \frac{1}{\frac{2z}{D-z^2} + \frac{1}{z+\sqrt{D}}},$$

hence

$$\sqrt{D} = \left[ z, \overline{\frac{2z}{d-z^2}, 2z} \right], \tag{6.5}$$

even if it does not coincide with its expansion with the standard algorithm (see [61]). Rédei rational functions are known to converge to $\sqrt{D}$ in $\mathbb{R}$ (see, for example, [50]). In [1], the authors proved that Rédei functions converge to $\sqrt{D}$ also in $\mathbb{Q}_p$, so that (6.5) is true also for $p$–adic numbers. This construction has been generalized in [5] in order to manage any quadratic irrational, not only square roots of integers. The authors proposed a generalization of Rédei rational functions to provide a periodic continued fraction for $\alpha$ root of the polynomial $x^2 + hx - d$, where $h, d \in \mathbb{Z}$. The expansion is

$$\alpha = \left[ z, \overline{-\frac{h+2z}{z^2+hz-d}, h+2z} \right], \tag{6.6}$$

that yields a periodic representation for $\alpha$ both in $\mathbb{R}$ and $\mathbb{Q}_p$. This result solves the problem of expressing every $p$–adic quadratic irrational as a periodic continued fraction, i.e. by means of a periodic sequence of rational numbers. However, it is not equivalent to Lagrange's Theorem, since the expansion is not obtained by a specific algorithm. In fact, in order to find the expansion (6.6) for $\alpha$, we need from the begin the knowledge that it is a quadratic irrational number and, in addition, of its characteristic polynomial over $\mathbb{Q}$. In the same paper, the authors characterized the cases when *Browkin II* provides a periodic expansion of the form (6.6).

**Theorem 6.2.9** ([5]). *Given $\alpha \notin \mathbb{Q}$ root of the polynomial $x^2 + hx - d$, with $h, d \in \mathbb{Z}$, Browkin II produces the $p$–adic continued fraction*

$$\alpha = \left[ z, \overline{-\frac{h+2z}{p}, h+2z} \right], \tag{6.7}$$

*if and only if*

$$1 \leq |z| \leq \frac{p-1}{2}, \quad 1 \leq |h+2z| \leq \frac{p-1}{2},$$

*for $z$ such that $z^2+hz-d=p$.*

The authors left open the problem of finding an actual algorithm that, for all quadratic irrationals in $\mathbb{Q}_p$, provides periodic representations of the form (6.6), that they call *standard*.

In [56], we employed an approach similar to Bedocchi [8–11] in order to characterize purely periodic continued fractions with *Browkin II* and to study the lengths of the pre-periods and the periods for periodic expansions. The situation is more complicated than *Browkin I*, because of the presence of the *sign* function in (3.6), hence it is possible to obtain only some partial results. The first issue arises when studying the purely periodic continued fractions. In fact, following an argument similar to the proof of Theorem 6.2.1, the conditions on the $p$–adic absolute values of $\alpha$ and its conjugate are only necessary.

**Theorem 6.2.10.** *If $\alpha \in \mathbb{Q}_p$ has a purely periodic continued fraction expansion $\alpha = [\overline{a_0, \ldots, a_{k-1}}]$ with Browkin II, then*

$$|\alpha|_p = 1, \quad |\overline{\alpha}|_p < 1.$$

*Proof.* For the proof of this result, we adapt the technique of [8, Proposition 3.1] for the case of *Browkin II*.
Let us notice that, by the pure periodicity,

$$v_p(\alpha) = v_p(a_0) = v_p(a_k) = 0,$$

then $|\alpha|_p = 1$. If we set, for all $n \in \mathbb{N}$,

$$\alpha_n = [a_n, a_{n+1}, \ldots, a_{n+k-1}, \alpha_n] = [a'_0, a'_1, \ldots, a'_{k-1}, \alpha_n],$$

and $\frac{A'_n}{B'_n}$ are its convergents, then:

$$B'_{k-1}\alpha_n^2 + (B'_{k-2} - A'_{k-1})\alpha_n - A'_{k-2} = 0.$$

By the observation of Remark 4.1.1, we can write

$$|\alpha_n \overline{\alpha}_n|_p = \left|\frac{A'_{k-2}}{B'_{k-1}}\right|_p = \frac{|a'_0|_p |a'_1|_p \dots |a'_{k-2}|_p}{|a'_1|_p \dots |a'_{k-2}|_p |a'_{k-1}|_p} = \frac{|a'_0|_p}{|a'_{k-1}|_p} = \frac{|a_n|_p}{|a_{n+k-1}|_p},$$

from which we get

$$|\overline{\alpha}_n|_p = \frac{1}{|a_{n+k-1}|_p}.$$

Since $k-1$ is odd, then:

$$\begin{cases} |\overline{\alpha}_n|_p = 1 & \text{if } n \text{ odd} \\ |\overline{\alpha}_n|_p < 1 & \text{if } n \text{ even,} \end{cases}$$

and, in particular, for $n = 0$, $|\overline{\alpha}|_p = |\overline{\alpha}_0|_p < 1$. □

In light of Theorem 6.2.10, it is meaningful to wonder which are (and if there exist) the $p$–adic numbers satisfying the necessary condition for pure periodicity.

**Proposition 6.2.11.** *Let $\alpha = a + \sqrt{D} \in \mathbb{Q}_p$, with $a, D \in \mathbb{Z}$, $D$ not a square,*

$$\sqrt{D} = a_0 + a_1 p + a_2 p^2 + \dots.$$

*Then $|\alpha|_p = 1$ and $|\overline{\alpha}|_p < 1$ if and only if $a \equiv a_0 \mod p$.*

*Proof.* Let us notice that $a_0 \not\equiv 0 \mod p$ and, if $|\alpha|_p = 1$ and $|\overline{\alpha}|_p < 1$, then

$$v_p(\overline{\alpha}) = v_p(a - a_0 - a_1 p - a_2 p^2 - \dots) > 1;$$

it means that $a - a_0 \equiv 0 \mod p$, so $a \equiv a_0 \mod p$.
Vice versa, if $a \equiv a_0 \mod p$, then $a = a_0 + kp$, for some $k \in \mathbb{Z}$. Therefore,

$$v_p(\alpha) = v_p(a + \sqrt{D}) = v_p(2a_0 + (k + a_1)p + \dots) = 0,$$

since $2a_0 \not\equiv 0 \mod p$, for $p \neq 2$; moreover

$$v_p(\overline{\alpha}) = v_p(a - \sqrt{D}) = v_p((k - a_1)p + \ldots) > 0.$$

Hence, in this case, $|\alpha|_p = 1$ and $|\overline{\alpha}|_p < 1$. □

In order to study the converse of Theorem 6.2.10, we need some preparatory lemma. We introduce the following notation for the sets of the partial quotients that can be generated by the function $s$ and the function $t$:

$$J_p = \left\{ \frac{a_0}{p^n} \;\middle|\; n \in \mathbb{N},\ -\frac{p^{n+1}}{2} < a_0 < \frac{p^{n+1}}{2} \right\} = \mathbb{Z}\left[\frac{1}{p}\right] \cap \left(-\frac{p}{2}, \frac{p}{2}\right),$$

and

$$K_p = \left\{ \frac{a_0}{p^n} \;\middle|\; n \geq 1,\ -\frac{p^n}{2} < a_0 < \frac{p^n}{2} \right\} = \mathbb{Z}\left[\frac{1}{p}\right] \cap \left(-\frac{1}{2}, \frac{1}{2}\right).$$

The following lemma on the partial quotients generated by the function $s$ is due to Bedocchi.

**Lemma 6.2.12** ([8]). *For all $a, b \in J_p$, with $a \neq b$, we have $v_p(a - b) \leq 0$.*

In [56], we proved a similar lemma for the function $t$ and the set $K_p$.

**Lemma 6.2.13** ([56]). *For all $a, b \in K_p$, with $a \neq b$, we have $v_p(a - b) < 0$.*

*Proof.* Let us write $a = \frac{a_0}{p^n}$ and $b = \frac{b_0}{p^m}$, with $v_p(a_0) = v_p(b_0) = 0$. We can notice that $n, m \geq 1$ since $v_p(a)$ and $v_p(b)$ are both negative. If $n \neq m$, we may suppose $n > m$ without loss of generality, and we get

$$\begin{aligned} v_p(a - b) &= v_p\left(\frac{a_0}{p^n} - \frac{b_0}{p^m}\right) = v_p\left(\frac{a_0 - b_0 p^{n-m}}{p^n}\right) = \\ &= v_p(a_0 - b_0 p^{n-m}) - v_p(p^n) = (n - m) - n = -m < 0. \end{aligned}$$

If $n = m$, then

$$v_p(a - b) = v_p\left(\frac{a_0}{p^n} - \frac{b_0}{p^n}\right) = v_p\left(\frac{a_0 - b_0}{p^n}\right) = v_p(a_0 - b_0) - n.$$

Since $|a_0 - b_0| < p^n$, necessarily $v_p(a_0 - b_0) < n$, hence

$$v_p(a - b) = v_p(a_0 - b_0) - n < 0,$$

and this concludes the proof. □

As already pointed out, unfortunately the converse of Theorem 6.2.10 is not true and the best that one can prove is stated in the following theorem.

**Theorem 6.2.14.** *Consider $\alpha \in \mathbb{Q}_p$ with periodic Browkin II expansion*

$$\alpha = [a_0, a_1, \ldots, a_{h-1}, \overline{a_h, \ldots, a_{h+k-1}}].$$

*If*

$$|\alpha|_p = 1, \quad |\overline{\alpha}|_p < 1,$$

*then the pre-period length can not be odd.*

*Proof.* Let us notice that, by the hypothesis and the construction of *Browkin II*, the period length $k$ is even and, for all $j \in \mathbb{N}$,

$$\begin{aligned} |\alpha|_p &= |\alpha_{2j}|_p = 1, \\ v_p(\alpha) &= v_p(a_0) = v_p(a_{2j}) = 0. \end{aligned}$$

Moreover,

$$\begin{aligned} |\overline{\alpha}_0|_p &= |\overline{\alpha}|_p < 1, \\ v_p(\overline{\alpha}_0) &= v_p(\overline{\alpha}) > 0, \end{aligned}$$

and it follows that:

$$\begin{aligned} v_p(\overline{\alpha}_1) &= v_p\left(\frac{1}{\overline{\alpha}_0 - a_0}\right) = -v_p(\overline{\alpha}_0 - a_0) = -v_p(a_0) = 0, \\ v_p(\overline{\alpha}_2) &= v_p\left(\frac{1}{\overline{\alpha}_1 - a_1}\right) = -v_p(\overline{\alpha}_1 - a_1) = -v_p(a_1) > 0. \end{aligned}$$

Hence, the $p$–adic absolute value of each complete quotient is, for all $j \in \mathbb{N}$,

$$\begin{array}{lll} |\alpha|_p = 1, & |\alpha_{2j+1}|_p > 1, & |\alpha_{2j}|_p = 1, \\ |\overline{\alpha}|_p < 1, & |\overline{\alpha}_{2j+1}|_p = 1, & |\overline{\alpha}_{2j}|_p < 1. \end{array}$$

Since $\alpha$ has a periodic expansion,

$$\frac{1}{\alpha_{h-1}-a_{h-1}} = \alpha_h = \alpha_{h+k} = \frac{1}{\alpha_{h+k-1}-a_{h+k-1}}.$$

So we obtain:

$$|\alpha_{h-1}-\alpha_{h+k-1}|_p = |a_{h-1}-a_{h+k-1}|_p,$$

and, analogously,

$$|\overline{\alpha}_{h-1}-\overline{\alpha}_{h+k-1}|_p = |a_{h-1}-a_{h+k-1}|_p.$$

By contradiction, if the pre-period length $h$ is odd, both $h-1$ and $h+k-1$ are even. Then $v_p(\overline{\alpha}_{h-1}) > 0$ and $v_p(\overline{\alpha}_{h+k-1}) > 0$, so:

$$\begin{aligned} v_p(a_{h-1}-a_{h+k-1})_p = v_p(\overline{\alpha}_{h-1}-\overline{\alpha}_{h+k-1}) \geq \\ \geq \min\{v_p(\overline{\alpha}_{h-1}), v_p(\overline{\alpha}_{h+k-1})\} > 0. \end{aligned}$$

By Lemma 6.2.12, we have that $a_{h-1} = a_{h+k-1}$ and the claim is proved. □

**Remark 6.2.15.** *In the proof of Theorem 6.2.14 we obtained that, for $h$ odd, $a_{h+k} = a_h$ implies $a_{h+k-1} = a_{h-1}$. This is done by using Lemma 6.2.12 of Bedocchi for the function $s$. In Lemma 6.2.13 we proved a similar result for the second function $t$. Lemma 6.2.13 allows us to get the implication from $a_{h+k} = a_h$ to $a_{h+k-1} = a_{h-1}$ also for $h$ even, but only in the case where the odd partial quotients are obtained using the floor function $t$ without the sign. In fact, in this case, if the pre-period length $h$ is even, both $h-1$ and $h+k-1$ are odd. Then $v_p(\overline{\alpha}_{h-1}) = 0$ and $v_p(\overline{\alpha}_{h+k-1}) = 0$. Therefore, if $a_{h-1} = t(\alpha_{h-1})$ and $a_{h+k-1} = t(\alpha_{h+k-1})$, then $a_{h-1}, a_{h+k-1} \in K_p$. Reasoning as in the proof of Theorem 6.2.14 for $h$ odd, we get*

$$\begin{aligned} v_p(a_{h-1}-a_{h+k-1})_p = v_p(\overline{\alpha}_{h-1}-\overline{\alpha}_{h+k-1}) \geq \\ \geq \min\{v_p(\overline{\alpha}_{h-1}), v_p(\overline{\alpha}_{h+k-1})\} \geq 0. \end{aligned}$$

*We conclude by Lemma 6.2.13 that $a_{h-1} = a_{h+k-1}$ also when $h$ is even.*

We have seen in Remark 6.2.15 that using Lemma 5.2.2 and Lemma 6.2.13 we obtain that $a_{h+k} = a_h$ implies $a_{h+k-1} = a_{h-1}$ also for $h$ even when these

two partial quotients are computed using the function $t$. The problem with *Browkin II* is that, for some odd $n \in \mathbb{N}$,

$$a_n = t(\alpha_n) - sign(t(\alpha_n)).$$

This happens when $\alpha_n$ has not the zero term, in order to always recover a partial quotient with null $p$–adic valuation. In the following example we see that this case can actually occur.

**Example 6.2.16.** *Let us consider*

$$\sqrt{30} = 3 - 3 \cdot 7 + \ldots \in \mathbb{Q}_7,$$

*then the expansion of* $\alpha = \sqrt{30} + 3$ *is*

$$\sqrt{30} + 3 = \left[ -1, \frac{3}{7}, 3, \frac{2}{7}, \overline{1, \frac{2}{7}, -2, \frac{3}{7}, 1, \frac{2}{7}, 2, \frac{1}{7}, -1, -\frac{5}{7}} \right],$$

*that is not purely periodic and has pre-period* $4$*. Notice that the* $7$*–adic number* $\alpha$ *satistfies the hypothesis of Theorem 6.2.14 since*

$$\begin{aligned} v_7\left(3 + \sqrt{30}\right) &= 0, \\ v_7\left(3 - \sqrt{30}\right) &= v_7\left( -3 \cdot 7 + \ldots \right) > 0. \end{aligned}$$

*In this case we can not make the step backward from* $a_4 = a_{14}$ *to* $a_3 = a_{13}$ *since*

$$\begin{aligned} a_3 &= t(\alpha_3) = \frac{2}{7}, \\ a_{13} &= t(\alpha_{13}) - sign(t(\alpha_{13})) = \frac{2}{7} - 1 = -\frac{5}{7}. \end{aligned}$$

*In fact in the generation of* $a_{13}$ *it is used the sign function along with the* $t$ *function.*

In Remark 6.2.15 and Example 6.2.16, we have observed that the converse of Theorem 6.2.10 holds whenever the function *sign* does not appear during

the generation of the even partial quotients $a_h$ and $a_{h+k}$, or whenever they use the same function sign. This problem on the *sign* functions affects also the possible lengths of the pre-periods that, as we see in the next results, can be various. In particular, we prove the following theorem.

**Theorem 6.2.17** ([56]). *Let $\sqrt{D}$ be defined in $\mathbb{Q}_p$, with $D \in \mathbb{Z}$ not a square. Then, if $\sqrt{D}$ has a periodic continued fraction with Browkin II, the pre-period has length either 1 or even.*

In order to do that, we need some preparatory result. In particular, we introduce the following modification of *Browkin II*.

**Definition 6.2.18** (*Browkin II**). *We call Browkin II* the algorithm where the role of the functions $s$ and $t$ is switched. Starting from $\alpha_0 \in \mathbb{Q}_p$, with $v_p(\alpha_0) < 0$, the partial quotients of the $p$–adic continued fraction expansion are obtained for $n \geq 0$ by*

$$\begin{cases} a_n = s(\alpha_n) & \text{if } n \text{ odd} \\ a_n = t(\alpha_n) & \text{if } n \text{ even and } v_p(\alpha_n - t(\alpha_n)) = 0 \\ a_n = t(\alpha_n) - sign(t(\alpha_n)) & \text{if } n \text{ even and } v_p(\alpha_n - t(\alpha_n)) \neq 0 \\ \alpha_{n+1} = \frac{1}{\alpha_n - a_n}. \end{cases} \tag{6.8}$$

The $p$–adic convergence of this continued fraction is guaranteed by Theorem 4.2.5 and it is not hard to see that the observations of Remark 4.1.1 hold also for *Browkin II**. Using the same argument of Theorem 6.2.10 and Theorem 6.2.14, adapting it by switching the even and the odd steps, it is possible to prove two analogous theorems also for *Browkin II**.

**Theorem 6.2.19.** *If $\alpha \in \mathbb{Q}_p$ has a purely periodic continued fraction expansion $\alpha = [\overline{a_0, \ldots, a_{k-1}}]$ with Browkin II*, then*

$$v_p(\alpha) < 0, \quad v_p(\overline{\alpha}) = 0.$$

**Theorem 6.2.20.** *Let $\alpha \in \mathbb{Q}_p$ with periodic Browkin II* expansion*

$$\alpha = [a_0, a_1, \ldots, a_{h-1}, \overline{a_h, \ldots, a_{h+k-1}}].$$

*Then, if*

$$v_p(\alpha) < 0, \quad v_p(\overline{\alpha}) = 0,$$

*the pre-period length can not be even.*

In the following example, as we have done in Example 6.2.16, we show that a full converse of Theorem 6.2.19 is not true.

**Example 6.2.21.** *Under these hypotheses, Theorem 6.2.20 is the best we can obtain as a converse of Theorem 6.2.19. In fact, if we consider the expansion of* $\alpha = \frac{2+\sqrt{79}}{75}$ *in* $\mathbb{Q}_5$ *is*

$$\frac{2+\sqrt{79}}{75} = \Big[-\frac{7}{25}, 1, \frac{2}{5}, 2, -\frac{2}{5}, 1, \frac{1}{5}, 2, -\frac{4}{25}, 2, \frac{1}{5}, 1, -\frac{2}{5}, \overline{2, \frac{2}{5}, 1, -\frac{7}{25}, -1, \frac{1}{5}, 2, \frac{9}{25}, -1, -\frac{3}{5}}\Big],$$

*that is not purely periodic and has pre-period* 15. *Notice that* $\alpha$ *satisfies the hypothesis of Theorem 6.2.20 since starting from*

$$\sqrt{79} = 2 + 2 \cdot 5^2 + 5^3 + \ldots \in \mathbb{Q}_5,$$

*then:*

$$v_5\Big(\frac{2+\sqrt{79}}{75}\Big) = v_5(2+\sqrt{79}) - v_5(75) = v_p(4+\ldots) - 2 = -2 < 0,$$
$$v_5\Big(\frac{2-\sqrt{79}}{75}\Big) = v_5(2-\sqrt{79}) - v_5(75) = v_5(2 \cdot 5^2 + 5^3 + \ldots) - 2 = 0.$$

As consequence of the previous results, we are able to provide the proof of Theorem 6.2.17, characterizing the length of the pre-periods for square roots of integers that have a periodic representation by means of *Browkin II*.

*Proof of Theorem 6.2.17.* Notice that $\alpha = \sqrt{D}$ can not have purely periodic continued fraction, by Theorem 6.2.10. We can then write it as

$$\alpha = a_0 + \frac{1}{\alpha_1}.$$

Since $\alpha$ has a periodic continued fraction, also $\alpha_1$ has periodic continued fraction. We are going to show that:

$$\begin{aligned} i) \quad & v_p(\alpha_1) = v_p\left(\frac{1}{\alpha - a_0}\right) = -v_p(\alpha - a_0) < 0, \\ ii) \quad & v_p(\overline{\alpha}_1) = v_p\left(\frac{1}{\overline{\alpha} - a_0}\right) = -v_p(\overline{\alpha} - a_0) = 0. \end{aligned}$$

Notice that $i)$ is satisfied since $s(\alpha) = a_0$ and $v_p(\alpha - a_0) > 0$. Since $\overline{\alpha} = -\sqrt{D}$, then

$$\overline{\alpha} = -a_0 + a_1' p + a_2' p^2 + \dots.$$

Now, $v_p(\overline{\alpha} - a_0) = 0$ if and only if $a_0 \neq -a_0$, that is $2a_0 \neq 0$. This is always the case for $p \neq 2$, so, by Theorem 6.2.20, $\alpha_1$ can not have an even pre-period length. So $\alpha$ has either pre-period of length 1 or of even length, as wanted. □

Finally, we analyze the length of the period for periodic *Browkin II* continued fractions, trying to obtain some results similar to Proposition 6.2.3. First of all let us notice that, by construction, the length can not be odd. In fact, the odd partial quotients are always rational numbers with negative valuation, while even partial quotients are integers. In [16], Browkin provided an example of an infinite family of square roots of integers having periodic *Browkin II* continued fraction expansion with period of length 2.

**Proposition 6.2.22** ([16]). *Let $a, c, D \in \mathbb{Z}$, with $p \nmid acD$, $b \in \mathbb{Z}\left[\frac{1}{p}\right]$, $D$ not a perfect square. Then*

$$\sqrt{D} = \left[a, \overline{b, c}\right],$$

*if and only if $c = 2a$, $b = \frac{2a}{dp^k}$, for some $k \geq 1$, $d | 2a$ and $m = a^2 + dp^k$. Moreover, there are infinitely many $a, b, c$ with such property.*

In the same paper, Browkin also constructed a family of periodic continued fractions with period of length 4. However, he did not succed to prove that there exist, among them, infinitely many square roots of integers. We solved this problem in [56] by constructing, for every prime $p$, an infinite family of periodic *Browkin II* continued fractions with period of length 4.

**Theorem 6.2.23.** *Given* $D = \dfrac{1-p^t}{(1-p)^2} \cdot p^2$, *for any integer* $t \geq 2$, *then the Browkin II expansion of* $\pm\sqrt{D}$ *is*

$$\pm\sqrt{D} = \left[0, \pm\frac{1}{p}, \overline{\mp 1, \mp\frac{2(p^{t-1}-1)}{(p-1)p^{t-1}}, \mp 1, \pm\frac{2}{p}}\right].$$

*Proof.* In the following, we suppose $p = 4k+1$, the proof for the case $p = 4k-1$ is similar.
From [9, Eq. 2.1], it follows that

$$\sqrt{D} = p(1+p+\ldots+p^{t-1}) + Ap^{t+1},$$

where

$$A = -\frac{p-1}{2} + p - \frac{p-1}{2}p^2 + p^3 - \ldots - \frac{p-1}{2}p^{t-1} + A'p^t,$$

for a certain $A' \in \mathbb{Q}_p$ with $v_p(A') = 0$ and assuming $t$ odd (a similar result holds for $t$ even). Thus, considering $\alpha_0 = \sqrt{D}$, we immediately get $a_0 = s(\alpha_0) = 0$. Applying *Browkin II*, we obtain

$$\alpha_1 = \frac{\sqrt{D}}{D} = \frac{1}{p} - 1 + \frac{Ap^{t+1}}{q \cdot p^2},$$

where $q = \dfrac{1-p^t}{16k^2}$, and so $a_1 = t(\alpha_1) = \dfrac{1}{p}$. The next complete quotient is

$$\alpha_2 = \frac{\sqrt{D}+qp}{1-q} = \frac{(2-p)(1-p^t) + A(p-1)^2p^t}{p^{t-1}+p-2}.$$

Since

$$\frac{1}{p^{t-1}+p-2} = \frac{p-1}{2} + \ldots$$

we have $a_2 = s(\alpha_2) = -1$. In the next step, we have

$$\alpha_3 = \frac{p-\sqrt{D}}{p-\sqrt{D}+p\sqrt{D}} = -\frac{p^2+\ldots+p^t+Ap^{t+1}}{(1-A+Ap)p^{t+1}} = \\ = -\frac{1}{B}\left(\frac{1}{p^{t-1}}+\ldots+\frac{1}{p}\right)-\frac{A}{B},$$

where $B = 1-A+Ap$ and $v_p(A) = v_p(B) = 0$. Now, we prove that $\frac{1}{B} = 2+Cp^t$ for some $C$ such that $v_p(C) = 0$. In this way, it follows that

$$a_3 = t(\alpha_3) = -2\left(\frac{1}{p^{t-1}}+\ldots+\frac{1}{p}\right) = -\frac{p^{t-1}-1}{2kp^{t-1}},$$

considering that $4k = p-1$. To prove that $\frac{1}{B} = 2+Cp^t$, first of all we can observe that

$$B = 1+\left(\frac{p-1}{2}-p+\frac{p-1}{2}p^2-\ldots+\frac{p-1}{2}p^{t-1}+\ldots\right)+ \\ +\left(-\frac{p-1}{2}p+p^2-\frac{p-1}{2}p^3+\ldots-\frac{p-1}{2}p^t+\ldots\right).$$

Using that $1+\frac{p-1}{2} = -\frac{p-1}{2}+p$, we obtain

$$B = -\frac{p-1}{2}-\frac{p-1}{2}p-\ldots-\frac{p-1}{2}p^t+\ldots$$

Thus, we have that $\frac{1}{B} = 2+\ldots$ and we want to prove that $v_p\left(\frac{1}{B}-2\right) \geq t+1$. To prove this, it is sufficient to observe that

$$1-2B = p^{t+1}+\ldots$$

We continue to apply *Browkin II* and we get, after some calculations,

$$\alpha_4 = \frac{p^t(p-1)}{p^t - p - (p-1)\sqrt{D}}.$$

Exploiting the previous results, we have

$$\alpha_4 = -\frac{1}{1+Ap},$$

and considering that $\dfrac{-1}{1+Ap} = -1 + \ldots$, we obtain $a_4 = -1$. For the next step, we have

$$\alpha_5 = \frac{p - p^t + (p-1)\sqrt{D}}{p - p^{t+1} + (p-1)\sqrt{D}} = 1 + \frac{1}{Ap} = \frac{2}{p} - 1 + \ldots$$

from which $a_5 = t(\alpha_5) = \dfrac{2}{p}$. Finally, one can check that

$$\frac{1}{\alpha_5 - a_5} = \alpha_2,$$

and the thesis follows. □

**Corollary 6.2.24.** *There are infinitely many $\sqrt{D} \in \mathbb{Q}_p$, with $D \in \mathbb{Z}$, having a periodic $p$–adic expansion with period 4 by means of Browkin II.*

*Proof.* Since $p$ and $(1-p)^2$ are coprime, then there exist infinitely many integers $t$ such that $p^t \equiv 1 \pmod{(1-p)^2}$. By Theorem 6.2.23 we know that $\sqrt{\dfrac{1-p^t}{(1-p)^2} \cdot p^2}$ has a $p$–adic expansion with period 4 by means of *Browkin II* for all $t \geq 2$ and the thesis follows. □

The problems that we have highlighted for *Browkin II* are due to the unforeseeable use of the sign function. In fact, the properties of periodicity of *Browkin II* strongly depend on the application of the sign function during the algorithm. For this reason, in the first part of [55], we tried to give some methodology to predict the use of the sign function and allow a better understanding of the properties of periodicity.

**Definition 6.2.25.** *Given* $\alpha_0 = \sum_{n=-r}^{+\infty} a_n p^n \in \mathbb{Q}_p$, *let us define the function* $B : \mathbb{Q}_p \to \{-1, 0, +1\}$ *as follows:*

$$B(\alpha) := \begin{cases} -1 & \text{if } a_0 = 0 \text{ and } sign(t(\alpha)) = -1 \\ 0 & \text{if } a_0 \neq 0 \\ +1 & \text{if } a_0 = 0 \text{ and } sign(t(\alpha)) = +1. \end{cases} \tag{6.9}$$

Using this definition, we can rewrite *Browkin II* as

$$\begin{cases} b_n = s(\alpha_n) & \text{if } n \text{ even} \\ b_n = t(\alpha_n) - B(\alpha_n) & \text{if } n \text{ odd} \\ \alpha_{n+1} = \frac{1}{\alpha_n - b_n}, \end{cases}$$

for all $n \geq 0$. Notice that we are interested on the value of $B(\alpha_n)$ only for odd $n$, i.e., when we use the function $t$. The problem of determining the exact behaviour of $B(\alpha_n)$ seems to be hard in general but it is crucial for the study of the periodicity of *Browkin II*. In the following theorem, we prove a necessary and sufficient condition to decide whether or not the sign function is going to be used at the $(k+1)$-th step, only by looking at the coefficients of the $p$–adic expansion of the $k$-th complete quotient. The effectiveness of this result is that it does not require the explicit computation of $\alpha_{k+1}$. Before stating the theorem, we need the following definition.

**Definition 6.2.26.** *Given* $\alpha = \sum_{i=-r}^{+\infty} c_i p^i \in \mathbb{Q}_p$, *we define the matrix*

$$C_\alpha = \begin{pmatrix} c_{n+1} & c_n & 0 & \dots & 0 \\ c_{n+2} & c_{n+1} & c_n & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ c_{2n-1} & c_{2n-2} & \dots & \ddots & c_n \\ c_{2n} & c_{2n-1} & \dots & \dots & c_{n+1} \end{pmatrix},$$

*where* $n = v_p(\alpha - s(\alpha))$.

**Theorem 6.2.27.** *Given $\alpha_0 \in \mathbb{Q}_p$, for all even $k \in \mathbb{N}$, $B(\alpha_{k+1}) \neq 0$ if and only if $det(C_{\alpha_k}) = 0$, where $\alpha_k$ is the $k$-th complete quotient of the Browkin II expansion of $\alpha_0$.*

*Proof.* Let $\alpha_k = \sum_{i=-r'}^{+\infty} c_i p^i$ and $\alpha_{k+1} = \sum_{i=-r}^{+\infty} d_i p^i$ be two consecutive complete quotients, with $k$ even. By definition $B(\alpha_{k+1}) \neq 0$ if and only if $d_0 = 0$. We call $n = v_p(\alpha_k - s(\alpha_k)) > 0$, so that

$$\alpha_k - s(\alpha_k) = c_n p^n + c_{n+1} p^{n+1} + \dots.$$

In this case the valuation of $\alpha_{k+1}$ is

$$v_p(\alpha_{k+1}) = -v_p(\alpha_k - s(\alpha_k)) = -n,$$

hence we can write it as

$$\alpha_{k+1} = d_{-n}\frac{1}{p^n} + d_{-(n-1)}\frac{1}{p^{n-1}} + \ldots + d_{-1}\frac{1}{p} + d_0 + \dots.$$

We want that $\alpha_{k+1}(\alpha_k - s(\alpha_k)) = 1$, that is,

$$c_n d_{-n} + (c_{n+1} d_{-n} + c_n d_{-(n-1)})p + \ldots + (c_{2n} d_{-n} + \ldots + c_n d_0)p^n + \ldots = 1.$$

Hence, the coefficients $d_i$ are uniquely determined as solutions of the following system:

$$\begin{cases} d_{-n} c_n = 1 \\ d_{-n} c_{n+1} + d_{-(n-1)} c_n = 0 \\ d_{-n} c_{n+2} + d_{-(n-1)} c_{n+1} + d_{-(n-2)} c_n = 0 \\ \dots \\ \sum_{k=0}^{n} d_{-n+k} c_{2n-k} = 0. \end{cases}$$

If we call

$$C = \begin{pmatrix} c_n & 0 & 0 & \dots & 0 \\ c_{n+1} & c_n & 0 & \dots & 0 \\ c_{n+2} & c_{n+1} & c_n & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ c_{2n} & c_{2n-1} & \dots & c_{n+1} & c_n \end{pmatrix}$$

the $(n+1) \times (n+1)$ matrix of the coefficients, then $d_0$ is

$$d_0 = \frac{det \begin{pmatrix} c_n & 0 & 0 & \dots & 1 \\ c_{n+1} & c_n & 0 & \dots & 0 \\ c_{n+2} & c_{n+1} & c_n & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ c_{2n} & c_{2n-1} & \dots & c_{n+1} & 0 \end{pmatrix}}{det(C)}.$$

In particular, $d_0 = 0$ if and only if the numerator is zero, i.e. $det(C_{\alpha_k}) = 0$. □

Although it is possible to predict the appearance of the sign function one step in advance, it seems difficult to generalize this construction to make a prediction at a generic step. Therefore, the use of the sign function makes incomplete the study of the periodicity.

For all the reasons highlighted in this section, in [55] we introduced Algorithm (3.10), that is very similar to *Browkin II* but its properties do not rely on the *sign* function $B$.

## 6.3 Periodicity of the new algorithm

In this section, we study the periodicity of Algorithm (3.10), that we introduced in [55], in order to improve *Browkin II*.

**Theorem 6.3.1.** *If $\alpha \in \mathbb{Q}_p$ has a periodic continued fraction expansion by means of Algorithm* (3.10)*, then the expansion is purely periodic if and only if*

$$|\alpha|_p \geq 1, \qquad |\overline{\alpha}|_p < 1.$$

*Proof.* By the pure periodicity, we get that

$$|\alpha|_p = |a_0|_p = |a_k|_p \geq 1,$$

since the length $k$ of the period is even. Indeed, as in *Browkin II*, we can not have periodic continued fractions of odd period length since we use different floor functions. For the norm of its conjugate $\overline{\alpha}$ we apply the usual relation (see [8] and [56]), that is

$$|\overline{\alpha}|_p = \frac{1}{|a_{k-1}|_p}.$$

Since $k-1$ is odd, this implies that $|a_{k-1}|_p > 1$ and $|\overline{\alpha}|_p < 1$, proving the necessary condition for the pure periodicity. Conversely, let us consider a periodic continued fraction expansion

$$\alpha = [a_0, \ldots, a_{h-1}, \overline{a_h, \ldots, a_{h+k-1}}],$$

and let us assume that $|\alpha|_p \geq 1$ and $|\overline{\alpha}|_p < 1$. We are going to prove that $h = 0$, namely the expansion is purely periodic. For all $n \in \mathbb{N}$, the valuations of the complete quotients are

$$\begin{aligned} v_p(\alpha_{2n}) &= v_p(a_{2n}) \leq 0, \\ v_p(\alpha_{2n+1}) &= v_p(a_{2n+1}) < 0, \end{aligned}$$

and the valuations of their conjugates are

$$\begin{aligned} v_p(\overline{\alpha}_{2n+1}) &= v_p\left(\frac{1}{\overline{\alpha}_{2n} - a_{2n}}\right) = -v_p(\overline{\alpha}_{2n} - a_{2n}) = -v_p(a_{2n}) \geq 0, \\ v_p(\overline{\alpha}_{2n+2}) &= v_p\left(\frac{1}{\overline{\alpha}_{2n+1} - a_{2n+1}}\right) = -v_p(\overline{\alpha}_{2n+1} - a_{2n+1}) = -v_p(a_{2n+1}) > 0. \end{aligned}$$

By the periodicity of the continued fraction of $\alpha$, we can observe that

$$\frac{1}{\alpha_{h-1} - a_{h-1}} = \alpha_h = \alpha_{h+k} = \frac{1}{\alpha_{h+k-1} - a_{h+k-1}}.$$

Therefore, we easily obtain the two relations

$$v_p(\alpha_{h-1} - \alpha_{h+k-1}) = v_p(a_{h-1} - a_{h+k-1}),$$
$$v_p(\overline{\alpha}_{h-1} - \overline{\alpha}_{h+k-1}) = v_p(a_{h-1} - a_{h+k-1}).$$

Now, let us assume by contradiction that the pre-period is an odd integer $h \geq 1$. Since in this case $h-1$ and $k-1$ are even,

$$v_p(\overline{\alpha}_{h-1}) > 0 \quad \text{and} \quad v_p(\overline{\alpha}_{h+k-1}) > 0.$$

It follows that

$$v_p(a_{h-1} - a_{h+k-1})_p = v_p(\overline{\alpha}_{h-1} - \overline{\alpha}_{h+k-1}) \geq \min\{v_p(\overline{\alpha}_{h-1}), v_p(\overline{\alpha}_{h+k-1})\} > 0.$$

Since the partial quotients $a_{h-1}$ and $a_{h+k-1}$ are generated with the function $s$, by Proposition 6.2.12 we conclude that $a_{h-1} = a_{h+k-1}$, hence the pre-period can not be odd.
Let us now assume that the pre-period is an even integer $h \geq 2$. In this case $h-1$ and $k-1$ are odd, hence

$$v_p(\overline{\alpha}_{h-1}) \geq 0, \quad v_p(\overline{\alpha}_{h+k-1}) \geq 0.$$

Reasoning as in the previous case, we obtain

$$v_p(a_{h-1} - a_{h+k-1})_p = v_p(\overline{\alpha}_{h-1} - \overline{\alpha}_{h+k-1}) \geq \min\{v_p(\overline{\alpha}_{h-1}), v_p(\overline{\alpha}_{h+k-1})\} \geq 0$$

In this second case, $a_{h-1}$ and $a_{h+k-1}$ are generated with the function $t$, hence by Lemma 6.2.13 we conclude that $a_{h-1} = a_{h+k-1}$. Thus the pre-period can not be a positive even number. It follows that $h = 0$ and the expansion of $\alpha$ with the Algorithm (3.10) is purely periodic. □

Now we analyze the possible pre-periods for the expansions of square roots of integers obtained using Algorithm (3.10). In particular, we are going to show that the pre-period length of periodic continued fraction expansions is always 1 for square roots of integers with valuation zero, obtaining a result similar to Galois' Theorem for classical continued fractions.

In order to prove it, we define the following algorithm, which is similar to the Algorithm (3.10) but the role of the functions $s$ and $t$ is switched.

$$\begin{cases} a_n = t(\alpha_n) & \text{if } n \text{ even} \\ a_n = s(\alpha_n) & \text{if } n \text{ odd} \\ \alpha_{n+1} = \frac{1}{\alpha_n - a_n}. \end{cases} \tag{6.10}$$

This is the same technique that we used in Section 6.2 to prove Theorem 6.2.17 for the pre-periods of *Browkin II*. The $p$–adic convergence of the continued fraction generated by Algorithm (6.10) is guaranteed by Theorem 4.2.1 since, also in this case, $v_p(a_n a_{n+1}) < 0$ for all $n \in \mathbb{N}$. In order to characterize the length of the pre-periods for Algorithm (3.10) we need an analogue of Theorem 6.3.1 for Algorithm (6.10).

**Theorem 6.3.2.** *Let us consider $\alpha \in \mathbb{Q}_p$ with a periodic continued fraction obtained using Algorithm* (6.10)*. Then the expansion is purely periodic if and only if*

$$|\alpha|_p > 1, \qquad |\overline{\alpha}|_p \leq 1.$$

*Proof.* The proof is straightforward adapting the technique of Theorem 6.3.1 and switching the use of the two floor functions. □

Using the results of Theorem 6.3.1 and 6.3.2 we are able to prove the following result, characterizing the pre-period of periodic continued fraction expansions of square roots of integers obtained using the Algorithm (3.10).

**Proposition 6.3.3.** *Let $\sqrt{D} \in \mathbb{Q}_p$, with $D \in \mathbb{Z}$ not a square and $p \nmid D$, having a periodic continued fraction obtained with Algorithm* (3.10)*. Then the pre-period has length* 1*.*

*Proof.* By the characterization of Theorem 6.3.1, $\alpha$ can not have a purely periodic continued fraction. We can write $\alpha$ as

$$\alpha = c_0 + \frac{1}{\alpha_1},$$

where $c_0 = s(\alpha)$ and $\alpha_1$ is the second complete quotient. In order to prove that the periodic expansion of $\alpha$ has pre-period of length 1 we show that $\alpha_1$ has purely periodic expansion with Algorithm (6.10) starting with the function $t$. Therefore, by Theorem 6.3.2, we want to prove that $v_p(\alpha_1) < 0$ and $v_p(\overline{\alpha}_1) \geq 0$. First of all we notice that, since $\alpha$ has a periodic continued fraction expansion, also $\alpha_1$ does. Then, by the construction of the algorithm,

$$v_p(\alpha_1) = -v_p(\alpha - s(\alpha)) < 0,$$

hence the condition on $\alpha_1$ is true. Since $\overline{\alpha} = -\sqrt{D}$, then

$$\overline{\alpha} = -a_0 + c_1' p + c_1' p^2 + \dots.$$

We have that

$$v_p(\overline{\alpha}_1) = -v_p(\overline{\alpha} - a_0) < 0,$$

if and only if $v_p(-2a_0 + \dots) > 0$, that is never the case for $p \neq 2$. This means that $v_p(\overline{\alpha}_1) \geq 0$ and, by Theorem 6.3.2, it has a purely periodic expansion

$$\alpha_1 = [\overline{a_1, \dots, a_k}].$$

Therefore, the expansion of $\alpha = \sqrt{D}$ is

$$\sqrt{D} = [a_0, \overline{a_1, \dots, a_k}],$$

that has pre-period 1. □

To conclude this section, we consider the case $\alpha = \sqrt{D}$, with $v_p(\sqrt{D}) \neq 0$. If $v_p(\sqrt{D}) < 0$, then

$$\alpha_1 = \frac{1}{\alpha - a_0}, \quad \overline{\alpha}_1 = \frac{1}{\overline{\alpha} - a_0},$$

so that $v_p(\alpha_1) < 0$ and $v_p(\alpha_1) > 0$. Hence, with a similar argument of Proposition 6.3.3, also in this case we can conclude that $\alpha_1$ is purely periodic and the continued fraction of $\alpha$ has pre-period 1. Notice that, if $v_p(\sqrt{D}) < 0$, then $D$ is not an integer but a rational whose denominator is divided by $p$. Instead,

if $v_p(\sqrt{D}) > 0$, then $a_0 = 0$ and

$$\alpha_1 = \frac{1}{\alpha}, \quad \overline{\alpha}_1 = \frac{1}{\overline{\alpha}}.$$

Since $v_p(\alpha_1) = v_p(\overline{\alpha}_1) < 0$, we are exactly in the previous case, so the expansion of $\alpha$ has pre-period 2 with a 0 as first partial quotient. Hence, we have proved the following result, very similar to (6.2) for classical continued fractions.

**Proposition 6.3.4.** *Let $\sqrt{D} \in \mathbb{Q}_p$, with $D \in \mathbb{Z}$ and $v_p(\sqrt{D}) = e$, having a periodic continued fraction using the Algorithm* (3.10)*. Then the expansion of $\sqrt{D}$ has pre-period*

$$\begin{cases} 1 & \text{if } e \leq 0 \\ 2 & \text{if } e > 0. \end{cases}$$

*Moreover, in the case $e > 0$, its continued fraction expansion is*

$$\sqrt{D} = [0, a_0, \overline{a_1, \ldots, a_h}],$$

*where $a_0, \ldots, a_h$ are the partial quotients of*

$$\frac{\sqrt{D}}{D} = [a_0, \overline{a_1, \ldots, a_h}].$$

# Chapter 7

# Experimental computations

In this section we collect some numerical results about the periodicity of Browkin's algorithms (3.5) and (3.6) and we compare them with Algorithm (3.10). In Section 6.3, and in particular in Theorem 6.3.1 and Proposition 6.3.4, we showed that our Algorithm (3.10) improves the properties of Browkin's algorithm from a theoretical point of view. The content of this section is based on the analysis performed in [55], and it aims to show that our algorithm provides better results also from an experimental point of view. In fact, Algorithm (3.10) appears to become periodic on more quadratic irrationals than *Browkin I* and *Browkin II* for all odd primes less than 100, except $p = 3$ for *Browkin II*. All the computations have been carried out on the first 1000 complete quotients of $\sqrt{D} \in \mathbb{Q}_p$, for all the odd primes $p$ less than 100 and $1 \leq D \leq 1000$, with $D$ not a square and $v_p(D) = 0$. The numerical computations have been performed using SageMath and the code is publicly available [1].

## 7.1 Some *Browkin II* expansions

We start with an observation on the Euclidean norm of odd partial quotients, that allows us to correct some wrong *Browkin II* expansions listed in [16].

**Remark 7.1.1.** *The Euclidean norm of the odd partial quotients in Browkin II can not be greater than* 1. *In fact, we know by Lemma 5.2.2 that* $0 \leq |t(\alpha_k)| < \frac{1}{2}$

[1] https://github.com/giulianoromeont/p-adic-continued-fractions

*for all $k \in \mathbb{N}$. Then, if the sign is not used, $|a_k| = |t(\alpha_k)| < \frac{1}{2}$. If the sign is used, then $|a_k| = 1 - |t(\alpha_k)|$, so $0 < |a_k| < 1$, for $k$ odd.*

Starting from Remark 7.1.1, we can notice that some of the expansions listed in [16] are wrong. In fact, in the 5–adic continued fraction of $\sqrt{34}$, $\sqrt{39}$, $\sqrt{54}$, $\sqrt{69}$ and $\sqrt{99}$, respectively, $a_5 = -\frac{28}{25}$, $a_9 = -\frac{6}{5}$, $a_9 = \frac{28}{25}$, $a_3 = \frac{6}{5}$ and $a_{13} = \frac{32}{25}$, that are all greater than 1 in Euclidean norm. We believe it is an error of implementation where the *sign* function is added instead of being subtracted from $t(\alpha_k)$. Three of them are still periodic and the correct expansions are

$$\sqrt{34} = \left[2, \overline{-\frac{1}{5}, 1, -\frac{2}{5}, -1, \frac{22}{25}, -1, -\frac{2}{5}, 1, -\frac{1}{5}, -1, -\frac{6}{25}, -1}\right],$$

$$\sqrt{54} = \left[2, \frac{2}{25}, -1, \frac{1}{5}, -2, -\frac{1}{5}, \overline{-1, -\frac{2}{5}, 1, \frac{4}{5}}\right],$$

$$\sqrt{69} = \left[2, \overline{-\frac{2}{5}, 1, -\frac{4}{5}, 1, -\frac{1}{5}, -1, -\frac{2}{5}, 2, -\frac{1}{5}, 2, -\frac{12}{25}, 2, -\frac{1}{5}, 2, -\frac{2}{5}, -1, -\frac{1}{5}, 1, -\frac{4}{5}, 1, -\frac{2}{5}, -1, \frac{2}{5}, 1, -\frac{76}{125}, 1, \frac{2}{5}, -1}\right],$$

while for $\sqrt{39}$ and $\sqrt{99}$ we have not observed any period.

## 7.2 Periodic square roots of integers

In this section we collect the results on the periodicity of Algorithm (3.10), compared with *Browkin I* and *Browkin II*.

**Example 7.2.1.** *The behaviour of the periodicity of the three algorithms can be different. In this example we see some of the several possible cases. We consider $p = 5$, but analogous observations hold for other primes. In $\mathbb{Q}_5$, $\sqrt{19}$ has a periodic continued fraction using Algorithm* (3.10)*, with expansion*

$$\sqrt{19} = \left[2, \overline{-\frac{2}{5}, 2, \frac{1}{5}, -2, -\frac{2}{5}, -\frac{12}{5}, \frac{2}{5}, -2, \frac{8}{25}, 2, \frac{1}{5}, -1, -\frac{2}{5}, -\frac{8}{5}, \frac{2}{5}, -2, \frac{12}{25}, 2, \frac{2}{5}, -1}\right],$$

*but no period has been detected with Browkin I nor Browkin II, within* 1000 *partial quotients. On the other hand, using Browkin II,* $\sqrt{69}$ *is periodic (see above) while no period has been observed using the other algorithms. Moreover, for some square roots of integers, Browkin II and Algorithm* (3.10) *are both periodic but they have different expansions. For example, the Browkin II expression of* $\sqrt{129}$ *is*

$$\sqrt{129} = \left[2, \frac{4}{125}, -1, -\frac{4}{5}, 1, \frac{4}{5}, -1, \frac{4}{5}, -1, -\frac{2}{5}, \right.$$
$$\left. 2, -\frac{1}{5}, 2, \frac{2}{5}, 2, -\frac{1}{5}, 2, -\frac{2}{5}, \overline{-1, \frac{4}{5}, -1, -\frac{1}{5}, -2, \frac{3}{5}}\right],$$

*while with Algorithm* (3.10) *it is*

$$\sqrt{129} = \left[2, \overline{\frac{4}{125}, -1, \frac{1}{5}, -\frac{4}{5}, -\frac{1}{5}, -1, -\frac{2}{5}, 2, -\frac{1}{5}, 2,} \right.$$
$$\left. \overline{\frac{2}{5}, 2, -\frac{1}{5}, 2, -\frac{2}{5}, -1, -\frac{1}{5}, -\frac{4}{5}, \frac{1}{5}, -1}\right].$$

*Using Browkin I, we did not detect any period for* $\sqrt{129}$.

In Tables 7.3, 7.4, 7.5 in Section 7.6, we can see that periodic square roots of integers with *Browkin I* are very few compared to *Browkin II* and Algorithm (3.10). Moreover, except for $p = 3$, the number of periodic expansion with Algorithm (3.10) is greater or equal than *Browkin II*. In Figure 7.1 we plot the number of detected periodic square roots of integers for all the three algorithms, varying the prime $p$.

**Remark 7.2.2.** *Browkin II and Algorithm* (3.10) *tend to present a similar behaviour for large primes. This result is expected since the two algorithms are different only in the case when* $a_0 = 0$ *in the* $p$*–adic expansion of one of the odd complete quotients and the probability of having it equal to zero is around* $\frac{1}{p}$*, which approaches zero for growing* $p$.

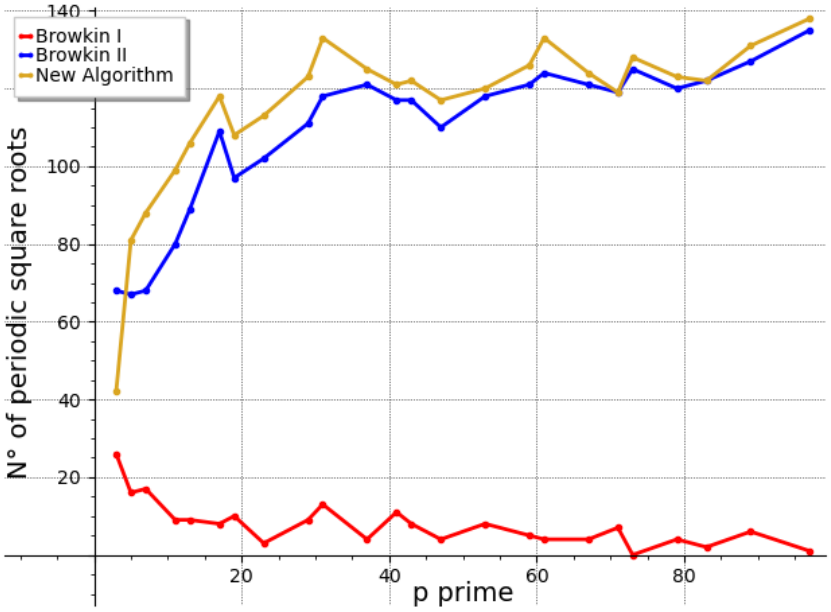


Figure 7.1: Number of detected periodic square roots of integers with *Browkin I*, *Browkin II* and Algorithm (3.10).

## 7.3 Pre-periods of periodic expansions

The length of the pre-period of periodic continued fractions obtained by *Browkin I* is 2 (see [8]) and by Algorithm (3.10) is 1 (see Proposition 6.3.3). On the contrary, for the lengths of the pre-periods of *Browkin II*, Theorem 6.2.17 seems the best we can obtain. In fact, during our analysis, although most of the square roots presented pre-period 1, we also observed pre-periods of several even lengths. In *Browkin II*, pre-periods of even length are an "anomalous" behaviour which occurs when the *sign* function is used in (3.6) (for more details, see [56]). Therefore, in light of Remark 7.2.2, for large values of $p$ we expect to have often pre-period 1. Indeed, for $p \geq 31$, no pre-period greater than 1 has been observed. In Table 7.1, we list the mean pre-periods of periodic *Browkin II* continued fractions up to $p = 29$.

| p | 3 | 5 | 7 | 11 | 13 | 17 | 19 | 23 | 29 |
|---|---|---|---|---|---|---|---|---|---|
| Mean pre-period | 18.85 | 7.49 | 2.96 | 1.45 | 1.39 | 1.17 | 1.08 | 1.13 | 1.01 |

Table 7.1: Mean pre-periods of periodic *Browkin II* expansions.

## 7.4 Periods of periodic expansions

The length of the periods for periodic *Browkin I* continued fractions is very often 2, especially for large values of $p$. In fact, when $p$ increases, periodic *Browkin I* continued fractions are rare and most expansions have both pre-period and period of length 2. Moreover, we can notice that the mean period length for *Browkin II* and Algorithm (3.10) is, in general, decreasing for growing $p$. In Figure 7.2, we plot the mean period of periodic square roots of integers for all the three algorithms, varying the prime $p$.

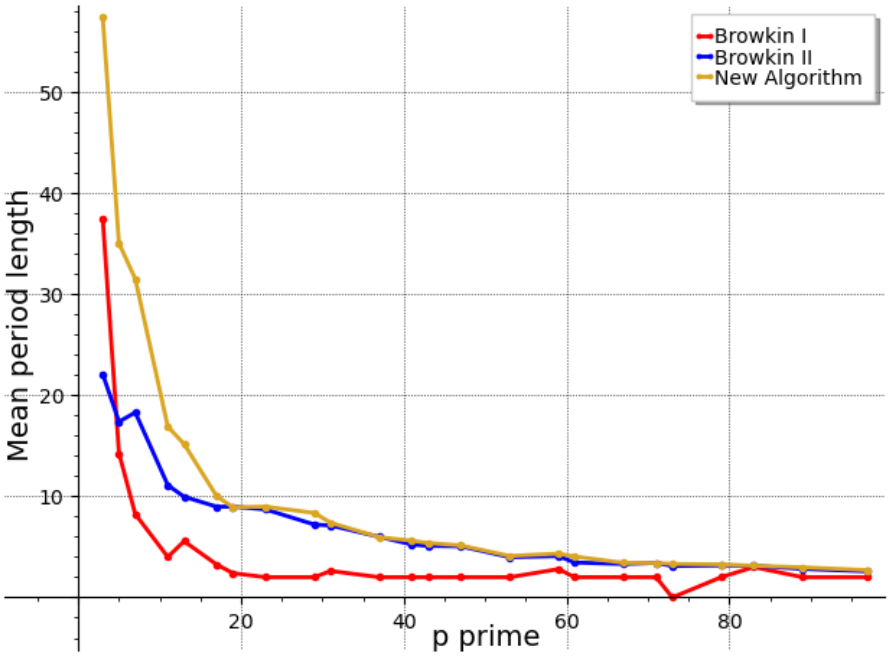


Figure 7.2: Mean periods of periodic square roots with *Browkin I*, *Browkin II* and Algorithm (3.10).

From Tables 7.3, 7.4, 7.5 in Section 7.6, we can observe that, when periodicity is detected, long periods are very uncommon for all values of $p$,

especially for $p$ large. Indeed, for *Browkin II* and Algorithm (3.10) the 90% of the periods are shorter than 30 for all $11 \leq p \leq 97$. In Figure 7.3, we plot the length of the periods for periodic square roots of integers, in function of the size of the integer $D$, for $p = 5$.

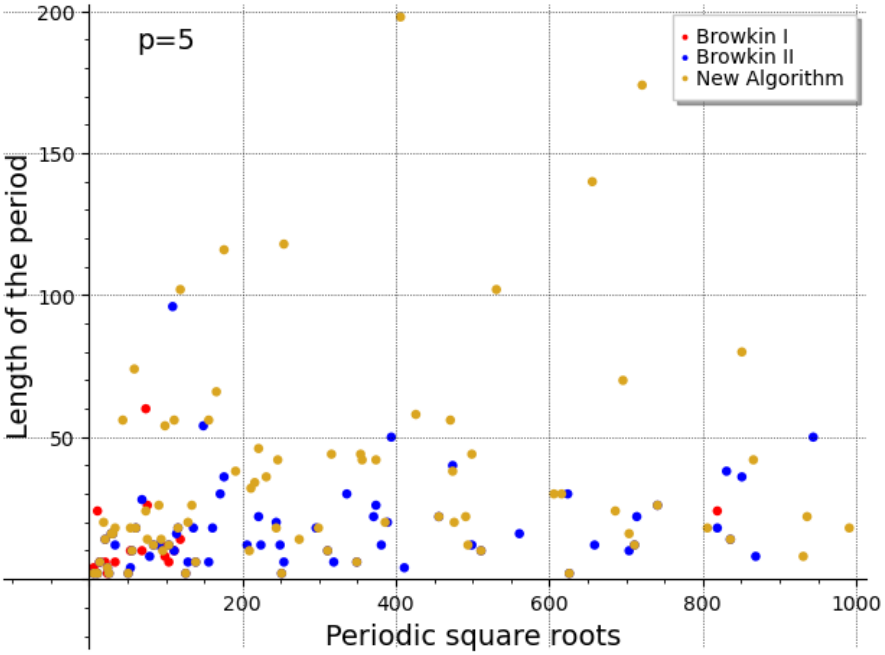


Figure 7.3: Period lengths of periodic square roots with *Browkin I*, *Browkin II* and Algorithm (3.10), for $p = 5$.

**Remark 7.4.1.** *The numerical computations about periodicity give the suggestion that the Lagrange's Theorem does not hold for p–adic continued fractions obtained by the studied algorithms (even if a proof of this statement is still missing). Indeed, for continued fractions over the real numbers, the maximum length of the periods for the square root* $\sqrt{D}$ *for all integers* $1 \leq D \leq 1000$ *is 60. On the contrary, for Browkin I and Algorithm* (3.10) *there are some square roots whose expansion, if periodic, should have a period greater than 998 and 999, respectively, and this seems very unlikely. A similar observation holds also for Browkin II, even if in this case we do not know a-priori the length of the pre-period, making more difficult to deal with the study of the periodicity of this algorithm. However, it seems really unlikely, for instance,*

*that Browkin II produces a periodic expansion for* $\sqrt{19}$ *in* $\mathbb{Q}_5$ *with the sum of the lengths of pre-period and period greater than* 1000.

## 7.5 Quality of approximation

In this section we analyze the approximations of square roots of integers by means of the sequence of convergents of the three algorithms. In general, we can observe that given $\alpha = [a_0, a_1, \ldots]$, we have

$$\alpha = [a_0, a_1, \ldots, a_n, \alpha_{n+1}] = \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}},$$

from which

$$\alpha - \frac{A_n}{B_n} = \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}} - \frac{A_n}{B_n} = \frac{(-1)^n}{(\alpha_{n+1}B_n + B_{n-1})B_n}.$$

Since $v_p(\alpha_{n+1}) = v_p(a_{n+1})$, then $v_p(\alpha_{n+1}B_n + B_{n-1}) = v_p(B_{n+1})$ and therefore

$$v_p\left(\alpha_0 - \frac{A_n}{B_n}\right) = -v_p(B_nB_{n+1}), \tag{7.1}$$

i.e.,

$$\left|\alpha - \frac{A_n}{B_n}\right|_p = p^{v_p(B_nB_{n+1})}, \tag{7.2}$$

that was already obtained in (4.2). We have also observed in Remark 4.1.1 that

$$v_p(B_n) = v_p(a_0) + v_p(a_1) + \ldots + v_p(a_n),$$

for all $n \in \mathbb{N}$. Thus, considering (7.1) and (7.2), the study of the quality of the approximations of $\alpha$ is related to the decreasing of $v_p(B_n)$ and consequently to the values of $v_p(a_n)$. From the definitions of the three algorithms, we know that:

i) $v_p(a_n) < 0$ for all $n \in \mathbb{N}$, for *Browkin I*;

ii) $v_p(a_{2n}) = 0$ and $v_p(a_{2n+1}) < 0$ for all $n \in \mathbb{N}$, for *Browkin II*;

iii) $v_p(a_{2n}) \leq 0$ and $v_p(a_{2n+1}) < 0$ for all $n \in \mathbb{N}$, for Algorithm (3.10).

Therefore, we expect the approximations given by the convergents of continued fractions obtained by *Browkin I* to be better than those obtained by Algorithm (3.10), which should be better than *Browkin II*. In Table 7.2 we list, for some values of $p$, the mean valuation after 10, 100 and 1000 steps by means of *Browkin I*, *Browkin II* and Algorithm (3.10).

| p=5 | 10 steps | 100 steps | 1000 steps |
|---|---|---|---|
| *Browkin I* | -11.1 | -123.1 | -1246.4 |
| *Browkin II* | -6.1 | -62.8 | -629.8 |
| Algorithm (3.10) | -7.0 | -73.6 | -744.3 |

| p=23 | 10 steps | 100 steps | 1000 steps |
|---|---|---|---|
| *Browkin I* | -9.4 | -103.4 | -1043.8 |
| *Browkin II* | -5.2 | -52.6 | -525.8 |
| Algorithm (3.10) | -5.4 | -54.7 | -547.8 |

| p=47 | 10 steps | 100 steps | 1000 steps |
|---|---|---|---|
| *Browkin I* | -9.2 | -101.2 | -1021.6 |
| *Browkin II* | -5.0 | -50.9 | -508.9 |
| Algorithm (3.10) | -5.1 | -52.0 | -520.5 |

| p=89 | 10 steps | 100 steps | 1000 steps |
|---|---|---|---|
| *Browkin I* | -9.1 | -100.1 | -1010.3 |
| *Browkin II* | -5.0 | -50.5 | -504.3 |
| Algorithm (3.10) | -5.1 | -50.9 | -509.2 |

Table 7.2: Values of $v_p(B_n)$ with *Browkin I*, *Browkin II* and Algorithm (3.10) after 10, 100 and 1000 steps for $p = 5, 23, 47, 89$.

The experimental results listed in the previous tables are in line with the considerations on the valuation of the partial quotients of the three algorithms. In fact, *Browkin I* decreases the valuation of $B_n$ at each step, *Browkin II* at half of the steps and Algorithm (3.10) on slightly more than half of the steps. Let us compare the quality of this approximation, given by the convergents

of a continued fraction, with the classical rational approximation given by the $p$–adic expansion of $\alpha$ stopped at the $n$-th digit. For $\alpha = \sum_{i=0}^{+\infty} a_i p^i \in \mathbb{Q}_p$, the sequence $\{C_n\}_{n\in\mathbb{N}}$, with $C_n = a_0 + a_1 p + \ldots + a_n p^n$, approximates $\alpha$ with error

$$|\alpha - C_n|_p = |a_{n+1}p^{n+1} + \ldots|_p \leq \frac{1}{p^{n+1}}.$$

Therefore $C_n$ usually provides a better approximation than *Browkin II* and Algorithm (3.10) but worse than *Browkin I*.

## 7.6 Tables

In the following tables we collect the computational results about the periodicity properties of Algorithms (3.5),(3.6) and (3.10). All the computations have been performed on the first 1000 complete quotients of $\sqrt{D} \in \mathbb{Q}_p$, for all the odd primes $p$ less than 100 and $1 \leq D \leq 1000$, with $D$ not a square and $v_p(D) = 0$. The numerical simulations have been performed in SageMath and the code is publicly available[2]. The tables collect results about:

- the number of square roots which are periodic within 1000 steps,
- the mean length of the period,
- the value $h$ such that 75% of the lengths of the periods detected are less or equal $h$,
- the value $h$ such that 90% of the lengths of the periods detected are less or equal $h$,
- the total number of positive integers $D$ less than 1000 such that $\sqrt{D} \in \mathbb{Q}_p$, $D$ is not a square and $v_p(D) = 0$.

[2] https://github.com/giulianoromeont/p-adic-continued-fractions

| p | Periodic | Mean period | 75% | 90% | Total |
|---|---|---|---|---|---|
| 3 | 26 | 37.46 | 52 | 88 | 313 |
| 5 | 16 | 14.25 | 14 | 24 | 375 |
| 7 | 17 | 8.24 | 8 | 16 | 402 |
| 11 | 9 | 4 | 4 | 6 | 426 |
| 13 | 9 | 5.56 | 6 | 6 | 433 |
| 17 | 8 | 3.25 | 4 | 4 | 440 |
| 19 | 10 | 2.4 | 2 | 2 | 445 |
| 23 | 3 | 2 | 2 | 2 | 450 |
| 29 | 9 | 2 | 2 | 2 | 453 |
| 31 | 13 | 2.62 | 2 | 2 | 456 |
| 37 | 4 | 2 | 2 | 2 | 456 |
| 41 | 11 | 2 | 2 | 2 | 457 |
| 43 | 8 | 2 | 2 | 2 | 458 |
| 47 | 4 | 2 | 2 | 2 | 461 |
| 53 | 8 | 2 | 2 | 2 | 460 |
| 59 | 5 | 2.8 | 2 | 2 | 461 |
| 61 | 4 | 2 | 2 | 2 | 462 |
| 67 | 4 | 2 | 2 | 2 | 462 |
| 71 | 7 | 2 | 2 | 2 | 465 |
| 73 | 0 | none | none | none | 462 |
| 79 | 4 | 2 | 2 | 2 | 468 |
| 83 | 2 | 3 | 2 | 2 | 464 |
| 89 | 6 | 2 | 2 | 2 | 466 |
| 97 | 1 | 2 | 2 | 2 | 464 |

Table 7.3: *Browkin I*

| p | Periodic | Mean period | 75% | 90% | Total |
|---|---|---|---|---|---|
| 3 | 68 | 22.09 | 26 | 42 | 313 |
| 5 | 67 | 17.37 | 22 | 36 | 375 |
| 7 | 68 | 18.29 | 22 | 42 | 402 |
| 11 | 80 | 11.10 | 16 | 22 | 426 |
| 13 | 89 | 9.96 | 10 | 18 | 433 |
| 17 | 109 | 8.97 | 10 | 20 | 440 |
| 19 | 97 | 8.97 | 10 | 14 | 445 |
| 23 | 102 | 8.70 | 10 | 20 | 450 |
| 29 | 111 | 7.21 | 8 | 14 | 453 |
| 31 | 118 | 7.12 | 8 | 14 | 456 |
| 37 | 121 | 5.98 | 6 | 12 | 456 |
| 41 | 117 | 5.23 | 6 | 10 | 457 |
| 43 | 117 | 5.09 | 6 | 10 | 458 |
| 47 | 110 | 5.05 | 6 | 10 | 461 |
| 53 | 118 | 3.98 | 6 | 8 | 460 |
| 59 | 121 | 4.08 | 6 | 6 | 461 |
| 61 | 124 | 3.45 | 4 | 6 | 462 |
| 67 | 121 | 3.30 | 4 | 6 | 462 |
| 71 | 119 | 3.41 | 4 | 6 | 465 |
| 73 | 125 | 3.10 | 4 | 6 | 462 |
| 79 | 120 | 3.17 | 2 | 6 | 468 |
| 83 | 122 | 3.13 | 2 | 6 | 464 |
| 89 | 127 | 2.82 | 2 | 6 | 466 |
| 97 | 135 | 2.58 | 2 | 4 | 464 |

Table 7.4: *Browkin II*

| p | Periodic | Mean period | 75% | 90% | Total |
|---|---|---|---|---|---|
| 3 | 42 | 57.38 | 72 | 112 | 313 |
| 5 | 81 | 35.01 | 42 | 70 | 375 |
| 7 | 88 | 31.50 | 38 | 80 | 402 |
| 11 | 99 | 16.89 | 22 | 30 | 426 |
| 13 | 106 | 15.17 | 18 | 30 | 433 |
| 17 | 118 | 10.02 | 14 | 22 | 440 |
| 19 | 108 | 8.91 | 10 | 18 | 445 |
| 23 | 113 | 8.97 | 10 | 22 | 450 |
| 29 | 123 | 8.36 | 10 | 18 | 453 |
| 31 | 133 | 7.38 | 8 | 14 | 456 |
| 37 | 125 | 5.95 | 6 | 12 | 456 |
| 41 | 121 | 5.60 | 6 | 10 | 457 |
| 43 | 122 | 5.38 | 6 | 10 | 458 |
| 47 | 117 | 5.15 | 6 | 10 | 461 |
| 53 | 120 | 4.10 | 6 | 8 | 460 |
| 59 | 126 | 4.33 | 6 | 10 | 461 |
| 61 | 133 | 4.05 | 6 | 8 | 462 |
| 67 | 124 | 3.42 | 4 | 6 | 462 |
| 71 | 119 | 3.41 | 4 | 6 | 465 |
| 73 | 128 | 3.31 | 4 | 6 | 462 |
| 79 | 123 | 3.27 | 2 | 6 | 468 |
| 83 | 122 | 3.13 | 2 | 6 | 464 |
| 89 | 131 | 2.98 | 2 | 6 | 466 |
| 97 | 138 | 2.70 | 2 | 6 | 464 |

Table 7.5: Algorithm (3.10)

# Chapter 8

# Conclusions and open problems

In this last chapter I briefly survey the main still open problems for $p$–adic continued fractions that I have tackled in my research. I would like to informally summarize some of the main paths we have tried to follow, hoping to provide some useful hints to those who want to face these (or similar) problems. This section can be read also independently of the rest of the thesis, from those who have some familiarity with the theory of continued fractions in $\mathbb{Q}_p$. Some of the reasonings and computations in this section have been recently included in [66]. In general, we mainly moved in two directions: the first is the proof of the periodicity properties of already existent $p$–adic continued fractions, and the second is the research of several further modifications of the known algorithms in order to get somewhere "nearer" Lagrange's Theorem.

As we have largely discussed in the previous chapters, Browkin's papers [15, 16] introduced two algorithms, *Browkin I* and *Browkin II*, having the really nice property of providing a finite continued fraction for every rational numbers. This result is accomplished by allowing negative partial quotients, and choosing the representatives modulo $p$ in $\left\{-\frac{p-1}{2},\dots,\frac{p-1}{2}\right\}$ instead of $\{0,\dots,p-1\}$. This is a painful trade-off, since continued fractions with negative partial quotients behave in a really different way, also in $\mathbb{R}$, and several proofs can not be adapted. For example, I have given several thoughts to the real convergence of $p$–adic continued fractions.

## 8.1 Real convergence of $p$–adic continued fractions

The problem in full generality could be stated as: when does a continued fraction $[a_0, a_1, \ldots]$ converge both in the $p$–adic and in the real topology? Not always, of course. For example, the well known continued fraction

$$[\overline{1}] = \frac{1+\sqrt{5}}{2}, \tag{8.1}$$

converges in $\mathbb{R}$ to the golden mean, but does not converge in $\mathbb{Q}_p$, for the reasons explained in Chapter 4. Moreover, also a continued fraction $[a_0, a_1, \ldots]$ with rational partial quotients that converges in $\mathbb{Q}_p$ not necessarily converges in $\mathbb{R}$ (not even in $\mathbb{C}$). For example

$$\left[\frac{1}{p}, \frac{1}{p^2}, \frac{1}{p^3}, \cdots\right]$$

converges to a $p$–adic number since $v_p(a_n) < 0$ for all $n$, but the series

$$\sum_{n=0}^{\infty} a_n = \sum_{n=0}^{\infty} \frac{1}{p^{n+1}} = \frac{1}{1-p},$$

converges in Euclidean absolute value. Therefore, for a known result of convergence, the continued fraction $[a_0, a_1, \ldots]$ diverges to $+\infty$ in the Euclidean setting (see, for example, the chapter dedicated to convergence in Wall's book [75], in particular Theorem 6.1).

Convergence is usually easier for periodic continued fractions. However, as we have seen in (8.1), periodic continued fractions that converge in $\mathbb{R}$ not necessarily converge in $\mathbb{Q}_p$. Also periodic $p$–adic continued fractions can be not convergent with respect to the Euclidean absolute value. For example, if we consider $[\overline{\frac{2}{5}, -\frac{2}{5}}]$, then

$$\alpha = \frac{\alpha_2 A_1 + A_0}{\alpha_2 B_1 + B_0} = \frac{\frac{21}{25}\alpha + \frac{2}{5}}{-\frac{2}{5}\alpha + 1}. \tag{8.2}$$

This means that $\alpha$ is a root of $5x^2 - 2x + 5 = 0$, that has negative discriminant $\Delta = -96$. So, if it converged, it should converge to a non-real complex number, which is clearly not possible, as the convergents are all rationals and $\mathbb{R}$ is a complete field.

In the following, we delve into the case of our interest, that is when the continued fractions are obtained starting from an element $\alpha$. In order to properly speak about real and $p$–adic convergence to $\alpha$ of a continued fraction, $\alpha$ must be embedded in both the reals and the $p$–adics. Therefore we introduce some context and notation for the interesting cases of our study, the quadratic irrationals. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible quadratic polynomial with rational coefficients and let us suppose that $f$ splits both in $\mathbb{R}$ and in $\mathbb{Q}_p$. We call $\alpha$ and $\overline{\alpha}$ its roots in $\mathbb{R}$ and we call $\alpha^{(p)}$ and $\overline{\alpha}^{(p)}$ its roots in $\mathbb{Q}_p$. Capuano, Veneziano and Zannier [22] proved the following result for Ruban's continued fraction.

**Theorem 8.1.1** ([22]). *The Ruban's continued fraction of a quadratic irrational always converges in* $\mathbb{R}$.

Ruban's continued fractions, as we discussed in Chapter 6, are not always periodic for quadratic irrationals. The periodic expansion of a $p$–adic quadratic irrational $\alpha^{(p)}$ can be easily showed to converge in $\mathbb{R}$ to $\alpha$. However, when Ruban's continued fraction of $\alpha^{(p)}$ is non-periodic, we know that it converges in $\mathbb{R}$, but we do not know to which real number it converges. The authors of [22], left the following, probably hard but probably true, conjecture.

**Conjecture 8.1.2** ([22]). *Ruban's continued fraction of a quadratic irrational is either periodic or it converges in* $\mathbb{R}$ *to a transcendental number.*

This conjecture is quite reasonable, since algebraic numbers are countable and hence have measure 0 in $\mathbb{R}$. Therefore, we expect a continued fraction having an "unknown" limit to converge to a transcendental number.

For Browkin's continued fractions, we have experimentally observed similar results. In the following we speak of either *Browkin I* or *Browkin II* or our Algorithm (3.10), since they show similar behaviours of real convergence.

Periodic continued fractions of quadratic irrationals that have embeddings both in $\mathbb{R}$ and in $\mathbb{Q}_p$, clearly converge simultaneously in $\mathbb{R}$ and in $\mathbb{Q}_p$ to roots of the same minimal polynomial, respectively $\alpha$ and $\alpha^{(p)}$. Also Browkin's expansions of quadratic irrationals for which we did not observed any periodicity seem to converge to some real number. Therefore we leave the following conjecture, that is the analogue of Theorem 8.1.1 for Browkin's continued fractions.

**Conjecture 8.1.3.** *The Browkin's continued fraction of a quadratic irrational always converges in* $\mathbb{R}$.

Again, the problem in generalizing the proof of Theorem 8.1.1 is the presence of negative partial quotients. In fact, the fundamental hypothesis of the theorem of convergence used in [22] is that the partial quotients are positive.

However, let us assume Conjecture 8.1.3 to be true and let us go on. Browkin's continued fractions seem to converge, both in the periodic and non-periodic cases, to some real number. However, in the non-periodic cases, they seem to converge very neetly "somewhere else" in $\mathbb{R}$. In fact, for those $p$–adic quadratic irrationals $\alpha^{(p)}$ that we believe to be non-periodic (based on brute-force search of the periodicity for a large number of steps), the continued fraction is approaching really well a real number that is completely different from $\alpha$. Since converging to $\alpha$ is a necessary condition for the periodicity of the $p$–adic continued fraction of $\alpha^{(p)}$, proving the convergence to another real number would be an example of a non-periodic Browkin's continued fraction. However, we were not able to exhibit such an example. Even if the continued fractions that are apparently non-periodic seem to converge really well to another real number, it remains a (very convincing, but heuristic) computational observation.

Also, we did not observe any continued fraction of $\alpha^{(p)}$ that seems to converge in $\mathbb{R}$ to $\alpha$ and does not become periodic. If it does not show a period, the continued fraction seems really far from $\alpha$ in Euclidean absolute value. Therefore we leave the following conjecture, that I consider so far the

main and most important conjecture for the periodicity of $p$–adic continued fraction.

**Conjecture 8.1.4.** *Let* $[a_0, a_1, \ldots]$ *be the Browkin I, Browkin II or Algorithm* (3.10) *expansion of a* $p$*–adic quadratic irrational* $\alpha^{(p)}$ *that can be embedded in the real numbers. Let us call* $\alpha$ *the image of* $\alpha^{(p)}$ *in* $\mathbb{R}$*. Then,* $[a_0, a_1, \ldots]$ *is eventually periodic if and only if* $[a_0, a_1, \ldots]$ *converges to* $\alpha$ *with respect to the Euclidean absolute value.*

As we discussed, one implication is true. In fact, by the periodicity, $\alpha$ and $\alpha^{(p)}$ are roots, respectively over $\mathbb{R}$ and over $\mathbb{Q}_p$ of the same polynomial of degree 2. Therefore, $[a_0, a_1, \ldots]$ converges to $\alpha^{(p)}$ in $\mathbb{Q}_p$ by the correctness of the algorithms. Moreover, it converges to $\alpha$ in $\mathbb{R}$ by a known theorem of convergence for periodic continued fractions (see, for example, Theorem 8.1 in [75]). This can be not true, of course, if the quadratic irrational $\alpha^{(p)}$ has no real embedding, as it happens in Equation (8.2) where the quadratic polynomial has negative discriminant and hence $\alpha^{(p)}$ is embedded in $\mathbb{C}\backslash\mathbb{R}$.

Therefore, the difficult part of Conjecture 8.1.4 is to prove that if the $p$–adic continued fraction of the quadratic irrational $\alpha^{(p)}$ converges in $\mathbb{R}$ to $\alpha$, then it becomes periodic at some point. I believe this is not an easy problem, but I would expect someone to solve it at some point. This problem can be stated in harder or easier ways, for which I leave the following three conjectures, in order of difficulty. The main underlying question is: does the convergence to a real quadratic irrational provide a sufficient condition for the periodicity? If the partial quotients are positive integers, the answer is yes, by Lagrange's Theorem.

The first conjecture has nothing to deal with $p$–adic continued fractions, but it would easily imply Conjecture 8.1.4.

**Conjecture 8.1.5.** *Let* $[a_0, a_1, \ldots]$*, where* $a_n \in \mathbb{Q}$ *for all* $n$*. If* $[a_0, a_1, \ldots]$ *converge to a real quadratic irrational, then the continued fraction is periodic.*

**Conjecture 8.1.6.** *Let* $[a_0, a_1, \ldots]$*, where* $a_n \in \mathbb{Q}$ *for all* $n$*. If* $[a_0, a_1, \ldots]$ *converge simultaneously in* $\mathbb{R}$ *and* $\mathbb{Q}_p$*, respectively to a real quadratic irrational*

*$\alpha$ and its image $\alpha^{(p)}$ inside $\mathbb{Q}_p$, then the continued fraction $[a_0, a_1, \ldots]$ is periodic.*

**Conjecture 8.1.7.** *Let $[a_0, a_1, \ldots]$ the $p$–adic continued fraction, obtained with either Browkin I, Browkin II or Algorithm* (3.10)*, of a quadratic irrational $\alpha^{(p)}$ that has an image $\alpha$ inside $\mathbb{R}$. If $[a_0, a_1, \ldots]$ converge to $\alpha$ in $\mathbb{R}$, then the continued fraction is periodic.*

Conjecture 8.1.5 implies Conjecture 8.1.6, that implies Conjecture 8.1.7, as we are giving more restrictive hypotheses. I honestly would not be surprised if Conjecture 8.1.5 was false in general. I think that Conjecture 8.1.6 is true and I strongly believe that Conjecture 8.1.7 holds. In Conjecture 8.1.7 we have a more precise shape of the rational numbers of the continued fractions, because they are "legal" partial quotients of *Browkin I*, *Browkin II* or Algorithm (3.10). I think that giving an answer to Conjecture 8.1.5 would be hard even if we restrict to positive rationals.

**Example 8.1.8.** *Let us consider $\sqrt{19}$ in $\mathbb{Q}_5$. The polynomial $x^2 - 19$ has a root, and hence two roots, in $\mathbb{Q}_5$. In fact, $19 \equiv 4 \mod 5$ is a square modulo 5, that by Hensel's Lemma is a necessary and sufficient condition for $\sqrt{19}$ to be defined in $\mathbb{Q}_p$. This is the first and simplest example of $\sqrt{D}$, with $D > 0$ non-square integer that is a quadratic residue modulo $p$, such that Browkin I and Browkin II continued fractions seem to be non-periodic. The expansions of $\sqrt{14}$ and $\sqrt{21}$, that are the quadratic residues modulo 5 nearest to $\sqrt{19}$, have expansions*

$$\sqrt{14} = \left[2, -\frac{3}{5}, \overline{-\frac{9}{5}, -\frac{6}{5}, \frac{166}{125}, -\frac{6}{5}, -\frac{9}{5}, -\frac{8}{5}}\right],$$
$$\sqrt{21} = \left[1, \frac{3}{5}, \overline{\frac{3}{5}, -\frac{4}{5}, \frac{3}{5}, -\frac{7}{5}, \frac{26}{25}, -\frac{7}{5}}\right],$$

*with Browkin I and*

$$\sqrt{14} = \left[2, \overline{\frac{2}{5}, -1, -\frac{1}{5}, 2, -\frac{1}{5}, -1}\right],$$
$$\sqrt{21} = \left[1, \overline{-\frac{2}{5}, 1, \frac{2}{5}, 2, \frac{1}{5}, -2, \frac{2}{5}, -2, \frac{1}{5}, 2, \frac{2}{5}, 1, -\frac{2}{5}, 2}\right],$$

*with Browkin II.*

*For the examples listed before, we did not find any period with a search up to* $50.000$ *complete quotients. It seems really unlikely to have periodicity of small square roots for small primes* $p$ *with such a long period. In fact, "small" square roots tend to have short periods whenever they are periodic, as it happens for real continued fractions and as we can see for* $\sqrt{14}$ *and* $\sqrt{21}$ *in the previous example.*

*This observation already suggests that is really unlikely for* $\sqrt{19}$ *to have a periodic continued fraction with Browkin I and Browkin II. Also, if we look at the convergents, we can notice the following. For the Browkin I expansion of* $\sqrt{19}$*,*

$$\frac{A_{10}}{B_{10}} = 1.35736553571026\ldots$$
$$\frac{A_{100}}{B_{100}} = 1.35738766711068\ldots$$
$$\frac{A_{1000}}{B_{1000}} = 1.35738766711068\ldots$$
$$\frac{A_{5000}}{B_{5000}} = 1.35738766711068\ldots$$
$$\frac{A_{10000}}{B_{10000}} = 1.35738766711068\ldots$$

*and this approximation just gets better going forward with the expansion. It seems that the Browkin I continued fraction of* $\sqrt{19}$ *is converging to a real number which is, however, different from* $\sqrt{19} \approx 4.36$*. Proving that this expansion is not actually convergent to something near* $4.36$ *would be a counterexample for the periodicity of Browkin I. However, we did not manage*

*to prove it for* $\sqrt{19}$ *or for any other quadratic irrational. Similar results are true for Browkin II, where the convergents of* $\sqrt{19}$ *are*

$$\begin{aligned}
\frac{A_{10}}{B_{10}} &= 2.57225268855495\ldots,\\
\frac{A_{100}}{B_{100}} &= 1.89462102495469\ldots,\\
\frac{A_{1000}}{B_{1000}} &= 1.89443989021177\ldots,\\
\frac{A_{5000}}{B_{5000}} &= 1.89443989021177\ldots,\\
\frac{A_{10000}}{B_{10000}} &= 1.89443989021177\ldots.
\end{aligned}$$

*Also the Browkin II convergents of* $\sqrt{19}$ *seem clearly converging to some real number. This real number, also in this case, is different from* $\sqrt{19} \approx 4.36$*. With our algorithm* (3.10)*,* $\sqrt{19}$ *has periodic expansion*

$$\sqrt{19} = \left[2, \overline{-\frac{2}{5}, 2, \frac{1}{5}, -2, -\frac{2}{5}, -\frac{12}{5}, \frac{2}{5}, -2, \frac{8}{25}, 2, \frac{1}{5}, -1, -\frac{2}{5}, -\frac{8}{5}, \frac{2}{5}, -2, \frac{12}{25}, 2, \frac{2}{5}, -1}\right].$$

*For* $\sqrt{39}$ *we did not observed any period up to* $50.000$ *steps. As for Browkin's algorithms, the convergents seem to approach very neetly some real numbers. In fact,*

$$\begin{aligned}
\frac{A_{10}}{B_{10}} &= 3.11589405199643\ldots,\\
\frac{A_{100}}{B_{100}} &= 3.24461192422490\ldots,\\
\frac{A_{1000}}{B_{1000}} &= 3.23880830293096\ldots,\\
\frac{A_{5000}}{B_{5000}} &= 3.23880830293096\ldots,\\
\frac{A_{10000}}{B_{10000}} &= 3.23880830293096\ldots,
\end{aligned}$$

*that is far from* $\sqrt{39} \approx 6.24$*, to which they should converge if the continued fraction became periodic.*

It seems really likely, in Example 8.1.8, that the convergents of $\sqrt{19}$ and $\sqrt{39}$ are converging to something else rather than to $\sqrt{19}$ and $\sqrt{39}$. We can notice it also by looking at the difference between two consecutive partial quotients

$$\left|\frac{A_{n+1}}{B_{n+1}} - \frac{A_n}{B_n}\right| = \frac{1}{|B_n||B_{n+1}|}. \tag{8.3}$$

The denominators of the convergents are generated as in (2.2), therefore

$$B_{n+1} = a_{n+1}B_n + B_{n-1}.$$

Here, when the partial quotients are all positive, we clearly have $B_{n+1} > B_{n-1}$, hence it eventually increases, possibly in different ways, at both odd and even steps. This means that the distance between two consecutive convergents tends to zero in $\mathbb{R}$ as $n$ increases. Therefore by Equation (8.3), we expect $\frac{A_n}{B_n}$ to not "move too much", especially for large values of $n$.

For the continued fractions provided Browkin's algorithms and Algorithm (3.10), the denominators $B_n$ are not always increasing. In fact, since the partial quotients are allowed to be negative, this can lead to cancellations and the sequence $B_n$ can be decreasing in absolute value at some step. However, this is really rare and usually does not happens. In fact, as it is true that partial quotients can get really small and negative and mix up in order to make $B_n$ small in absolute value, it does not actually happens.

In order to have a small partial quotient, for example equal to $\frac{1}{p^5}$ in *Browkin I* at some step $n$, we should have

$$v_p(\alpha_{n-1} - a_{n-1}) = v_p(a_1 p + a_2 p^2 + \ldots) = 5.$$

It means that $a_1 = a_2 = a_3 = a_4 = 0$, where $a_1, a_2, a_3, a_4 \in \left\{-\frac{p-1}{2}, \ldots, -\frac{p-1}{2}\right\}$ are representatives modulo $p$. However, it is widely believed that the $p$–adic digits of irrationalities are uniformly distributed in $\{0, \ldots, p-1\}$, and hence in $\left\{-\frac{p-1}{2}, \ldots, -\frac{p-1}{2}\right\}$. Therefore, the probability of having 4 consecutive 0's

is $\frac{1}{p^4}$. The dominating term of $B_n$ is $a_1 \cdot a_2 \cdot \ldots \cdot a_n$. Therefore, when $|a_i| > 1$, we expect to have an exponential growth of the $B_n$. And, especially for big values of $p$, it is very rare to have $|a_i| < 1$. In particular, notice that if in the $p$–adic expansion of

$$a_i = c_{-r}\frac{1}{p^r} + \ldots + c_{-1}\frac{1}{p} + c_0,$$

$|c_0| \geq 2$, then $|a_i| > 1$.

This observation led me to carry out a probabilistic argument. In the following section, we make the assumption of uniform distribution of the digits in the $p$–adic expansion of a quadratic irrational and we prove that the size of partial quotients really tends to be big, and it increases with $p$.

## 8.2 The probabilistic approach for convergence

**Assumption 8.2.1.** *Let $\alpha = \sum_{n=r}^{+\infty} c_n$ be a $p$–adic quadratic irrational. Then, for all $n \geq r$ and for all $k \in \{0, \ldots, p-1\}$,*

$$\mathbb{P}(c_n = k) = \frac{1}{p}.$$

*In other words, the coefficients of the $p$–adic expansion of $\alpha$ are uniformly distributed in the finite set $\{0, \ldots, p-1\}$.*

**Remark 8.2.2.** *By the assumption, it is implied also the uniform distribution of the coefficients of the partial quotients in both Browkin's and Ruban's continued fractions.*

First we compute the probability for a complete quotient to have a given $p$–adic valuation.

**Proposition 8.2.3.** *Let $k \geq 1$ be an integer For all $n$,*

$$\mathbb{P}(v_p(\alpha_n) = -k) = \frac{p-1}{p^k}.$$

*Proof.* The valuation of $\alpha_n$ is $-k$ if and only if

$$\alpha_{n-1} - a_{n-1} = a_k p^k + \dots.$$

This is equivalent to ask that $a_1 = a_2 = \ldots = a_{k-1} = 0$, that happens with probability

$$\mathbb{P}(a_1 = a_2 = \ldots = a_{k-1} = 0) = \frac{1}{p^{k-1}},$$

and $a_k \neq 0$, that happens with probability

$$\mathbb{P}(a_k \neq 0) = \frac{p-1}{p},$$

and this proves the claim □

**Remark 8.2.4.** *Notice that, in fact*

$$\sum_{k=1}^{+\infty} \frac{p-1}{p^k} = (p-1)\left(\sum_{k=1}^{+\infty} \frac{1}{p^k}\right) = (p-1)\left(\sum_{k=0}^{+\infty} \frac{1}{p^k}\right) - (p-1) =$$
$$= (p-1)\left(\frac{1}{1-\frac{1}{p}}\right) - (p-1) = p - (p-1) = 1,$$

*so that it defines a distribution on the natural numbers.*

In the next Proposition, we compute the expected value of the valuation of a complete quotient.

**Proposition 8.2.5.** *For all $n$,*

$$\mathbb{E}(v_p(\alpha_n)) = \frac{p}{p-1}.$$

*Proof.* Let us notice that

$$\mathbb{E}(v_p(\alpha_n)) = \sum_{k=1}^{+\infty} k \frac{p-1}{p^k},$$

is a convergent series since

$$\lim_{k\to+\infty}\frac{(k+1)\frac{p-1}{p^{k+1}}}{k\frac{p-1}{p^k}}=\lim_{k\to+\infty}\frac{k+1}{kp}=\frac{1}{p}<1.$$

Then we compute

$$\begin{aligned}\mathbb{E}(v_p(\alpha_n))&=\sum_{k=1}^{+\infty}k\frac{p-1}{p^k}=(p-1)\sum_{k=1}^{+\infty}\frac{k}{p^k}+(p-1)\sum_{k=1}^{+\infty}\frac{1}{p^k}-(p-1)\sum_{k=1}^{+\infty}\frac{1}{p^k}=\\&=(p-1)\sum_{k=1}^{+\infty}\frac{k-1}{p^k}+(p-1)\sum_{k=1}^{+\infty}\frac{1}{p^k}=\\&=(p-1)\sum_{k=0}^{+\infty}\frac{k}{p^{k+1}}+(p-1)\left(\frac{1}{1-\frac{1}{p}}-1\right)=\\&=\frac{1}{p}\sum_{k=0}^{+\infty}k\frac{p-1}{p^k}+1=\frac{1}{p}\sum_{k=1}^{+\infty}k\frac{p-1}{p^k}+1.\end{aligned}$$

It means that, for $\mathbb{E}=\mathbb{E}(v_p(\alpha_n))$,

$$\mathbb{E}=\frac{1}{p}\mathbb{E}+1,$$

that is,

$$\mathbb{E}=\mathbb{E}(v_p(\alpha_n))=\frac{p}{p-1}.$$

□

**Remark 8.2.6.** *Proposition 8.2.5 tells us that, especially for large prime $p$, having large negative valuation is extremely rare. This is what we expect, since large valuations are caused by several consecutive $0's$, and under the uniformity assumption each zero appears with probability $\frac{1}{p}$.*

Notice that the expected value of any partial quotient in *Browkin I* is $\mathbb{E}(a_n)=0$ for all $n\in\mathbb{N}$. This is due to the choice of the symmetric interval $\{-\frac{p-1}{2},\dots,\frac{p-1}{2}\}$. Therefore, to have an estimate of the size of the partial quotient, we compute it for its Euclidean absolute value.

**Proposition 8.2.7.** *Let $a$ be a Browkin I partial quotient and let $k \geq 1$. Then, the expected value of its absolute value is*

$$\mathbb{E}(|a| \mid v_p(a) = -k) = \frac{p^{2(k+1)} - 1}{4p^{2k+1}},$$

*and, in general,*

$$\mathbb{E}(|a|) = \frac{p}{4}\left(1 - \frac{1}{p^2+p+1}\right)$$

*Proof.* The expected value of the constant term $c_0$ is 0, but in absolute value it is

$$\begin{aligned}\mathbb{E}(|c_0|) &= \frac{1}{p}(0+2+\ldots+p-1) = \frac{2}{p}(1+\ldots+\frac{p-1}{2}) = \\ &= \frac{2}{p}\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)\frac{1}{2} = \frac{p^2-1}{4p}\end{aligned}$$

The expected value of $|c_0 + c_1\frac{1}{p}|$ is composed by the case where $c_0 = 0$, i.e.

$$\frac{2}{p}\left(1+\ldots+\frac{p-1}{2}\right),$$

and the cases where $c_0 \neq 0$. When $c_0 \neq 0$, the positive elements $c_0 + c_1\frac{1}{p}$ are exactly the ones with positive $c_0 \in \left\{0, \ldots, \frac{p-1}{2}\right\}$. For $c_0 \neq 0$, all the elements $c_0 + c_1 p$ and $c_0 - c_1 p$ cancel out, and all of them are counted twice (the positive and the negative one). Therefore, for all choices of $c_0 \neq 0$ we have a summand of the kind $2pc_0$, since the tails with $c_1$ eliminate and there are exactly $p$ summands. Now we can compute

$$\begin{aligned}\mathbb{E}\left(\left|c_0 + \frac{c_1}{p}\right|\right) &= \frac{1}{p^2}\left(\frac{2}{p}\left(1+\ldots+\frac{p-1}{2}\right) + 2p\left(1+\ldots+\frac{p-1}{2}\right)\right) = \\ &= \frac{1}{p^2}\cdot\frac{p-1}{2}\cdot\frac{p+1}{2}\cdot\frac{1}{2}\left(\frac{2}{p}+2p\right) = \\ &= \frac{p^2-1}{8p^2}\cdot\frac{2+2p^2}{p} = \frac{p^4-1}{4p^3}.\end{aligned}$$

In the general case, with a similar reasoning we obtain

$$\mathbb{E}\left(\left|c_0+\frac{c_1}{p}+\ldots+\frac{c_k}{p^k}\right|\right)=\frac{1}{p^2}\mathbb{E}\left(\left|c_1+\ldots+\frac{c_k}{p^{k-1}}\right|\right)+\frac{2p^k}{p^{k+1}}\left(1+\ldots+\frac{p-1}{2}\right)=$$
$$=\frac{1}{p^2}\mathbb{E}\left(\left|c_1+\ldots+\frac{c_k}{p^{k-1}}\right|\right)+\frac{2p^k(p^2-1)}{8p^{k+1}}=$$
$$=\frac{1}{p^2}\mathbb{E}\left(\left|c_1+\ldots+\frac{c_k}{p^{k-1}}\right|\right)+\frac{p^2-1}{4p}.$$

The reason why $\frac{1}{p^2}$ appears in the first summand, is that, when $c_0=0$, we can collect $\frac{1}{p}$ from the sum and, moreover, the expected value on $k+1$ terms is divided by $p$ one time more than the expected value on $k$ terms. For the second summand, as before we have two times every value, every $k$-tuple cancel and they are exactly $p^k$, so we multiply that for every value of $c_0$ in $\{0,\ldots,\frac{p-1}{2}\}$. Now, if we call

$$\mathbb{E}_k=\mathbb{E}\left(\left|c_0+\frac{c_1}{p}+\ldots+\frac{c_k}{p^k}\right|\right),$$

then we have:

$$\mathbb{E}_k=\frac{p^2-1}{4p}+\frac{1}{p^2}\mathbb{E}_{k-1}=\frac{p^2-1}{4p}+\frac{p^2-1}{4p}\cdot\frac{1}{p^2}+\frac{1}{p^4}\mathbb{E}_{k-2}=$$
$$=\frac{p^2-1}{4p}\left(1+\frac{1}{p^2}+\frac{1}{p^4}+\ldots+\frac{1}{p^{2(k-1)}}\right)+\frac{1}{p^{2k}}\mathbb{E}_0=$$
$$=\frac{p^2-1}{4p}\left(1+\frac{1}{p^2}+\frac{1}{p^4}+\ldots+\frac{1}{p^{2(k-1)}}+\frac{1}{p^{2k}}\right)=$$
$$=\frac{p^2-1}{4p}\left(\frac{p^{2(k+1)}-1}{p^{2k}(p^2-1)}\right)=\frac{p^{2(k+1)}-1}{4p^{2k+1}}.$$

□

*Now, we can compute*

$$\begin{aligned}
\mathbb{E}(|a|) &= \sum_{k=1}^{+\infty} \mathbb{E}(|a| \ | v_p(a) = k)\mathbb{P}(v_p(a) = k) = \sum_{k=1}^{+\infty} \frac{p^{2(k+1)}-1}{4p^{2k+1}} \cdot \frac{p-1}{p^k} = \\
&= \frac{p-1}{4} \sum_{k=1}^{+\infty} \frac{p^{2k+2}-1}{p^{3k+1}} = \frac{p-1}{4} \left( \sum_{k=1}^{+\infty} \frac{1}{p^{k-1}} - \sum_{k=1}^{+\infty} \frac{1}{p^{3k+1}} \right) = \\
&= \frac{p-1}{4} \left( \sum_{k=0}^{+\infty} \frac{1}{p^k} - \frac{1}{p^2} \sum_{k=0}^{+\infty} \frac{1}{p^{3k}} \right) = \frac{p-1}{4} \left( \frac{1}{1-\frac{1}{p}} - \frac{1}{p^2} \cdot \frac{1}{1-\frac{1}{p^3}} \right) = \\
&= \frac{p-1}{4} \left( \frac{p}{p-1} - \frac{p}{p^3-1} \right) = \frac{1}{4} \left( p - \frac{p}{p^2+p+1} \right) = \\
&= \frac{p}{4} \left( 1 - \frac{1}{p^2+p+1} \right).
\end{aligned}$$

**Remark 8.2.8.** *Let us notice that we always expect $|a| > 1$ for all odd $p$ except $p = 3$. Moreover, the expected size of every partial quotients grows linearly with the prime $p$:*

$$\begin{aligned}
p = 13 \quad &\Longrightarrow \quad \mathbb{E}(|a|) \approx 3.23, \\
p = 43 \quad &\Longrightarrow \quad \mathbb{E}(|a|) \approx 10.74, \\
p = 211 \quad &\Longrightarrow \quad \mathbb{E}(|a|) \approx 52.75 \\
p = 839 \quad &\Longrightarrow \quad \mathbb{E}(|a|) \approx 289.75.
\end{aligned}$$

**Example 8.2.9.** *For $p = 7823$, the expansion of $\sqrt{15648}$ with Algorithm* (3.10) *provides the following convergents:*

$$\begin{aligned}
\frac{A_{10}}{B_{10}} &= 3337.56023127383\ldots,\\
\frac{A_{100}}{B_{100}} &= 3337.56023127383\ldots,\\
\frac{A_{1000}}{B_{1000}} &= 3337.56023127383\ldots,\\
\frac{A_{5000}}{B_{5000}} &= 3337.56023127383\ldots,\\
\frac{A_{10000}}{B_{10000}} &= 3337.56023127383\ldots.
\end{aligned}$$

*Indeed, the continued fraction seems to rapidly converge to a real limit, which is different from $\sqrt{15648} \approx 125.09$. In this case, it is really unlikely for the convergents to deviate from that value, due to Equation* (8.3)*. In fact, we expect $|B_n|$ to grow exponentially as*

$$|B_n| \sim |a_1| \ldots |a_n|,$$

*where the expected value of each partial quotient is, by Proposition 8.2.7,*

$$\mathbb{E}(|a|) \approx 1955.75.$$

Finally, in light of the preceding discussion, we leave the following conjecture.

**Conjecture 8.2.10.** *Let $\{|B_n|\}_{n\in\mathbb{N}}$ be the sequence of denominators of convergents of a random Browkin I, Browkin II or Algorithm* (3.10) *$p$–adic continued fraction, where $p \geq 5$. Then $|B_n|$ tends to $+\infty$ with probability* 1.

# Chapter 9

# Other works

The aim of this last section is to briefly summarize the content of the other works and preprints carried out during my Ph. D., not strictly connected to $p$–adic continued fractions, that are [3, 23, 27, 42].

In [3], written in collaboration with Gessica Alecci, Piotr Miska and Nadir Murru, we deepened the properties of the Lucas atoms. It is the result of the research developed during the visiting period of Piotr Miska in Torino. Lucas atoms were introduced by Sagan and Tirell in [70] and they are irreducible factors of Lucas polynomials. We gave a more natural and powerful definition using bivariate cyclotomic polynomial and we solved some conjectures on the $p$–adic valuation left by the authors in [70]. At the end of the paper, we prove that the sequence of Lucas atoms is not holonomic, i.e., it does not satisfy any recurrence relation, also considering the coefficients being polynomials, contrarily to the Lucas sequence that is a binary linear recurrent sequence.

In [27], written in collaboration with some other members of the CrypTO group of Torino, Antonio J. Di Scala, Andrea Gangemi and Gabriele Vernetti, we generalize a paper of 2020 by Sala, Sogiorno and Taufer [71]. The authors of [71], have been surprisingly able to recover the private keys of some Bitcoin addresses and to spend a small amount of their cryptocurrency. This result was unexpected, since the recovery of non-trivial private keys for blockchain addresses is deemed to be an infeasible problem. In particular, the security of Bitcoin transactions is guaranteed by the hardness of solving the discrete

logarithm problem over the elliptic curve *secp256k1*. The attack consisted in a brute-force search for private keys inside a small peculiar subset of points of the *secp256k1*, that unexpectedly led to actual addresses. In [27], we generalize the attack to other small subsets of private keys in the *secp256k1* and to other blockchains using the same curve, namely Ethereum, Dogecoin, Litecoin, Dash, Zcash and Bitcoin Cash. The contribution of the paper is also to provide all the code and techniques that we have used to perform this exhaustive search for all the addresses that have ever appeared in these blockchains.

Finally, [23] and [42] are two works on the study of universal quadratic forms over number fields, produced during my research period at Charles University in Prague, under the supervision of Prof. Vítězslav Kala. A quadratic form is universal if it represents all positive integers. An example is the classical sum of four squares $x^2+y^2+z^2+t^2$, that has been proved to be universal by Lagrange. Over number fields, a universal form is required to represent all totally positive integers, i.e. all the algebraic integers that are positive with respect to all the embeddings. The first paper [23] is written in collaboration with Ondřej Chwiedziuk, Matěj Doležálek, Emma Pěchoučková, Zdeněk Pezlar, Om Prakash, Anna Růžičková and Mikuláš Zindulka, as a product of the research carried out during the Number Theory Student Seminar, and we investigate a generalization of quadratic forms over number fields. A generalized quadratic form can be expressed in terms of variables and their conjugates. We characterize the real quadratic fields that admit a universal binary generalized form of such kind and we show that there are only finitely many such fields where a ternary generalized form can be universal.

In [42], a preprint recently finished in collaboration with Vítězslav Kala and Jakub Krásenský, we study criterion sets for universality over number fields. A criterion set is a subset $S$ of the totally positive integers with the property that representing all elements in $S$ is a sufficient condition for universality. A famous example is the set $\{1,2,3,5,6,7,10,14,15\}$, that is a criterion set for universality over $\mathbb{Z}$ for classical quadratic forms. We give a characterization of criterion sets for universality over number fields and we

show that they always exist and they are unique. We prove that criterion sets contain exactly the *critical* elements, i.e. elements for which we can find a quadratic form representing everything else except that element. A famous example over $\mathbb{Z}$ is the quadratic form $x^2+2y^2+5z^2+5t^2$, that represents all positive integers except 15, therefore implying that 15 is a critical element for integral quadratic forms. We also extend the results for universality over a general subset of the totally positive integers.

# Bibliography


[1] M. Abrate, S. Barbero, U. Cerruti, N. Murru, *Periodic representations and rational approximations of square roots*, J. Approx. Theory, **175** (2013), 83-90.

[2] B. Adamczewski, Y. Bugeaud, *On the complexity of algebraic numbers II. Continued fractions*, Acta Math., **195** (2005), 1-20.

[3] G. Alecci, P. Miska, N. Murru, G. Romeo, *On alternative definition of Lucas atoms and their p-adic valuations*, preprint (2023), arXiv: arXiv:2308.10216.

[4] S. Baker, *Continued fractions of transcendental numbers*, Mathematika, **9** (1962), 1–8.

[5] S. Barbero, U. Cerruti, N. Murru, *Periodic representations for quadratic irrationals in the field of p–adic numbers*, Math. Comp., **90**(331) (2021), 2267-2280.

[6] S. Barbero, U. Cerruti, N. Murru, *Periodic Representations and Approximations of p–adic Numbers Via Continued Fractions*, Exp. Math. (2021).

[7] P. G. Becker, *Periodizit¨atseigenschaften p-adischer Kettenbr¨uche*, Elem. Math., **45** (1990), 1–8.

[8] E. Bedocchi, *Nota sulle frazioni continue p–adiche*, Ann. Mat. Pura Appl., **152** (1988), 197-207.

[9] E. Bedocchi, *Remarks on Periods of p–adic Continued Fractions*, Boll. Unione Mat. Ital., **7** (1989), 209-214.

[10] E. Bedocchi, *Sur le developpement de $\sqrt{m}$ en fraction continue p–adique*, Manuscr. Math., **67** (1990), 187-195.

[11] E. Bedocchi, *Fractions continues p–adique: périodes de longueur paire*, Boll. Unione Mat. Ital., (7) **7-A** (1993), 259-265.

[12] R. Belhadef, H. A. Esbelin, *On the Complexity of p–adic continued fractions of rational numbers*, Turk. J. of Analysis and Number Theory **10**(1) (2022), 4-11.

[13] R. Belhadef, H. A. Esbelin, T. Zerzaihi, *Transcendence of Thue–Morse p–adic continued fractions*, Mediterr. J. Math. **13**(4) (2016), 1429-1434.

[14] L. Bernstein, *The Jacobi-Perron Algorithm—Its Theory and Application*, Lecture Notes in Mathematics, Vol. 207, Springer-Verlag, Berlin-New York, (1971).

[15] J. Browkin, *Continued fractions in local fields, I*, Demonstr. Math., **11** (1978), 67-82.

[16] J. Browkin, *Continued fractions in local fields, II*, Math. Comp., **70** (2000), 1281-1292.

[17] P. Bundschuh, *p-adische Kettenbrüche und Irrationalität p-adischer*, Elem. Math. **32** (1977), no. 2, 36–40.

[18] G. Cantor, *Über eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen*, J. Reine Angew. Math. **77** (1874), 258–262.

[19] L. Capuano, M. Mula, L. Terracini, *Quaternionic p–adic continued fractions*, Comm. Algebra (2024), 1-21.

[20] L. Capuano, N. Murru, L. Terracini, *On periodicity of p–adic Browkin continued fractions*, Math. Z. **305**(2) (2023), 17.

[21] L. Capuano, N. Murru, L. Terracini, *On the finiteness of $\mathfrak{P}$–adic continued fractions for number fields.*, Bull. Soc. Math. France **150** (2021), 743-772.

[22] L. Capuano, F. Veneziano, U. Zannier, *An effective criterion for periodicity of l-adic continued fractions*, Math. Comp. **88**(319) (2019), 1851–1882.

[23] O. Chwiedziuk, M. Doležálek, E. Pěchoučková, Z. Pezlar, O. Prakash, G. Romeo, A. Růžičková, M. Zindulka, *Representing rational integers by generalized quadratic forms over quadratic fields*, preprint (2024), arXiv: arXiv:2403.07171.

[24] K. Conrad, *The p–adic expansion of rational numbers*, Math. Dept. UConn, Expository article, https://kconrad.math.uconn.edu/blurbs/gradnumthy/rationalsinQp.pdf.

[25] A. A. Deanin, *Periodicity of p–adic continued fraction expansions*, J. Number Theory **23** (1986), 367-387.

[26] Y. Deng, Z. Wang, *Convergence, finiteness and periodicity of several new algorithms of p–adic continued fractions*, Math. Comp. (2024).

[27] A. J. Di Scala, A. Gangemi, G. Romeo, G. Vernetti, *Special subsets of addresses for blockchains using the secp256k1 curve*, Mathematics, **10**(15):2746 (2022).

[28] E. Errthum, *A division algorithm approach to p–adic Sylvester expansions*, J. Number Theory **160** (2016), 1–10.

[29] L. Euler, *De fractionibus continuis dissertatio*, Commentarii academiae scientiarum Petropolitanae (1744), 98-137.

[30] É. Galois, *Démonstration d'un théoréme sur les fractions continues périodiques*, Annalles de mathématiques, **19** (1828), 294-301.

[31] F.Q. Gouvea, *p–adic numbers: an introduction*, Springer, (1997).

[32] A. Haddley, R. Nair, *On Schneider's continued fraction map on a complete non-archimedean field*, Arn. Math Jour. (2021).

[33] J. Hančl, A. Jaššová, P. Lertchoosakul, R. Nair, *On the metric theory of p–adic continued fractions*, Indag. Math. **24**(1) (2013), 42-56.

[34] H. Hasse, *Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkörper*, J. Reine Angew. Math. **153** (1924) 113–130.

[35] H. Hasse, *Number Theory*, Springer-Verlag, Berlin, Heidelberg, New York (1980).

[36] K. Hensel, *Über eine neue Begründung der Theorie der algebraischen Zahlen.*, Jahresber. Deutsch. Math.-Verein. **6** (1897), 83-88.

[37] C. Hermite, *Sur l'expression* $U \sin x + V \cos x + W$, J. de Crelle **76** (1873), 303-312.

[38] C. Hermite, *Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objects de la théorie des nombres*, J. Reine Angew. Math. **40** (1850), 261-278.

[39] J. Hirsh, L. C. Washington, *p–adic continued fractions*, The Raman. Jour. **25** (2011), 389-403.

[40] H. Hu, Y. Yu, Y. Zhao, *On the digits of Schneider's p–adic continued fractions*, J. Number Theory **187** (2018), 372-390.

[41] C. G. J. Jacobi, *Ges. Werke VI*, Berlin Academy, (1891), 385-426.

[42] V. Kala, J. Krásenský, G. Romeo, *Universality criterion sets for quadratic forms over number fields*, preprint (2024), arXiv: arXiv:2410.22507.

[43] A. Ya. Khinchin, *Continued fractions*, University of Chicago Press (1964).

[44] E. E. Kummer, *De numeris complexis, qui radicibus unitatis et numeris realibus constant*, Gratulationschrift der Univ. Breslau zur Jubelfeier der Univ. Königsberg (1844).

[45] E. E. Kummer, *Collected papers*, Springer-Verlag (1975).

[46] C. Lager, *A p–adic Euclidean algorithm*, Rose–Hulman Undergraduate Mathematics Journal **10**(9) (2009).

[47] J. L. Lagrange, *Solution d'un problème d'arithmétique*, (1766), appeared in: J. A. Serret, Oeuvres de Lagrange **1** (1867) 671-731.

[48] J. H. Lambert, *Mémoire sur quelques propriétés remarquables des quantités transcendantes circulaires et logarithmiques*, Histoire Acad. R. Sci. et Belles Lettr. Berlin, (1761), 265-322.

[49] V. Laohakosol, *A characterization of rational numbers by p–adic Ruban continued fractions*, Austral. Math. Soc. Ser. **39** (1985), no. 3, 300–305.

[50] R. Lidl, G.L. Mullen, G. Turnwald, *Dickson Polynomials*, Pitman Monographs and Surveys in Pure and Applied Math., (1969).

[51] F. von Lindemann, *Über die Zahl* $\pi$, Math. Ann. **20**(2) (1882), 213-225.

[52] J. Liouville, *Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique ni même réductible à des irrationnelles algébriques*, C.R. Acad. Sci. Paris **18** (1844), 883-885.

[53] I. Longhi, N. Murru, F. M. Saettone, *Heights and transcendence of p–adic continued fractions*, Ann. Mat. Pura Appl. (2024).

[54] K. Mahler, *On a geometrical representation of p–adic numbers*, Ann. of Math. (2) 41, (1940), 8-56.

[55] N. Murru, G. Romeo, *A new algorithm for p–adic continued fractions*, Math. Comp. **93**(347) (2024), 1309–1331.

[56] N. Murru, G. Romeo, G. Santilli, *On the periodicity of an algorithm for p–adic continued fractions*, Ann. Mat. Pura Appl. **202**(6) (2023), 2971–2984.

[57] N. Murru, G. Romeo, G. Santilli, *Convergence conditions for p–adic continued fractions*, Res. number theory **9**(3) (2023), 66.

[58] C.D. Olds, *Continued fractions*, New Marhematical Library (1963).

[59] T. Ooto, *Trascendental p–adic continued fractions*, Math. Z. **287** (2017), no. 3-4, 1053-1064.

[60] T. Pejković, *Schneider's p–adic continued fractions*, Acta Math. Hung. (2023), 1-25

[61] O. Perron, *Die lehre von den Kettenbrüchen*, B. G. Teubner **36** (1913).

[62] O. Perron, *Grundlagen für eine theorie des Jacobischen kettenbruchalgorithmus*, Math. Ann. **64**(1) (1907), 1-76.

[63] A. J. van der Poorten, *Schneider's continued fraction*, Number theory with an emphasis on the Markoff spectrum (Provo, UT, 1991) Lecture Notes in Pure and Appl. Math. **147** (1993), 271–281.

[64] L. Rédei, *Über eindeutig umkehrbare Polynome in endlichen Körpern*, Acta Sci. Math. **11** (1946), 85-92.

[65] G. Romeo, *Continued fractions in the field of p–adic numbers*, Bulletin of the American Mathematical Society **61**(2) (2024), 343-371.

[66] G. Romeo, *Real convergence and periodicity of p–adic continued fractions*, preprint (2024), arXiv: arXiv:2410.09215.

[67] D. Rosen, *A class of continued fractions associated with certain properly discontinuous groups*, Duke Math. J. **21** (1954), 549–564.

[68] D. Rosen, *Research problems: Continued fractions in algebraic number fields*, Amer. Math. Monthly **84**(1) (1977), 37–39.

[69] A. A. Ruban, *Certain metric properties of the p–adic numbers*, Sibirsk Math. Z., **11** (1970), 222-227, English translation: Siberian Math. J **11**, 176-180.

[70] B. E. Sagan, J. Tirrell, *Lucas atoms*, Adv. Math., **374** (2020).

[71] M. Sala, D. Sogiorno, D. Taufer, *A Small Subgroup Attack on Bitcoin Address Generation*, Mathematics, **8:10** (2020), 16451-16458.

[72] J. P. Serre, *A course in arithmetic*, Springer Science & Business Media, (2012).

[73] T. Schneider, *Uber p-adische Kettenbruche*, Symp. Math. , **4** (1969), 181-189.

[74] F. Tilborghs, *Periodic p–adic continued fractions*, Simon Stevin, **64** (1990), no. 3-4, 383–390.

[75] H. S. Wall, *Analytic theory of continued fractions*, Courier Dover Publications, (2018).

[76] L. Wang, *p–adic continued fractions, I, II*, Scientia Sinica, Ser. A **28** (1985), 1009-1023.

[77] B. M. M. de Weger, *Approximation lattices of p–adic numbers*, J. Number Theory, **24**(1) (1986), 70-88.

[78] B. M. M. de Weger, *Periodicity of p–adic continued fractions*, Elemente der Math., **43** (1988), 112-116.

[79] S. Yasutomi, *Simultaneous Convergent Continued Fraction Algorithm for Real and p–adic Fields with Applications to Quadratic Fields.*, preprint (2023), arXiv:2309.09447.