UNIVERSITÀ
DI TRENTO

DEPARTMENT OF MATHEMATICS
Master's Degree in Mathematics

Browkin's p-adic Continued Fractions

and an analysis of open problems

Student:
Leonardo Errati

Supervisor:
prof. Nadir Murru

Co-Supervisor:
doc. Giuliano Romeo

SUMMARY

Fables begin with "once upon a time", but number theory begins with "fix a prime p". So, unless otherwise specified, consider it fixed.

In CHAPTER 1 we construct $\mathbb{Q}_p$. This must not be thought of as "taking $\mathbb{Q}$ in base p" or "the set of p-adic rationals", which does not exist in literature. They are p-adic numbers, an extension of $\mathbb{Q}$ different from $\mathbb{R}$ introduced by Kurt Hensel [15]. This is achieved by completing $\mathbb{Q}$ under an absolute value not equivalent to the Euclidean one, yielding an extension different from $\mathbb{R}$. We can also prove this is the only non-trivial absolute value on $\mathbb{Q}$ not equivalent to it. A great deal can be said about this new ultrametric space: we will describe the most important properties.

In CHAPTER 2 we define and study continued fractions in $\mathbb{R}$, along with their well-known core properties. We will appreciate how they can so nicely describe rationals and quadratic irrationals (Euler's and Lagrange's theorems), while expanding on some tools that will be useful in the study of such properties: convergents and linear fractional operators.

In CHAPTER 3 we will show how hard it is to extend the "usual" algorithm to $\mathbb{Q}_p$. This is due to the vast difference introduced by the p-adic absolute value. Some properties are lost, some are preserved, some are conjectured. We will tackle a few of these conjectures: for example, given a continued fraction algorithm on the field $\mathbb{K}$ with input α, is it true that it outputs a periodic sequence of partial quotients if and only if $[\mathbb{K}(\alpha) : \mathbb{K}] = 2$ as field extension? This is true in the usual algorithm for $\mathbb{K} = \mathbb{R}$, but does not hold in general for those we can propose for $\mathbb{K} = \mathbb{Q}_p$. The most promising ones are by Polish mathematician J. Browkin: we will study his first, Browkin I.

Lastly, in APPENDIX A one can find some details on the algorithms used to provide examples and graphs.

premise

$\mathbb{Z}$	the ring of integers
$\mathbb{Q}$	the field of rationals
p	a fixed integer prime

Chapter 1

$\mathbb{Z}_p$	the ring of p-adic integers
$\mathbb{Q}_p$	the field of p-adic numbers
ν_p	the p-adic valuation
$\varprojlim_{i \in I} R_i$	inverse limit of the rings $(R_i)_I$
$\lvert\cdot\rvert$	a generic norm / absolute value
$\lvert\cdot\rvert_p$	the p-adic norm / absolute value
$\lvert\cdot\rvert_\infty$	the Euclidean norm / absolute value
DVR	discrete valuation ring

Chapter 2

I	index set, either $I = \{0, 1, \ldots, n\}$ or $I = \mathbb{N}$
$[a_0, b_1 : a_1, \ldots]$	general continued fraction of complex $(a_i)_I, (b_i)_I$
$[a_0, a_1, a_2, \ldots]$	canonical continued fraction of partial quotients $(a_i)_I$
$\mathbb{P}$	set of irrational numbers
C_i	i-th convergent of the continued fraction
$L_m(\cdot)$	linear fractional operator associated to the matrix m

Chapter 3

P0	convergence of the algorithm in $\mathbb{Q}_p$
P1	finiteness of the algorithm for $\alpha \in \mathbb{Q}$
P2	periodicity of algorithm output iff α is quadratic irrational
$r(\cdot)$	Ruban's floor function
$s(\cdot)$	Browkin's (first) floor function
$t(\cdot)$	Browkin's (second) floor function
$\mathbb{Z}[1/p]$	ring of s-integers
norm$(\cdot)$	number theoretical norm
trace$(\cdot)$	number theoretical trace

There is a great deal of ambiguity on the term "norm". In the geometrical or analytical sense, it is an absolute value on a *normed vector space*. In a number theoretical sense, one usually means the *field norm* or *ideal norm*. They are sometimes used interchangeably. We will try to make a clear distinction, but caveat lector.

Contents

Chapter 1

The field of p-adic numbers

It is an habit of old to view integers in base 10. Although motivated by valid biological reasons, this choice can be considered rather arbitrary by mathematicians. Sumerians worked in base 60, which is a *highly composite number* and simplifies many calculations involving it, and used 10 as sub-base to represent their sexagesimal digits. They would perhaps consider our base 10 quite naive.
To our credit, base 10 incidentally provides an excellent trade-off between size of the multiplication table (10×10) and length of integer representations. Of course base 2 has an even smaller multiplication table, but representing the number "one million" requires twenty digits!

We will start working with bases different from ten, in which case we will display numbers with red bold digits. For example, in base 5

$$27 = 1 \times 5^2 + 0 \times 5^1 + 2 \times 5^0 = \mathbf{102}_5$$
$$183 = 1 \times 5^3 + 2 \times 5^2 + 1 \times 5^1 + 3 \times 5^0 = \mathbf{1213}_5$$

Following the usual convention for base 10, we will arrange powers of the base in a decreasing fashion. This is what computer scientists refer to as *little endian* in their binary case. Integers from 0 to 9 are called *digits*, and to maintain the parallelism we will refer to values between 0 and $p-1$ as **p-adic digits**.

We will start working with prime bases, gradually building up to the construction of the field of p-adic numbers and witnessing how they relate to some common structures in algebra.
This chapter is an introduction on p-adic numbers roughly arising from personal remarks on Gouvea [13]. Useful contributions can be also found in Pomerantz [31] for mathematical analysis in the p-adic setting, Madore [22] and Conrad [10] for an introduction on p-adic rational numbers and the properties of their expansions, Schikhof [38] for some results on analysis and topology and Serre [40] for results in group theory.

1.1 Representations with non-negative powers

On operations over $\mathbb{Z}$ in prime base.

Throughout the following chapter, p is a fixed odd prime unless specified.

While working in base p, one of the most difficult tasks is to actually remember the algorithms we were taught back in elementary school. All examples in this section will consider the prime base $p = 11$, so our digits will be **0**,**1**,**2**,**3**,**4**,**5**,**6**,**7**,**8**,**9**,***X*** with the rule that **1** + ***X*** = 11 = **10**. They can be referred to as the *11-adic digits*.

Problem 1 Consider a fixed prime p. Write integers m as $m = \sum_{i=0}^{+\infty} a_i p^i$ for integer coefficients a_i of values $0 \leq a_i \leq p-1$.

Addition is simple, **123** + **34** = **157**. We can easily check for correctness[1].

$$\begin{aligned} \mathbf{123} + \mathbf{34} &= \left(1 \times 11^2 + 2 \times 11^1 + 3 \times 11^0\right) + \left(3 \times 11^1 + 4 \times 11^0\right) \\ &= 1 \times 11^2 + 5 \times 11^1 + 7 \times 11^0 = \mathbf{157} \end{aligned}$$

Multiplication follows similarly, and all usual rules still hold. Negative integers are harder to study in a way that satisfies Problem 1. Expressing **−1** is a sufficient condition to obtain all of them.

Lemma 1.1 Fix an integer p. Then $-1 = \sum_{i=0}^{+\infty} (p-1)p^i$.

Sketch of proof. Intuitively, we can escalate a single carry-over to the whole series.

$$\begin{aligned} 1 + \sum_{i=0}^{+\infty} (p-1)p^i &= 1 + (p-1)p^0 + (p-1)p + (p-1)p^2 + (p-1)p^3 + \dots \\ &= (p-1+1) + (p-1)p + (p-1)p^2 + (p-1)p^3 + \dots \\ &= (p-1+1)p + (p-1)p^2 + (p-1)p^3 + \dots \\ &= (p-1+1)p^2 + (p-1)p^3 + \dots = 0 \end{aligned}$$

We will need better tools to construct a formal proof. □

It might seem that we swept something under the rug, and that is actually the case. This series does not converge in the usual sense, but we will see how that is possible in our setting. For $p = 11$,

$$\mathbf{-1} = 10 \times 11^0 + 10 \times 11^1 + 10 \times 11^2 + \dots = \dots \mathbf{XXXXXXXXXX}$$

Remark that due to our notation there are infinitely many digits on the left. We can express **−7** in a way that satisfies Problem 1:

$$\begin{aligned} \mathbf{-7} &= 7 \sum_{i=0}^{+\infty} (10)11^i = \sum_{i=0}^{+\infty} (70)11^i = \sum_{i=0}^{+\infty} (6 \times 11 + 4)11^i \\ &= \sum_{i=0}^{+\infty} (6)11^{i+1} + \sum_{i=0}^{+\infty} (4)11^i = \sum_{i=1}^{+\infty} (6)11^i + \sum_{i=0}^{+\infty} (4)11^i \\ &= \sum_{i=1}^{+\infty} (X)11^i + \mathbf{4} = \dots \mathbf{XXXXXXXXX4} \end{aligned}$$

[1] The amount of mistakes one does in these is perhaps independent from the fixed integer base.

Since all digits of any y and $-y$ add up to zero, we can prove the following.

Lemma 1.2 Consider $y = a_0 + a_1 p + a_2 p^2 + \dots$, then $-y = b_0 + b_1 p + b_2 p^2 + \dots$ is constructed as follows:

(i) ignore all trailing zeroes: these b_i are zero

(ii) for the first index k such that a_k is non-zero, $b_k = p - a_k$

(iii) then we must account for carrying, hence for $k' > k$, $b_{k'} = p - 1 - a_{k'}$

This makes additive inverses easier to handle, and actually proves that the inverse we found before was correct.

1.2 Representations with negative powers

On operations over $\mathbb{Q}$ in prime base.

Recall that in $\mathbb{Z}$ division is often[2] undefined, and to account for this we need to work in $\mathbb{Q}$. Similarly, we need a variation of Problem 1 able to account for "decimal precision". In base 10 this is done including negative powers of 10.

Problem 2 Consider a fixed prime p. Write rationals $r = a/b$ as $r = \sum_{i=-k}^{+\infty} a_i p^i$ for integer coefficients a_i of values $0 \le a_i \le p-1$, and k such that a_{-k} is non-zero.

Let us start with an example. Consider $r = 144/23$,

$$r = \frac{144}{23} = \frac{1 \times p^2 + 2 \times p + 1}{2 \times p + 1}$$

and consider r as a formal series (i.e. we do not particularly care that $p = 11$ while dividing). The natural strategy is to seek for an expression $a_0 + a_1 p + a_2 p^2 + \dots$ such that

$$\begin{aligned}
\mathbf{121} &= 1 + 2p + 1p^2 \\
&= (1 + 2p)(a_0 + a_1 p + a_2 p^2 + a_3 p^3 + a_4 p^4 + \dots) \\
&= a_0(1 + 2p) + a_1 p(1 + 2p) + a_2 p^2(1 + 2p) + a_3 p^3(1 + 2p) + a_4 p^4(1 + 2p) + \dots \\
&= p^0(a_0) + p(2a_0 + a_1) + p^2(2a_1 + a_2) + p^3(2a_2 + a_3) + p^4(2a_3 + a_4) + \dots
\end{aligned}$$

therefore $a_0 = 1$, $a_1 = 0$, $a_2 = 1$, $a_3 = 9$, and

$$r = \dots \mathbf{24339101} = 1 + 0p + 1p^2 + 9p^3 + 3p^4 + 3p^5 + \dots$$

Notice how we used $p = 11$ at some point. This expansion satisfies Problem 1 since the powers of p are all non-negative, but not all rationals do. Consider $s = 144/(23 \times 11)$,

$$\begin{aligned}
s = \frac{144}{23 \times 11} &= p^{-1} \frac{144}{23} = p^{-1} \left(\frac{1 \times p^2 + 2 \times p + 1}{2 \times p + 1} \right) \\
&= 1p^{-1} + 0 + 1p + 9p^2 + 3p^3 + 3p^4 + \dots = \dots \mathbf{2433910.1}
\end{aligned}$$

[2] But not always! For example, one can reasonably write 6 divided by 3 in $\mathbb{Z}$. What is undefined is division with a non-integral remainder.

Dividing by a power of p shifts the expansion by one element, so we require a negative starting index $-k$. As noted by Madore [22], this is essentially the only operation that requires a generalisation to Problem 2. It is very convenient to introduce the set $\mathbb{Q}_p$ of all sums of powers of p satisfying it.

Definition 1.3 Fix a prime p in $\mathbb{Z}$, the **set of p-adic numbers** is

$$\mathbb{Q}_p = \left\{ x = \sum_{i=-k}^{+\infty} a_i p^i \text{ for } 0 \leq a_i \leq p-1 \text{ and } k \in \mathbb{Z} \right\}$$

and any $x \in \mathbb{Q}_p$ is called **p-adic series** or **p-adic number**.

This chapter will prove that this is a field extension of $\mathbb{Q}$, and the inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ justifies our results. We will need some further tools.

1.3 The p-adic absolute value

On the construction of a new absolute value from algebraic properties of primes p.

Definition 1.4 Fix a prime p in $\mathbb{Z}$, the **p-adic valuation on** $\mathbb{Z}$ is a function

$$\nu_p : \mathbb{Z} \longrightarrow \mathbb{N} \cup (+\infty)$$

that associates to any non-zero integer n the unique positive integer $\nu_p(n)$ such that $n = p^{\nu_p(n)} n'$ and $p \nmid n'$, the maximum power of p dividing n. We set by definition $\nu_p(0) = +\infty$ since every power of p divides 0.

An integer e such that $n = p^e n'$ and $p \nmid n'$ is trivially unique due to unique factorisation in $\mathbb{Z}$. In fact, the p-adic valuation of an integer n is the multiplicity m of p in the prime factorisation of n. For example

$$\begin{aligned} \nu_{11}(5) &= 0 \\ \nu_7(294) &= \nu_7(7^2 \times 6) = 2 \end{aligned}$$

The p-adic valuation map on $\mathbb{Z}$ is a completely additive arithmetic function, and it can be naturally extended to any $x = {}^a\!/_b \in \mathbb{Q}$ as $\nu_p(x) = \nu_p(a) - \nu_p(b)$. This corresponds to the same formula from Definition 1.4 applied on x.

Lemma 1.5 The basic properties of the p-adic valuation on $\mathbb{Q}$ are

(i) $\nu_p(xy) = \nu_p(x) + \nu_p(y)$

(ii) $\nu_p(x+y) \geq \min\{\nu_p(x), \nu_p(y)\}$

(iii) $\nu_p(x+y) = \min\{\nu_p(x), \nu_p(y)\}$ if $x \neq y$

The proof of these is very simple, just write x and y as powers of primes.
A natural requirement is for p to be prime. We could define a "m-adic valuation" for a composite m, but it would not satisfy these properties.

$$\begin{aligned} \nu_6(12 \times 3) &= \nu_6(36) = 2 \\ &= \nu_6(12)\nu_6(3) = 1 \times 0 = 0 \end{aligned}$$

Definition 1.6 Consider a field $\mathbb{K}$, an **absolute value** on $\mathbb{K}$ is a function

$$|\cdot| : \mathbb{K} \longrightarrow \mathbb{R}_+$$

that satisfies the following conditions:

(i) $|x| = 0$ if and only if $x = 0$

(ii) $|xy| = |x|\,|y|$ for all $x, y \in \mathbb{K}$

(iii) $|x + y| \leq |x| + |y|$ for all $x, y \in \mathbb{K}$

The absolute value is said **non-archimedean** if

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

Properties from Proposition 1.5 are very similar to some of Definition 1.6: products became sums and inequalities were reversed, just like with logarithms. In fact, we can exploit the p-adic evaluation on $\mathbb{Q}$ to create an absolute value.

Definition 1.7 The **p-adic absolute value on $\mathbb{Q}$** is defined as

$$|x|_p = p^{-\nu_p(x)}$$

where $|0|_p = 0$ by definition. We allow by convention that $p = \infty$ so that the usual Euclidean norm may be denoted as $|\cdot|_\infty$.

Theorem 1.8 $|\cdot|_p$ is a non-archimedean absolute value on $\mathbb{Q}$.

Proof. Fix a prime integer p. Consider properties (i), (ii), (iii), (iv) of absolute values. From Proposition 1.5 and Definition 1.7 is easy to see that (i), (ii) and (iv) hold. What is interesting is that the non-archimedean property (iv) implies (iii), since $max\{|x|, |y|\} \leq |x| + |y|$. If it was strictly larger, then without loss of generality $|x| > |x| + |y|$ and $|y| < 0$, which is impossible. □

A metric space with a non-euclidean distance is called **ultrametric space**, and the associated metric is called **super-metric**.
We just proved that $\left(\mathbb{Q}, |\ |_p\right)$ is ultrametric if we consider $d_p(x, y) = |x - y|_p$ distance induced by the absolute p-adic value. This property spawns nightmarish - but nonetheless correct - statements, like the fact that all triangles are isosceles, or that all points inside a ball are its center, or even worse that all balls of positive radius in the induced topology are clopen.
The reader might get a taste by realising that for $p = 5$ the integers 1 and 26 are closer in 5-adic norm than 1 and 2.

What mainly interests us is how this new absolute value impacts the convergence of our p-adic series. This will open a new path for our detour in $\mathbb{Q}_p$, as we will be able to start making comparisons with $\mathbb{R}$.

Lemma 1.9 If $|r|_p < 1$, the series $\sum_{i=0}^{+\infty} r^i$ converges to $\frac{1}{1-r}$ in $\left(\mathbb{Q}, |\cdot|_p\right)$.

Proof. Consider (s_n) the sequence of partial sums, $s_n = \sum_{i=0}^{n-1} r^i$. Then

$$s_n = r^0 + \cdots + r^{n-1}$$
$$rs_n = r^0 - r^n = 1 - r^n$$

thus we get $s_n(1-r) = 1-r^n$ and $s_n = {}^{1-r^n}/_{1-r}$. The critical part is noticing that the limit of r^n is 0 for $n \to +\infty$. Since $|r^n|_p = |r|_p \cdots |r|_p$ is a decreasing product of n elements, for any $m > 0$ there exists an $N \in \mathbb{N}$ such that for any $n > N$ we have $|r^n|_p < m$. Thus

$$\sum_{i=0}^{+\infty} r^i = \lim_{n\to\infty} s_n = \lim_{n\to\infty} \sum_{i=0}^{n-1} r^i = \lim_{n\to\infty} \frac{1-r^n}{1-r} = \frac{1}{1-r} \qquad \square$$

This is the first link for the analytical construction of $\mathbb{Q}_p$. We already meddled with this norm, for example with it the series in Lemma 1.1 converges.

Alternative proof of Lemma 1.1. Since $|p|_p = p^{-1} < 1$,

$$\sum_{i=0}^{+\inf} (p-1)p^i = (p-1)\sum_{i=0}^{+\inf} p^i = \frac{p-1}{1-p} = -1 \qquad \square$$

1.4 Structure of $\mathbb{Z}_p$ as inverse limit

On the construction of p-adic integers via inverse limit of rings.

Definition 1.10 Fix a prime p in $\mathbb{Z}$, the **set of p-adic integers** is

$$\mathbb{Z}_p = \left\{ r = \sum_{i=0}^{+\infty} a_i p^i \text{ for } 0 \le a_i \le p-1 \right\}$$

We saw in Section 1.1 that this set contains all elements of $\mathbb{Z}$. There is a strong link between $\mathbb{Z}_p$ and working modulo p. Consider the 11-adic integer $r = 7 + 3p + 1p^2 = 7 + 33 + 121 = 161$ and write

$$\begin{aligned} 161 \mod 11^1 &= 7 = \alpha_1 \\ 161 \mod 11^2 &= 40 = \alpha_2 \\ 161 \mod 11^3 &= 161 = \alpha_3 \\ 161 \mod 11^4 &= 161 = \alpha_4 \end{aligned}$$

This is what we usually do in base 10: working with increasing powers of 10 yields more digits of r, eventually stopping. New digits "are zero" for each extra step. If we set $\alpha_k = \alpha_3$ for $k \ge 4$, we get a sequence of integers (α_n) representing r in a process called *successive approximation*.

Definition 1.11 A sequence of integers (α_n) such that $\alpha_n \in \{0, 1, \dots, p^n - 1\}$ is called **p-coherent** if for every $n \ge 1$ it holds that $\alpha_{n+1} \equiv \alpha_n \mod p^n$.

Our sequence is 11-coherent, meaning that $\alpha_n - \alpha_{n+1} \in \mathbb{Z}/p^n\mathbb{Z}$. This is a sort of "measure of closeness": the last n digits of their p-adic expansion match up. The sequence describes an element of $\mathbb{Z}_p$ via successive approximation.

Definition 1.12 Consider a family of rings $(R_i)_{i\in I}$, with $I \subseteq \mathbb{N}$ set of indices, paired with ring morphisms $\psi_{ij} : R_j \to R_i$ for $i \le j$ such that

(i) ψ_{ii} is the identity on the ring R_i

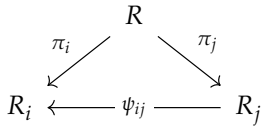
(ii) $\psi_{ik} = \psi_{ij} \cdot \psi_{jk}$ for any $j \in \{i, i+1, \dots, k\}$

If these are satisfied, the family of rings together with the family of morphisms is called **inverse system of rings** and the ψ_{ij} **transition morphisms**. We define the **inverse limit of the (inverse system of) rings** as

$$\varprojlim_{i \in I} R_i \coloneqq \left\{ x \in \prod_{i \in I} R_i \mid \psi_{ij}(a_j) = a_i \text{ for } i \leq j \text{ in } I \right\}$$

Inverse limits of different kind of structures arise from category theory: see MacLane [21] for a general introduction and Grillet [14] for an algebraic construction. We are only interested in inverse limits of rings and their properties.

Lemma 1.13 Let R be the limit of the inverse ring system $(R_i)_i$ with morphisms ψ_{ij}. Then R is a subring of the direct product of the R_i. It has natural projections $\pi_i : R \longrightarrow R_i$ such that for $i \leq j$ we have $\pi_i = \psi_{ij} \circ \pi_j$, or equivalently the following diagram commutes.



Proof. R is a subset of the direct product. All operations and natural projections π_i of the direct product are embedded in it. They are well-defined, for instance $r + s = (\alpha_0 + \beta_0, \alpha_1 + \beta_1, \dots) \in R$ because the ψ_{ij} are ring morphisms and behave well under these element-wise operations. Proving all ring properties for R is a simple matter of easy calculations, as

$$\begin{aligned}(r+s)+t &= (\alpha_0+\beta_0, \alpha_1+\beta_1, \alpha_2+\beta_2, \dots) + t \\ &= (\alpha_0+\beta_0+\gamma_0, \alpha_1+\beta_1+\gamma_1, \alpha_2+\beta_2+\gamma_2, \dots) \\ &= r + (\beta_0+\gamma_0, \beta_1+\gamma_1, \beta_2+\gamma_2, \dots) = r + (s+t)\end{aligned}$$

and we saw that in all steps these are elements of R. Finally $\pi_i = \psi_{ij} \circ \pi_j$, since

$$\psi_{ij} \circ \pi_j (r) = \psi_{ij} \left(\pi_j(r) \right) = \psi_{ij} \left(\alpha_j \right) = \alpha_i = \pi_i(r) \qquad \square$$

Fix $R_i = \mathbb{Z}/p^i\mathbb{Z}$. Consider the modular valuation maps

$$\begin{aligned}\psi_n : \mathbb{Z}/p^n\mathbb{Z} &\longrightarrow \mathbb{Z}/p^{n-1}\mathbb{Z} \\ r \mod p^n &\longmapsto r \mod p^{n-1}\end{aligned}$$

which are well-defined because p^n divides p^{n+1}. Consider also the transition morphisms

$$\psi_{ij} = \begin{cases} \psi_i \circ \cdots \circ \psi_j & \text{if } i < j \\ \psi_j \circ \cdots \circ \psi_i & \text{if } i > j \\ \text{identity on } R_i & \text{else} \end{cases}$$

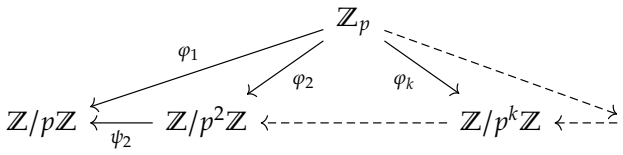
These satisfy Definition 1.12, and we will investigate R.

Theorem 1.14 ($\mathbb{Z}_p$ as inverse limit) There exists a map

$$\varphi : \mathbb{Z}_p \longrightarrow \prod_{n=0}^{+\infty} \mathbb{Z}/p^n\mathbb{Z}$$
$$r = \sum_{i=0}^{+\infty} a_i p^i \longmapsto (\alpha_0, \alpha_1, \alpha_2, \dots)$$

such that φ is a ring isomorphism and $(\alpha_n)_n$ is a p-coherent sequence.

Proof. Our setting is the following.



Define $\alpha_n \equiv r \mod p^n$. These are the terms of a p-coherent sequence, as a generic α_n lies in $\{0, \dots, p^n - 1\}$ with the usual choice of representatives and

$$\begin{aligned} \alpha_{n+1} \mod p^n &= \left(r \mod p^{n+1}\right) \mod p^n \\ &= r \mod p^n = \alpha_n \mod p^n \end{aligned}$$

which can only be done because ψ_n is well-defined. Moreover, they are unique by construction.
If we have $r, s \in \mathbb{Z}_p$ with $r \neq s$ with the same image, then their difference is zero in every $\mathbb{Z}/p^k\mathbb{Z}$ and the expansion in $\mathbb{Z}_p$ of $r - s$ is $0 + 0p + 0p^2 + \dots$ so the map is injective. This is the "gradual approximation" in each ideal $p^k\mathbb{Z}_p$ we described before, but is induced by conditions in each $p^k\mathbb{Z}$. The map is also surjective, since for any given sequence $(\alpha_n)_n$ we can construct an $r \in \mathbb{Z}_p$ such that $\varphi(r) = (\alpha_1, \alpha_2, \dots)$. It suffices to proceed as we did in our example. Finally, the image is an infinite direct product of rings, so it is a ring. □

Then $\mathbb{Z}_p$ is a ring with our $\varphi_i : \mathbb{Z}_p \to \mathbb{Z}/p^i\mathbb{Z}$ acting as its natural projections. Operations are those of the direct product of rings. This structure represents the approximation of r via a p-coherent sequence (α_n). On one side we have an algebraic structure ($\mathbb{Z}_p$), on the other side a topological structure. This theorem acts as a bridge.

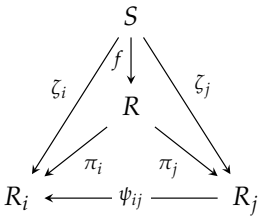
Corollary 1.15 $\mathbb{Z}_p$ is uncountable.

Sketch of proof. Consider Cantor's diagonal argument. If $\mathbb{Z}_p$ is countable we can construct a table where each entry is the coefficient of a power of p.

	1	p	p^2	p^3	p^4	p^5
r_0	**0**	2	1	0	4	7
r_1	0	**2**	5	1	3	6
r_2	1	5	**6**	2	4	5
r_3	0	1	3	**0**	7	4

Take the diagonal $d = 0 + 2p + 6p^2 + 0p^3 + \dots$ and construct d' with i-th entry different from that of d. For example, if d has a 0 put 1 and else put 0. This returns $d' = 1 + 0p + 0p^2 + 1p^3 + \dots$ which cannot be in the table. If it was, $d = r_k$ and the k-th entry would match with the k-th entry of d for some k. □

Theorem 1.16 (Universal property of inverse limits) Consider R inverse limit of the rings R_i paired with the transition morphisms ψ_{ij}. Then the pair (R, π_i) given by Lemma 1.13 is universal, meaning that any other pair (S, ζ_i) satisfying those properties has an unique morphism $f : S \to R$ such that the following diagram commutes.



Proof. See Gouvea [13] for more information. □

1.5 Structure of $\mathbb{Z}_p$ as ring

On the properties of elements and ideals of $\mathbb{Z}_p$ as integral domain.

Observant readers might have noticed some similarities with formal power series. If we set X in place of p, with the remark that $pX = p^2 = X^2$, $\mathbb{Z}_p$ can be seen as the quotient $\mathbb{Z}[[X]]/(X-p)$ with all its operations. We will keep referring to Definition 1.10, but it can be helpful keeping this trick in mind.

Proposition 1.17 An equivalent definition for $\mathbb{Z}_p$ is

$$\mathbb{Z}_p = \left\{ r \in \mathbb{Q}_p \ : \ |r|_p \leq 1 \right\}$$

The proof is simple, as having p-adic norm less than 1 implies having p-adic valuation greater than 0. Nevertheless, this result comes in handy while handling some algebraic properties.

Lemma 1.18 $\mathbb{Z}_p$ is a ring, and there exists a strict inclusion $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ acting as a natural ring homomorphism.

Proof. $\mathbb{Z}_p$ is a ring under the same operations of the direct product of the rings $\mathbb{Z}/p^k\mathbb{Z}$. The inclusion map is given by $n \mapsto (n \mod p, n \mod p^2, \dots)$, and is strict due to the cardinalities of $\mathbb{Z}$ and $\mathbb{Z}_p$. □

Consider for example $\mathbb{Z}_3$. It contains a copy of $\mathbb{Z}^+$ obtained expressing positive integers in base 3, and a copy of $\mathbb{Z}^-$ obtained multiplying positive integers by -1. The expansions of all integers are finite. But $\mathbb{Z}_3$ also contains some elements of $\mathbb{Q}$, and their expansion is *infinite*. Consider the periodic

$$\begin{aligned} r &= 2 + 0p + 1p^2 + 0p^3 + 1p^4 + 0p^5 + 1p^6 + \dots \\ &= 2 + \sum_{k=1}^{+\infty} 3^{2k} = 2 + \sum_{k=1}^{+\infty} 9^k = 1 + \frac{1}{1-9} = \frac{1 \times 8 - 1}{8} = \frac{7}{8} \end{aligned}$$

where the geometric series converges because 9 has 3-adic norm 3^{-2}. We also know that some numbers cannot be expressed in $\mathbb{Z}_3$, for example

$$\begin{aligned} s = \frac{7}{24} &= p^{-1}\frac{7}{8} = p^{-1}\left(2 + 0p + 1p^2 + 0p^3 + 1p^4 + 0p^5 + 1p^6 + \dots\right) \\ &= 2p^{-1} + 0 + 1p + 0p^2 + 1p^3 + 0p^4 + 1p^5 + \dots \end{aligned}$$

We hinted that division by p is essentially the only operation that cannot be expressed in $\mathbb{Z}_p$. This can be described as $\mathbb{Z}_p$ being a local ring.

Lemma 1.19 Consider the commutative ring $\mathbb{Z}_p$.

(i) An element is invertible if and only if it has unitary p-adic norm.

(ii) Any $r \in \mathbb{Z}_p$ can be written as $r = up^k$ for some $k \geq 0$ and $u \in \mathbb{Z}_p$ invertible.

(iii) $\mathbb{Z}_p$ is a principal ideal domain of Krull dimension one.

(iv) $\mathbb{Z}_p$ is a local ring whose unique maximal ideal is $(p) = \left\{x \in \mathbb{Q}_p \,:\, |r|_p < 1\right\}$.

Proof. Property (i). If x is invertible then $|rr^{-1}|_p = |r|_p|r^{-1}|_p = 1$ and by definition the norm of any r in $\mathbb{Z}_p$ is at most 1. If r has unitary norm then p does not divide r and they are relatively prime. There exist two integers x,y such that $rx + py = 1$, and

$$\begin{aligned} (xr)^{-1} &= \frac{1}{1-py} = \sum_{i=0}^{+\infty}(py)^i = 1 + yp + y^2p^2 + y^3p^3 = \dots \\ r\left(\frac{x}{1-py}\right) &= r + (ry)p + (ry^2)p^2 + (ry^3)p^3 + (ry^4)p^4 = \frac{rx}{1-py} = 1 \end{aligned}$$

where the geometric series converges because $\nu_p(yp) \geq 1$ and $|yp|_p \leq p^{-1} < 1$.

Property (ii). If $|r|_p = p^{-k}$, then p^k divides r and $u = {}^{r}\!/_{p^k}$ has unitary norm.

Property (iii). We first prove that all ideals are those generated by powers of p. From property (i) we know that an $r \in \mathbb{Z}_p$ is an unit if and only if $r = a_0 + a_1p + a_2p^2 + \dots$ with $a_0 \neq 0$. Remark that subsets of the form (p^k) are ideals, and any ideal containing an element of unitary norm is $\mathbb{Z}_p$ itself. These two facts prove that (p) is a maximal ideal, since every element outside of it is invertible. Any maximal ideal has to satisfy this property, so (p) is the *unique* maximal ideal. Consider now a generic proper ideal I. Pick the smallest k such that $I \subseteq (p^k)$ and $I \nsubseteq (p^{k+1})$, which must exist since $I \subseteq (p)$. We have elements $r \in I$ not contained in (p^{k+1}), and they can be written as $r = sp^k$ for $s \nmid p$. This means s has norm 1 and is invertible, so $rs^{-1} = p^k$ and $(p^k) \subseteq I$. We just proved that all ideals have form (p^k) for some k, thus they form a chain of inclusions

$$\mathbb{Z}_p = (1) \supset (p) \supset (p^2) \supset (p^3) \supset (p^4) \supset \cdots \supset (p^k) \supset \dots$$

The unique non-trivial maximal ideal is the one generated by p. It is also the only non-trivial prime ideal: for any other generator p^k the quotient ${}^{\mathbb{Z}_p}\!/_{(p^k)}$ is not an integral domain. For example in ${}^{\mathbb{Z}_p}\!/_{(p^2)}$ we have $(0 + 1p)(0 + 1p) \equiv 0$,

and in general we just consider $p \cdot p^{k-1} \equiv 0$. Hence the Krull dimension of $\mathbb{Z}_p$ is one. Of course $\mathbb{Z}_p$ is a domain, being a subring of the field[3] $\mathbb{Q}_p$.

Property (iv). We already proved that (p) is the unique maximal ideal of $\mathbb{Z}_p$. A commutative ring with an unique maximal ideal is local, and in particular $\mathbb{Z}_p$ is a **local domain**. □

If $x - y \in (p^k)$, they are "close" in p-adic norm. And if $x - y \in (p^{k+1}) \subset (p^k)$, they are even closer. The intersection of all ideals is the null ideal (0), so if this holds for all k we get $x = y$. Since a discrete valuation ring is a principal ideal domain with exactly one non-trivial maximal ideal, we have the following.

Theorem 1.20 $\mathbb{Z}_p$ is a discrete valuation ring (DVR).

One of the equivalent definitions of DVR requires a *discrete valuation function* on the ring, which would be the p-adic valuation. We could derive the same theory from the perspective of commutative algebra and discrete valuations.

Definition 1.21 (Atiyah and MacDonald [20], page 94) Let K be a field. A **discrete valuation on K** is a mapping $\nu : K^* \to \mathbb{Z}$ such that

(i) $\nu(xy) = \nu(x) + \nu(y)$, i.e. ν is an homomorphism,

(ii) $nu(x + y) \geq \min[\nu(x), \nu(y)]$.

The set $\{x \in K^* \mid \nu(x) \geq 0\} \cup \{0\}$ is a ring, called the **valuation ring of ν**. It is sometimes convenient to extend ν to the whole of K by putting $\nu(0) = +\infty$.

Proposition 1.22 (Atiyah and MacDonald [20], Proposition 9.2) Let A be a Noetherian local domain of (Krull) dimension one, $\mathfrak{m}$ its maximal ideal, $k = A/\mathfrak{m}$ its residue field. Then the following are equivalent:

(i) A is a discrete valuation ring,

(ii) A is integrally closed,

(iii) $\mathfrak{m}$ is a principal ideal.

Lemma 1.19 states that we are under these assumptions, so (i) and (iii) are equivalent. This proves Theorem 1.20. The theory of p-adic integers can be constructed from this, and we will hint at the procedure in Section 3.11.

1.6 Structure of $\mathbb{Q}$ as metric space

On norms over rational numbers and the completion of $\mathbb{Q}$.

We have a good understanding of $\mathbb{Z}_p$, but p-adic numbers, much like real numbers, rely on results from topology. That would require working on topological spaces and is not really worth getting into. We are still interested in the main results, so let us start from $\mathbb{Q}$.

Theorem 1.23 (Ostrowski) Any non-trivial absolute value on $\mathbb{Q}$ is equivalent to the Euclidian absolute value $|\cdot|_\infty$ or the p-adic absolute value $|\cdot|_p$.

[3] It is true that $\mathbb{Q}_p$ is a field, and we will show it independently from this. $\mathbb{Z}_p$ is presented before $\mathbb{Q}_p$ just for ease of explanation.

Proof. An excellent proof can be found in Schikhof's book [38]. □

The trivial absolute value is $|x|_0 = 0$ if $x = 0$ and $|x|_0 = 1$ otherwise. It is worth to mention a few points that arise comparing the proofs in Schikhof [38] and Gouvea [13].

(i) The proof separates the case of *archimedean* and *non archimedean* norm. The first is topologically equivalent to $|\cdot|_\infty$, the latter to some $|\cdot|_p$.

(ii) For $|\cdot|_p$, p must be prime. We already know there could possibly be zerodivisors otherwise. See Richeson [34] for more.

(iii) The absolute value $|\cdot|_p$ gives information on the prime factorisation, while $|\cdot|_\infty$ gives information on the sign.

From Theorem 1.14, we understood that dealing with elements of $\mathbb{Z}_p$ as sequences is easier. A similar theory can be extended to the elements of $\mathbb{Q}_p$.

Definition 1.24 A sequence (x_n) over a metric space $(\mathbb{X}, d)$ is called **Cauchy** if for any $\varepsilon > 0$ there exists an N such that $d(x_n - x_m) < \varepsilon$ for all $n, m > N$. The set $\mathbb{X}$ is called **complete with respect to** d if every Cauchy sequence of elements in $\mathbb{X}$ has limit in $\mathbb{X}$.

If the metric d is induced by a norm, we usually write it in place of d. It is well-known that $(\mathbb{R}, |\cdot|_\infty)$ is complete. $\mathbb{R}$ is actually the smallest field with an inclusion $\mathbb{Q} \hookrightarrow \mathbb{R}$ completing $\mathbb{Q}$ under $|\cdot|_\infty$. We might wonder whether $\mathbb{Q}$ is complete with respect to $|\cdot|_p$ instead. This is not always the case: with $|\cdot|_0$ all Cauchy sequences are eventually bounded by $|x_n - x_m|_0 < \varepsilon$, implying $|x_n - x_m|_0 = 0$ and $x_n = x_m$. They are stuck in x, which will be their limit.
First, remark that we are in a non-archimedean metric space.

Lemma 1.25 If $|\cdot|$ is a non-archimedean absolute value on $\mathbb{X}$, a sequence (x_n) of elements of $\mathbb{X}$ is Cauchy if and only if

$$\lim_{n \to +\infty} |x_{n+1} - x_n| = 0$$

Proof. If the sequence is Cauchy, the result is immediate.
Consider on the other hand x_m and x_n $(m > n)$ from Definition 1.24, $m = n + r$,

$$\begin{aligned} |x_m - x_n| &= |x_{n+r} - x_{n+r-1} + x_{n+r-1} - \cdots + x_{n+1} + x_n| \\ &\leq \max\{|x_{n+r} - x_{n+r-1}|, \ldots, |x_{n+1} - x_n|\} \to 0 \end{aligned}$$ □

Theorem 1.26 The field of rational numbers $\mathbb{Q}$ is not complete with respect to any of its non-trivial absolute values.

Sketch of proof. We already know it for $|\cdot|_\infty$. For $|\cdot|_p$, we can construct an adequate Cauchy sequence. Suppose p is odd, take an integer α such that

(i) α is not a square in $\mathbb{Q}$

(ii) p does not divide a

(iii) α is a quadratic residue modulo p

This always exists, consider any perfect square integer and add a suitable multiple of p. Consider now α_0 solution of $\alpha_0^2 \equiv \alpha \mod p$. Mahler [23] and Gouvea [13], both citing Dieudonnè [11], it is proved that if $p \neq 2$ we can iteratively take the next α_n such that

$$\begin{aligned} \alpha_n &\equiv \alpha_{n-1} \mod p^n \\ \alpha_n^2 &\equiv \alpha \mod p^{n+1} \end{aligned}$$

Since $|\alpha_{n+1} - \alpha_n|_p = |kp^{n+1}|_p \leq p^{-(n+1)}$ tends to zero, by Lemma 1.25 (α_n) is Cauchy. But the same reasoning gives $|\alpha_{n+1} - \alpha|_p = |kp^{n+1}|_p \leq p^{-(n+1)}$ so the limit in $\mathbb{Q}$ would be a square root of α, which does not exist by construction. For $p = 2$, we do the same but with αcubic root of 3. See Gouvea [13]. □

It makes sense to try completing $\mathbb{Q}$ with respect to $|\cdot|_p$. We will force it to contain all limits of Cauchy sequences of elements in $\mathbb{Q}$. This will also be a completion with respect to all non-archimedean absolute values, since due to Ostrowski's theorem they are equivalent to one of the $|\cdot|_p$.

1.7 Analytical construction of $\mathbb{Q}_p$

On the completion of $\mathbb{Q}$ with p-adic norms. Construction and first properties.

Lemma 1.27 Consider a non-archimedean absolute value $|\cdot|_p$ on $\mathbb{Q}$ and define $\mathcal{C}_p(\mathbb{Q}) = \{(x_n) \text{ Cauchy sequence in } (\mathbb{Q}, |\cdot|_p)\}$. Then $\mathcal{C}_p(\mathbb{Q})$ is a commutative ring with unity with the usual operations

$$\begin{aligned} (\alpha_n) + (\beta_n) &= (\alpha_n + \beta_n) \\ (\alpha_n) \cdot (\beta_n) &= (\alpha_n \cdot \beta_n) \end{aligned}$$

Proof. Consider Lemma 1.25 for Cauchy sequences on non-archimedean norms,

$$\begin{aligned} |\alpha_{n+1}\beta_{n+1} - \alpha_n\beta_n|_p &= |\alpha_{n+1}\beta_{n+1} - \alpha_{n+1}\beta_n + \alpha_{n+1}\beta_n - \alpha_n\beta_n|_p \\ &= |\alpha_{n+1}(\beta_{n+1} - \beta_n) + \beta_n(\alpha_{n+1} - \alpha_n)|_p \\ &\leq \max\left\{|\alpha_{n+1}|_p |\beta_{n+1} - \beta_n|_p, |\beta_n|_p |\alpha_{n+1} - \alpha_n|_p\right\} \longrightarrow 0 \\ |(\alpha_{n+1} + \beta_{n+1}) - (\alpha_n + \beta_n)|_p &= |(\alpha_{n+1} - \alpha_n) + (\beta_{n+1} - \beta_n)|_p \\ &\leq \max\left\{|\alpha_{n+1} - \alpha_n|_p, |\beta_{n+1} - \beta_n|_p\right\} \longrightarrow 0 \end{aligned}$$

□

Lemma 1.28 Define $\mathcal{M} = \{(\alpha_n) : x_n \to 0\}$ set of sequences that tend to 0 in $(\mathbb{Q}, |\cdot|_p)$, $\mathcal{M}$ is a maximal ideal of $\mathcal{C}_p(\mathbb{Q})$.

Proof. This requires some arguments from analysis, see Gouvea [13]. □

Theorem 1.29 Consider $\mathbb{Q}_p$ as the quotient of rings

$$\mathbb{Q}_p = {}^{\mathcal{C}_p(\mathbb{Q})}/_{\mathcal{M}}$$

(i) This construction is equivalent to Definition 1.3.

(ii) The p-adic absolute value on $\mathbb{Q}$ naturally extends to $\mathbb{Q}_p$.

(iii) $\mathbb{Q}_p$ is a field, and there exists a strict inclusion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ acting as a natural field homomorphism.

(iv) $\mathbb{Q}_p$ is complete with respect to the p-adic norm.

Sketch of proof. Point (i) is proved like we did for Theorem 1.14.
Point (ii) is easy if we consider any $\alpha \in \mathbb{Q}_p$ as the limit of a Cauchy sequence (α_n) and $|\alpha|_p$ as the limit of $|\alpha_n|_p$, which converges by the same non-archimedean argument we exploited to prove Lemma 1.27.
Point (iii) follows immediately from the equivalent construction as quotient by a maximal ideal[4]. The field homomorphism associates to any $x \in \mathbb{Q}$ the sequence of terms $\alpha_n = \alpha$, which is Cauchy and only depends on x.
Proof of (iv) requires a multi-step approach and we leave it out.
See Gouvea [13] for more details. □

Corollary 1.30 Considering $\alpha \in \mathbb{Q}_p$ as a series of powers of p, the lowest index k such that $a_k \neq 0$ is $\nu_p(\alpha)$.

An interesting remark on the construction of $\mathbb{Q}_p$ is that it somewhat resembles that of $\mathbb{R}$, but vastly differs due to the choice of a non-archimedean absolute value. Ostrowski's Theorem 1.23 proves that any non-trivial non-archimedean absolute value is equivalent to a $|\cdot|_p$, so the two families of completions[5] are $\mathbb{R}$ and $\mathbb{Q}_p$. In its extravagant fashion, $\mathbb{Q}_p$ mimics the behaviour of $\mathbb{R}$.

(i) We are used to see elements of $\mathbb{R}$ in base 10:

$$x = a_n a_{n-1} \dots a_1 a_0 \,.\, a_{-1} a_{-2} a_{-3} \dots a_{-k} \dots$$

This kind of expansion is called **left-tailed**, as it is (eventually) finite on the left and infinite on the right. This is an arbitrary choice, as we can easily make them **right-tailed**:

$$1492.37 = 7 \times 10^{-2} + 3 \times 10^{-1} + 2 \times 10^{0} + 9 \times 10^{1} + 4 \times 10^{2} + 1 \times 10^{4}$$

The same can be said for $\mathbb{Q}_p$.

(ii) Taking the quotient by $\mathcal{M}$, we forced all sequences (α_n) and (β_n) whose difference $(\alpha_n) - (\beta_n)$ tends to zero to be identified. This is also done in real analysis, and is usually stated as "changing a finite number of term does not affect the behaviour of a sequence".

The metric space $\mathbb{Q}_p$ offers a few additional nightmares mainly due to the p-adic norm. Some are counter-intuitive but perfectly sound. We can conclude with a few considerations to further this claim and there will be more in the next section.

Proposition 1.31 $\mathbb{Q}_p$ is uncountable.

We already know that $\mathbb{Z}_p$ is uncountable and $\mathbb{Z}_p \subset \mathbb{Q}_p$, so this should be no surprise. The cardinal number of $\mathbb{Q}_p$ is greater than $\aleph_0$, exactly like $\mathbb{R}$.

Proposition 1.32 If p and q are distinct primes, $\mathbb{Q}_p$ is not isomorphic to $\mathbb{Q}_q$.

[4] It is of course a general fact that the completion of a field $\mathbb{K}$ with respect to some absolute value embeds the original $\mathbb{K}$ as a subfield.

[5] Plus $\mathbb{Q}$ itself for the trivial absolute value, which is not very interesting.

Sketch of proof. This requires some notions of group theory, see Serre's book [40]. The fundamental issue is that $|q|_p = 1$, as $|q|_p = p^{\nu_p(q)} \neq 1$ would imply $p \mid q$, hence by Lemma 1.19 we know q is an unit in $\mathbb{Z}_p$ but not in $\mathbb{Z}_q$. This of course generalises to all other units, and finally to the group of units. □

Lemma 1.33 $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ under p-adic absolute value.

Proof. Consider (α_n) sequence of integers, by definition they all have p-adic absolute value $|\alpha_n|_p \leq 1$. Consider α their limit, we know it lies in $\mathbb{Q}_p$ since $\mathbb{Z} \subset \mathbb{Q}$. Pick an x_n such that $|\alpha - \alpha_n|_p < 1$, which exists since x is their limit. Then α is a p-adic integer, since

$$|\alpha|_p = |\alpha_n - (\alpha - \alpha_n)|_p \leq \max\left\{|\alpha_n|_p, |\alpha - \alpha_n|_p\right\} \leq 1$$ □

1.8 Structure of $\mathbb{Q}_p$ as field

On the algebraic properties of the field of p-adic numbers and its elements. Relations with p-adic integers.

Remark that $\mathbb{Q}_p$ is a local field which is an infinite extension of $\mathbb{Q}$. It contains a copy of $\mathbb{Z}$, so the ring morphism $\mathbb{Z} \to \mathbb{Q}_p$ is the inclusion and its kernel is 0, meaning that $\mathbb{Q}_p$ has characteristic zero. It is only fair to wonder whether $\mathbb{Q}_p$ is a number field or not.

Definition 1.34 A field $\mathbb{K}$ is called **(algebraic) number field** if it is an extension of $\mathbb{Q}$ of finite degree, i.e. it is a field containing $\mathbb{Q}$ and a finite-dimensional vector $\mathbb{Q}$-space.

Proposition 1.35 The field of p-adic numbers $\mathbb{Q}_p$ is not a number field.

Proof. Assume the extension is finite and algebraic of degree k, with $\mathcal{B}$ basis for $\mathbb{Q}_p$ over $\mathbb{Q}$. Since $\mathbb{Q}$ is infinite countable, $\mathbb{Q}$-linear combinations of elements of $\mathcal{B}$ can express a countable amount of elements. But $\mathbb{Q}_p$ is uncountable. □

With a number field, e.g. $\mathbb{Q}[\sqrt{3}]$, we would usually proceed describing its ring of integers. Luckily that theory can be generalised.

Definition 1.36 The **ring of integers** over a non-archimedean local field $(\mathbb{K}, |\cdot|)$ is the set of elements with absolute value $|k| \leq 1$.

$$\mathcal{O}_{\mathbb{K}} = \{k \in \mathbb{K} : |k| \leq 1\}$$

Then $\mathcal{O}_{\mathbb{K}}$ is a ring with respect to the same operations of $\mathbb{K}$: 0 and 1 lie in $\mathcal{O}_{\mathbb{K}}$, and with the strict triangle inequality of Definition 1.6

$$|k_1 + k_2| \leq \max\{|k_1|, |k_2|\} \leq 1$$
$$|k_1 k_2| \leq |k_1|\,|k_2| \leq 1$$

Lemma 1.37 The ring of integers of the field $\mathbb{Q}_p$ is $\mathbb{Z}_p$.

This justifies the name of $\mathbb{Z}_p$ and "p-adic integers", which arise from a comparison with the integers of number fields.
We also know that $\mathbb{Q}_p$ properly contains $\mathbb{Z}_p$. With the equivalence relation

$$(a,n) \sim (b,m) \iff am = bn$$

on $\mathbb{Z}_p$, the quotient ${}^{\mathbb{Z}_p \times \mathbb{Z}_p}/_{\sim}$ with the usual fractionary operations is $\mathrm{Frac}(\mathbb{Z}_p)$. We represent its elements as $\frac{a}{m}$.

Theorem 1.38 The field of fractions $\mathrm{Frac}(\mathbb{Z}_p)$ of the ring $\mathbb{Z}_p$ is $\mathbb{Q}_p$.

Proof. An element in $\mathrm{Frac}(\mathbb{Z}_p)$ has form $\frac{r}{s}$ for $r, s \in \mathbb{Z}_p$. From point (ii) of Lemma 1.19 we know that $s = up^k$ for u invertible in $\mathbb{Z}_p$ and $k \geq 0$, therefore

$$\frac{r}{s} = \frac{r}{up^k} = \frac{u^{-1}r}{p^k} = \frac{\sum_{j=0}^{+\infty} a_j p^j}{p^k} = \sum_{j=0}^{+\infty} a_j p^{(j-k)} = \sum_{i=-k}^{+\infty} a_{i+k} p^i$$

where we expanded the p- adic integer $u^{-1}r$. Given an element of $\mathbb{Q}_p$ we can proceed backwards to obtain an element of $\mathrm{Frac}(\mathbb{Z}_p)$. □

This can be seen as the localisation of $\mathbb{Z}_p$ at the subring of its non-zerodivisors, which is usually defined as a **total quotient ring**. Remark that $\mathbb{Z}_p$ is an integral domain.
We can generalise a previous lemma.

Theorem 1.39 Any $r \in \mathbb{Q}_p$ can be written as $r = up^e$ where u is a p-adic integer of unitary norm.

Proof. If $|r|_p = p^{-e} \neq 1$, then p^e divides r and we can write $u = {}^r/_{p^e}$. By definition no non-trivial power of p can divide u, which has unitary norm. Moreover u lies in $\mathbb{Z}_p$ by defnition of $\mathbb{Z}_p$. □

Proposition 1.40 $\mathbb{Q}_p$ is not algebraically closed. The algebraic closure $\overline{\mathbb{Q}_p}$ has infinite degree over $\mathbb{Q}$ and is not complete.

Proof. See for example Schikhof [38], which exploits Baire's theorem [3]. □

Hence $\mathbb{Q}_p$ has infinitely many inequivalent proper extensions, unlike $\mathbb{R}$ which is not closed but has a single proper extension $\mathbb{C} \simeq \mathbb{R}[i]$ complete and of degree two. As a final example and warning, consider the following.

Proposition 1.41 $\mathbb{Q}_p$ is an unordered field.

Sketch of proof. If we assume that $\mathbb{Q}_p$ contains a square root of $1 - p$, which we will prove later with Hensel's lemma, we can write in $\mathbb{Q}_p$

$$(1-p) \times 1^2 + 1 \times (\sqrt{1-p})^2 = 0$$

and from Rajwade's book [32] we know that if a null weighted sum of squares has non-zero weights then the field is unordered. □

This of course breaks most approaches to p-adic numbers. For instance, they cannot be constructed with a Dedekind-like approach to rationals.

1.9 Rational numbers in $\mathbb{Q}_p$

On the expression of rational numbers as p-adic numbers. Relation with periodic expansions.

We can concede ourselves the luxury of a brief excursion in this new exotic space. Theorem 1.29 says that $\mathbb{Q}$ is somewhat contained in $\mathbb{Q}_p$, not per se but as image of the inclusion map. So of course we do not expect $\mathbb{Q}_p$ to contain *exactly* $\mathbb{Q}$, only some sequences representing it. In a previous example we showed that $r = 2 + 0p + 1p^2 + 0p^3 + 1p^4 + 0p^5 + 1p^6 + \cdots = 7/8$ in $\mathbb{Q}_3$. It is no coincidence that the digits of r eventually repeat.

Definition 1.42 A sequence (a_n) is said **purely periodic (of period r)**, or purely periodic (of period k), if for any n we have $a_{n+k} = a_n$. Sometimes in the definition the r is dropped. The sequence is said **(eventually) periodic (of period k)** if it is purely periodic after ignoring some finite number of terms at the beginning.

The periodic behaviour of $7/8$ in $\mathbb{Q}_3$ is strictly tied to its value in $\mathbb{Z}$. A nice feature of $\mathbb{Q}_p$ is that one can exchange the negative sign for a different right-tailed expansion. It is not hard to prove that $s = -r = 1 + 2p + 1p^2 + 2p^3 + \ldots$. We will give some results by Conrad [10] that will get us used to periodicity in $\mathbb{Q}_p$.

Theorem 1.43 Consider r a rational number with unitary p-adic absolute value. The following are equivalent

(i) r has a periodic expansion in $\mathbb{Q}_p$

(ii) $r \in [-1, 0)$ in $\mathbb{Q}$

Proof. Assume (i). Then $v_p(r) = 0$, meaning that the expansion of period k is

$$\begin{aligned} r &= n_0 + n_1 p^1 + n_2 p^2 + \cdots + n_{k-1} p^{k-1} + n_0 p^k + n_1 p^{k+1} + \ldots \\ &= \left(n_0 + \cdots + n_{k-1} p^{k-1}\right) + p^k \left(n_0 + \cdots + n_{k-1} p^{k-1}\right) + p^{2k} \left(n_0 + \cdots + n_{k-1} p^{k-1}\right) + \ldots \\ &= \left(n_0 + \cdots + n_{k-1} p^{k-1}\right) \left(1 + p^k + p^{2k} + p^{3k} + \ldots\right) \\ &= \sum_{i=0}^{+\infty} \left(n_0 + \cdots + n_{k-1} p^{k-1}\right) p^{ik} = \frac{n_0 + \cdots + n_{k-1} p^{k-1}}{1 - p^k} \end{aligned}$$

Remark that $n_0 \neq 0$ because the valuation of r is zero. This means that due to the choice of representatives the numerator is an integer between 1 and $(p-1) + (p-1)p + \cdots + (p-1)p^{k-1} = p^k - 1$, so (ii) follows.
Assume (ii) instead. We can write $r = a/b$ with $a < 0$ and $b \geq 1$ both not divisible by p and coprime. Since $\gcd(p, b) = 1$ there is some k such that[6] $p^k \equiv 1 \mod b$, so $p^k = 1 + bb'$ for some positive integer b' and

$$r = \frac{a}{b} = \frac{ab'}{bb'} = \frac{-ab'}{1 - p^k}$$

[6]This procedure does not depend on the minimality of k, which only ensures that the length of the periodic part of the expansion is minimal.

Since $a < 0$ and $b' > 0$, $-1 \leq {}^{-ab'}/_{1-p^k} < 0$, then $0 < -ab \leq p^k - 1$ and $-ab$ has at most k digits in base p, so $-ab' = n_0 + \cdots + n_{k-1}p^{k-1}$ for some n_i.

$$\begin{aligned} r = \frac{a}{b} &= \frac{-ab'}{1-p^k} = \frac{n_0 + \cdots + n_{k-1}p^{k-1}}{1-p^k} = \sum_{i=0}^{+\infty} \left(n_0 + \cdots + n_{k-1}p^{k-1}\right) p^{ik} \\ &= \left(n_0 + \cdots + n_{k-1}p^{k-1}\right)\left(1 + p^k + p^{2k} + p^{3k} + \dots\right) \\ &= \left(n_0 + \cdots + n_{k-1}p^{k-1}\right) + p^k\left(n_0 + \cdots + n_{k-1}p^{k-1}\right) + p^{2k}\left(n_0 + \cdots + n_{k-1}p^{k-1}\right) + \dots \\ &= n_0 + n_1p^1 + n_2p^2 + \cdots + n_{k-1}p^{k-1} + n_0p^k + n_1p^{k+1} + \dots \end{aligned}$$

□

We can see that ${}^{-7}/_8$ in $\mathbb{Q}$ satisfies these hypotheses, and since (ii) holds then its expansion in $\mathbb{Q}_3$ must be periodic. The theorem also gives a way to calculate its expansion. Since $a = -7$ and $b = 8$, the smallest k such that $3^k \equiv 1 \mod 8$ is $k = 2$, with $3^2 = 1 \times 8 + 1$, we know that $k = 2$ and $b' = 1$. Finally,

$$\begin{aligned} s = -\frac{7}{8} &= -\frac{7 \times 1}{8 \times 1} = -\frac{7}{p^2-1} = \frac{7}{1-p^2} = \frac{1+2p}{1-p^2} = \sum_{i=0}^{+\infty} (1+2p)\, 3^{2k} \\ &= (1+2p)\left(1 + p^2 + p^4 + \dots\right) = (1+2p) + (1+2p)\, p^2 + (1+2p)\, p^4 + \dots \end{aligned}$$

This theorem must first be generalised to work with $r = -s = {}^7/_8$.

Theorem 1.44 Any number in $\mathbb{Q}_p$ has an eventually periodic expansion if and only if is a rational. Here we allow for integers to be considered periodic[7].

Proof. Step 1. Any periodic expansion $x = m_0m_1 \dots m_{j-1}\overline{n_0 \dots n_{k-1}}$ represents a rational, where j is the pre-period. A purely periodic expansion would have $j = 0$. This represents a rational number for the same reasoning as before.

$$\begin{aligned} x &= m_0m_1 \dots m_{j-1}\overline{n_0 \dots n_{k-1}} \\ &= m_0 + \cdots + m_{j-1}p^{j-1} + p^j\left(n_0 + \cdots + n_{k-1}p^{k-1}\right) + p^{j+k}\left(n_0 + \cdots + n_{k-1}p^{k-1}\right) + \dots \\ &= \left(m_0 + \cdots + m_{j-1}p^{j-1}\right) + p^j\left(n_0 + \cdots + n_{k-1}p^{k-1}\right)\left(1 + p^k + p^{2k} + p^{3k} + \dots\right) \\ &= \left(m_0 + \cdots + m_{j-1}p^{j-1}\right) + p^j \sum_{i=0}^{+\infty}\left(n_0 + \cdots + n_{k-1}p^{k-1}\right) p^{ik} \\ &= \left(m_0 + \cdots + m_{j-1}p^{j-1}\right) + p^j \frac{n_0 + \cdots + n_{k-1}p^{k-1}}{1-p^k} \end{aligned}$$

Step 2. We can work in $\mathbb{Z}_p$ without loss of generality: if $x \notin \mathbb{Z}_p$, define $y = p^e x$ with a large enough e and work on y. Then divide by p^e, which is just a shift. In other words, we extend our definition of periodicity to account for shifts of the sequence. They do not affect its behaviour.

Step 3. Consider the converse for a strictly negative integer x. Pick a j such that $0 < -x < p^j$ and write $y = -x$. We have $x = -y = \left(p^j - y\right) - p^j$ where $p^j - y$ is

[7] Remark that an integer in $\mathbb{Q}_p$ is eventually finite. Due to Definition 1.42, this is a periodic expansion with repeating zeroes

a positive integer not greater than p^j, so it has j digits $m_0, \dots, m_{j-1}$ in base p. Then x is eventually periodic,

$$x = \sum_{i=0}^{j-1} m_i p^i - p^j = \sum_{i=0}^{j-1} m_i p^i + \sum_{i=j}^{+\infty} (p-1) p^i$$

Step 4. Consider the converse for a negative rational x in $(-1, 0)$ of non-unitary p-adic norm and $e = \nu_p(x) \neq 0$ lying in $\mathbb{Z}_p$. We already know that this holds for negative rationals in $(-1, 0)$ of unitary norm, so we can factor out p from x and get $y = {}^{x}/_{p^e}$ rational of unitary absolute value lying in $({}^{-1}/_{p^e}, 0) \subset (-1, 0)$. Since y has a purely periodic expansion in $\mathbb{Q}_p$, x also has one. They have the same periodic part, just shifted right by e digits.

Step 5. Consider the converse for a negative rational less than -1 and not in $\mathbb{Z}$ lying in $\mathbb{Z}_p$. We can still find two consecutive integers such that $-N - 1 < x < -N$, so we have that $-1 < x + N < 0$. The expansion of $x + N$ is periodic due to step 3, but it could be eventually periodic depending on $\nu_p(x + N)$. In short, the expansion has form $x + N = a_0 + a_1 p + a_2 p^2 + \dots$ and becomes arbitrarily large[8], so we eventually find a j such that

$$a_0 + a_1 p + a_2 p^2 + \cdots + a_{j-1} p^{j-1} > N$$

Pick the smallest such j, a_j is non-zero.

$$x + N = \left(a_0 + a_1 p + a_2 p^2 + \cdots + a_{j-1} p^{j-1}\right) + \sum_{i=j}^{+\infty} a_i p^i$$

$$x = \left(a_0 + a_1 p + a_2 p^2 + \cdots + a_{j-1} p^{j-1} - N\right) + \sum_{i=j}^{+\infty} a_i p^i$$

Now we need to tweak it a little. The part between brackets is a positive integer upper-bounded by $p^j - 1$ by construction, so it can be written in base p and has at most j digits. Finally, we get

$$x = \left(b_0 + b_1 p + b_2 p^2 + \cdots + b_{j-1} p^{j-1}\right) + \sum_{i=j}^{+\infty} a_i p^i$$

which is still eventually periodic because the right part is unchanged.

Step 6. If x is positive, we can use a previous case on $y = -x$. By multiplying for -1, which is trivially periodic, we get an eventually periodic expansion. □

We already remarked that the proof of Theorem 1.43 gives us an algorithm, just not suitable for all rational numbers. The proof of Theorem 1.44 helps us generalise it to any rational x.

1.10 Square roots in $\mathbb{Q}_p$

On Hensel's lemma for the gradual approximation of polynomial solutions.

[8] In the usual sense! Not as an expansion.

In $\mathbb{R}$, the square root of r can be defined as the set of solutions of $x^2 - r$ in $\mathbb{R}$. When r is positive there are two solutions, when r is negative there is none. The **square root of N in $\mathbb{Q}_p$** is the set of solutions of $x^2 - r$ in $\mathbb{Q}_p$.
In the following, p will be an odd prime: in the examples, $p = 7$. The theory can be extended to $P = 2$, but in the next chapter we will only work on odd primes. Consider for example $r = 2$. Instead of solving directly, let us *successively approximate* it. This is equivalent to solving the set of congruences modulo 7^n

$$x^2 \equiv 2 \mod p^n$$

($n = 1$) Since 2 has Legendre symbol 1 it is a quadratic residual modulo 7, and the equation has two solutions. Both $x = 3$ and $x = 4$ satisfy it.

($n = 2$) We need to "lift" the solutions we found, meaning that they need to be evaluated modulo 49 instead of modulo 7. From $x \equiv 3 \mod 7$, we are trying to set $x = 3 + 7k$ and solve for k. Thus

$$x^2 = (3 + 7k)^2 = 9 + 42k + 49k^2 \equiv 2 \mod 49$$

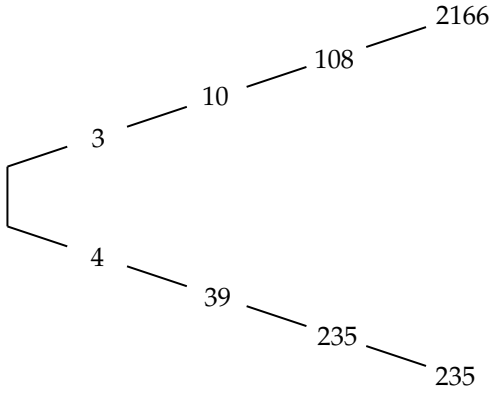
and it is easy to see that it only has solution $x \equiv 10 \mod 49$ for $k = 1$. Similarly, from $x \equiv 4 \mod 7$ we solve for k and get $x \equiv -10 \equiv 39 \mod 49$.

($n = 3$) Lifting again we get respectively 108 and 235 modulo 343.

This can be generalised. We are building two p-coherent sequences of integers of solutions (α_n) and (β_n) that still satisfy the congruence while going forward: $\alpha_{n+1} \equiv \alpha_n \mod p^n$. To turn a p-coherent sequence into the expansion of a p-adic integer, just expand in base p.

$$\begin{aligned}
&\alpha_1 = 3 && \beta_1 = 4 \\
&\alpha_2 = 10 = 3 + 1p && \beta_2 = 39 = 4 + 5p \\
&\alpha_3 = 108 = 3 + 1p + 2p^2 && \beta_3 = 235 = 4 + 5p + 4p^2 \\
&\alpha_4 = 2166 = 3 + 1p + 2p^2 + 6p^3 && \beta_4 = 235 = 4 + 5p + 4p^2 + 0p^3
\end{aligned}$$

Since the square root of two is well-known to be irrational, we also know that this expansion cannot be eventually periodic due to Theorem 1.44. In Gouvea [13], p-coherent sequences are visually represented by the following diagram.



Notice the choice of words: "iteratively solve". This kind of procedure is close to Newton's method. In $\mathbb{R}$, the roots of $f(x) = x^2 - r$ can be approximated fixing an initial x_0 and iteratively computing

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$$

until a satisfying value is reached. Convergence is quadratic under certain conditions. Here $f'(x)$ represents the usual derivative from analysis.
For example, with $f(x) = x^2 - 2$ and $x_0 = 5$,

step n	x_n	error
$n = 0$	$x_0 = 5.00$	-
$n = 1$	$x_1 = 2.70$	2.30
$n = 2$	$x_2 = 1.72$	0.98
$n = 3$	$x_3 = 1.44$	0.28

This heavily depends on floating point precision[9]. One must be careful, as $f(x) = x^2 + 1$ is always positive and the method does not converge. In $\mathbb{Q}_p$ this is more delicate.

Definition 1.45 Consider $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a^4x^4 + \dots$ polynomial in $R[x]$ for a generic ring R. Then its **formal derivative** is the polynomial

$$f'(x) = a_1 + 2a_2x + 3a_3x^2 + \dots$$

Theorem 1.46 (Hensel's Lemma) Consider $f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots$ polynomial in $\mathbb{Z}_p[x]$, suppose there exists a p-adic integer α_1 such that

(i) $f(\alpha_1) \equiv 0 \mod p\mathbb{Z}_p$
(ii) $f'(\alpha_1) \not\equiv 0 \mod p\mathbb{Z}_p$

There exists an unique p-adic integer α that is root of f and $\alpha \equiv \alpha_1 \mod p\mathbb{Z}_p$.

Proof. We will provide a p-coherent sequence of integers (α_n) and prove that α can be defined as its limit. Remark that in $\mathbb{Z}_p$ we have the chain of ideals

$$\mathbb{Z}_p = (1) \supset (p) \supset (p^2) \supset (p^3) \supset (p^4) \supset \dots \supset (p^k) \supset \dots$$

Given α_1, consider α_2 of form $\alpha_2 = \alpha_1 + k_1p$ for some p-adic integer k_1. This is what we did before, and we will again substitute in f to obtain an expression of α_2. Keep in mind that this does not depend on the index of α_2.

$$\begin{aligned}
f(\alpha_2) = f(\alpha_1 + k_1p) &= a_0 + a_1(\alpha_1 + k_1p) + a_2(\alpha_1 + k_1p)^2 + a_3(\alpha_1 + k_1p)^3 \\
&= a_0 + a_1(\alpha_1 + k_1p) + a_2\left(\alpha_1^2 + 2\alpha_1k_1p + k_1^2p^2\right) + a_3\left(\alpha_1^3 + 3\alpha_1^2k_1p + O(p^2)\right) + \dots \\
&= f(\alpha_1) + a_1(k_1p) + a_2\left(2\alpha_1k_1p + k_1^2p^2\right) + a_3\left(3\alpha_1^2k_1p + O(p^2)\right) + \dots \\
&= f(\alpha_1) + f'(\alpha_1)k_1p + a_2\left(k_1^2p^2\right) + a_3\left(O(p^2)\right)^3 + \dots \\
&\equiv f(\alpha_1) + f'(\alpha_1)k_1p \mod p^2
\end{aligned}$$

[9]Interestingly enough, p-adic numbers can sometimes be exploited to obtain error-free and precise arithmetic. See Abrahamis introduction [1].

If we manage to find k_1 such that the right hand side is zero, we also found α_2. From (i) we have that $f(\alpha_1) \equiv 0 \mod p$, so $f(\alpha_1) \equiv bp$ for some b. Then

$$pb + f'(\alpha_1)k_1 p \equiv 0 \mod p^2$$

$$b + f'(\alpha_1)k_1 \equiv 0 \mod p$$

$$k_1 \equiv -b\left(f'(\alpha_1)\right)^{-1} \mod p$$

where $f'(\alpha_1)$ is not divisible by p, hence is invertible in $\mathbb{Z}_p$ having unitary norm. Set $\alpha_2 = \alpha_1 + k_1 p$, we can repeat the procedure because it also satisfies (i) and (ii). The sequence we get is Cauchy by Lemma 1.25 and its limit α lies in $\mathbb{Z}_p$, the completion of $\mathbb{Z}$ under $|\cdot|_p$. The limit will also satisfy (i) by continuity and (ii) by construction. □

This is analogous to Newton's method. In fact, we could state it as

Corollary 1.47 Consider $f(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots$ polynomial in $\mathbb{Z}_p[x]$, suppose there exists a p-adic integer α_1 such that

(i) $|f(\alpha_1)|_p < 1$
(ii) $|f'(\alpha_1)|_p = 1$

then we can define a convergent sequence (α_n) by setting

$$\alpha_{n+1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$$

whose limit x is the unique p-adic integer such that $|x - \alpha_1| < 1$ and $f(\alpha) = 1$.

Proof. Substituting in the equation

$$\alpha_{n+1} = \alpha_n - x f(\alpha_n)\left(f'(\alpha_1)\right)^{-1} p = \alpha_n - \frac{f(\alpha_n)p}{p}\left(f'(\alpha_1)\right)^{-1} = \alpha_n - \frac{f(\alpha_n)}{f'(\alpha_n)}$$

and the rest is just rewriting the properties exploiting $|\cdot|_p$. □

There are some differences. For example, the procedure never leaves $\mathbb{Z}_p$ and always works. We also get much more information on α. Consider again $f(x) = x^2 - 2$ in $\mathbb{Q}_7$ with $f'(x) = 2x$. Focus on the first branch of solutions (those with $\alpha_1 = 3$).

$$\alpha_2 = 3 - \frac{7}{6} = \frac{11}{6} \equiv (11 \times 41) \equiv 10 \mod 7^2$$
$$\alpha_3 = 10 - \frac{98}{20} = \frac{51}{10} \equiv (51 \times 103) \equiv 108 \mod 7^3$$

and so on. We can formalise something we used to prove Proposition 1.41.

Corollary 1.48 The polynomial $f(x) = x^2 - (1 - p)$ has solutions in $\mathbb{Q}_p$.

Proof. By definition, $\sqrt{1-p}$ lies in $\mathbb{Z}_p$ if and only if $f(x) = x^2 - r$ has solutions modulo p, i.e. $1 - p$ must be a quadratic residue modulo p. But $1 - p \equiv 1 \mod p$, so $1 - p$ has Legendre symbol +1. □

In $\mathbb{R}$, having $f(x) = x^2 - r$ for a negative r immediately told us there were no real solutions. The equivalent remark in $\mathbb{Z}_p$ is that if r is not a quadratic residual there is no solution modulo p.

Lemma 1.49 Assume $p \neq 2$. If $a_1^2 \equiv u \mod p\mathbb{Z}_p$ for some p-adic integer a_1 and p-adic integral unit $u \in \mathbb{Z}_p^\times$, then u is the square of an unit $v \in \mathbb{Z}_p^\times$.

Proof. Consider $f(x) = x^2 - u$. Then $f(a_1) \equiv 0$ and $f'(a_1) = 2a_1 \not\equiv 0$ modulo $p\mathbb{Z}_p$ since $p \neq 2$. The solution is an unit, $v^2 = u$ implies $|v|_p^2 = |u|$. □

Lemma 1.50 Assume $p \neq 2$.

(i) An $a \in \mathbb{Q}_p$ is a square if and only if $a = p^{2n}u^2$ for $n \in \mathbb{Z}$, $u \in \mathbb{Z}_p^\times$.

(ii) The quotient group $\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2$ has order four. If $\gamma \in \mathbb{Z}_p^\times$ is any unit whose reduction modulo p is not a quadratic residue, then the set $\{1, p, \gamma, \gamma p\}$ is a complete set of representatives.

Proof. If $a = p^{2n}u^2$ for $u \in \mathbb{Z}_p^\times$ then it is a square. Assume a is a square, hence $a = (\gamma)^2$ for some γ. Remark that any $\gamma \in \mathbb{Q}_p$ can be written as

$$\gamma = p^{v_p(\gamma)}v_a \text{ for } v_a \text{ invertible in } \mathbb{Z}_p$$

therefore

$$a = (\gamma)^2 = \left(p^{v_p(\gamma)}v_\gamma\right)^2 = p^{2v_p(\gamma)}v_\gamma^2$$

For (ii), consider the cosets of $(\mathbb{Q}_p^\times)^2$ in $\mathbb{Q}_p^\times$ induced by γ non-square unit.

$$\begin{aligned}
1 \cdot (\mathbb{Q}_p^\times) &= \left\{a \in \mathbb{Q}_p^\times : a = 1 \cdot \beta^2 = p^{2v_p(\beta)}v_\beta^2 \text{ for some } \beta \in \mathbb{Q}_p^\times\right\} \\
1p \cdot (\mathbb{Q}_p^\times) &= \left\{a \in \mathbb{Q}_p^\times : a = 1p \cdot \beta^2 = p^{2v_p(\beta)+1}v_\beta^2 \text{ for some } \beta \in \mathbb{Q}_p^\times\right\} \\
\gamma \cdot (\mathbb{Q}_p^\times) &= \left\{a \in \mathbb{Q}_p^\times : a = \gamma \cdot \beta^2 = p^{2v_p(\beta)}\gamma v_\beta^2 \text{ for some } \beta \in \mathbb{Q}_p^\times\right\} \\
\gamma p \cdot (\mathbb{Q}_p^\times) &= \left\{a \in \mathbb{Q}_p^\times : a = \gamma p \cdot \beta^2 = p^{2v_p(\beta)+1}\gamma v_\beta^2 \text{ for some } \beta \in \mathbb{Q}_p^\times\right\}
\end{aligned}$$

Any a is not a square if it has odd valuation (due to the first point), non-square unitary part (Lemma 1.49) or both. These sets form a partition $(\mathbb{Q}_p^\times)^2$. □

1.11 Representation of elements of $\mathbb{Q}_p$

On the form of p-adic integers under a different set of representatives.

We will conclude with the generalisation of Problem 1 and Problem 2 from $\mathcal{A} = \{0, \ldots, p-1\}$ to any other set of representatives. We can operate exactly like in modular arithmetic, and this is induced by the structure of $\mathbb{Z}_p$.

Lemma 1.51 $\mathbb{Z}/p^k\mathbb{Z} \simeq \mathbb{Z}_p/p^k\mathbb{Z}_p$

Proof. Consider the map

$$\begin{aligned} f : \mathbb{Z}_p &\longrightarrow \mathbb{Z}_p \\ \alpha &\longmapsto \alpha p^k \end{aligned}$$

$$\begin{aligned} \ker(f) &= \left\{ a_0 + a_1 p + a_2 p^2 + \cdots \in \mathbb{Z}_p : 0 = a_0 p^k + a_1 p^{k+1} + a_2 p^{k+2} + \dots \right\} \\ &= \left\{ 0 + 0p + 0p^2 + \cdots \in \mathbb{Z}_p \right\} = \{0\} \\ \mathrm{im}(f) &= \left\{ \alpha \in \mathbb{Z}_p : \alpha = f(\beta) \text{ for some } \beta \text{ in } \mathbb{Z}_p \right\} = p^k \mathbb{Z}_p \end{aligned}$$

A sequence of ring morphisms $D \xrightarrow{f} E \xrightarrow{g} F$ is **exact** if $\mathrm{im}(f) = \ker(g)$. Starting from f, we seek for a map g and ring F such that $\ker(g) = p^k \mathbb{Z}_p$ and $\mathrm{im}(g) \subseteq F$.

$$\begin{aligned} g =: \mathbb{Z}_p &\longrightarrow \mathbb{Z}/p^k\mathbb{Z} \\ \alpha = \sum_{i=0}^{+\infty} a_i p^i &\longmapsto \sum_{i=0}^{k-1} a_i p^i \end{aligned}$$

$$\begin{aligned} \ker(g) &= \left\{ \alpha = \sum_{i=0}^{+\infty} a_i p^i \in \mathbb{Z}_p : 0 = a_0 + a_1 p^1 + a_2 p^2 + \cdots + a_{k-1} p^{k-1} \right\} \\ &= \left\{ 0 + 0p + \cdots + 0p^{k-1} + a_k p^k + \cdots \in \mathbb{Z}_p \right\} = p^k \mathbb{Z}_p \\ \mathrm{im}(g) &= \left\{ m \in \mathbb{Z}/p^k\mathbb{Z} : m = g(\beta) \text{ for some } \beta \text{ in } \mathbb{Z}_p \right\} = \mathbb{Z}/p^k\mathbb{Z} \end{aligned}$$

With this choice, the sequence is exact. Now construct

$$0 \xrightarrow{i} \mathbb{Z}_p \xrightarrow{f} \mathbb{Z}_p \xrightarrow{g} \mathbb{Z}/p^k\mathbb{Z} \xrightarrow{p} 0$$

where i is inclusion and p is projection to zero. This sequence is short (meaning it has five components) and exact in each step. Applying the isomorphism theorem of rings on g, since $\mathrm{im}(g) = \ker(p)$ and $\ker(g) = \mathrm{im}(f)$,

$$\begin{aligned} \mathbb{Z}_p/\ker(g) &\simeq \mathrm{im}(g) \\ \mathbb{Z}_p/p^k\mathbb{Z}_p &\simeq \mathbb{Z}/p^k\mathbb{Z} \end{aligned}$$

□

Theorem 1.52 (Invariance under representatives) Consider a set of representatives $\mathcal{A} \subset \mathbb{Z}_p$ of $\mathbb{Z}/p\mathbb{Z}$. Any $\alpha \in \mathbb{Q}_p$ can be uniquely written as

$$\alpha = \sum_{i=-k}^{+\infty} a_i p^i$$

where each coefficient a_i is an element of $\mathcal{A}$ and $-k = \nu_p(\alpha)$.

Proof. Assume $\alpha \in \mathbb{Z}_p$.
Find the unique representative a_0 in $\mathcal{A}$ such that $\alpha - a_0 \in \mathbb{Z}/p\mathbb{Z}$. Remark that $\mathbb{Z}/p\mathbb{Z} \simeq \mathbb{Z}_p/p\mathbb{Z}_p$, so $\alpha - a_0 = p\beta_1$ for some $\beta \in \mathbb{Z}_p$.
Find the unique representative a_1 in $\mathcal{A}$ such that $\beta_1 - a_1 \in \mathbb{Z}/p\mathbb{Z}$, so $\beta_1 - a_1 = p\beta_2$

for some $\beta \in \mathbb{Z}_p$. Proceed iteratively. If we stop at step n we find sequences $a_0, a_1, \ldots, a_n$ and $\alpha, \beta_1, \ldots, \beta_{n-1}$ such that

$$\begin{aligned} \alpha &= a_0 + a_1 p + a_2 p^2 + \cdots + p^{n-1}\beta_{n-1} \\ \nu_p\left[\alpha - \left(a_0 + a_1 p + a_2 p^2 + \cdots + p^{n-1}\beta_{n-1}\right)\right] &\geq n-1 \\ \left|\alpha - \left(a_0 + a_1 p + a_2 p^2 + \cdots + p^{n-1}\beta_{n-1}\right)\right| &\leq p^{-(n-1)} \end{aligned}$$

so the series converges in $\mathbb{Z}_p$ by Lemma 1.33, and indeed converges to α.
If $\alpha \notin \mathbb{Z}_p$ it suffices to multiply by $p^{\nu_p(\alpha)}$, expand as before, and then divide by $p^{\nu_p(\alpha)}$ to get the same result. □

We will usually switch between the two following complete sets of representatives of $\mathbb{Z}/p\mathbb{Z}$,

$$\mathcal{A} = \{0, \ldots, p-1\} \qquad\qquad \mathcal{B} = \left\{-\frac{(p-1)}{2}, \ldots, +\frac{(p-1)}{2}\right\}$$

Consider $\alpha \in \mathbb{Q}_p$. First remark that $\mathcal{A} \cap \mathcal{B}$ is non-empty so not all representatives need to be discarded. Start from the first non-zero coefficient, the one with index $i = \nu_p(\alpha)$. If $a_i \notin \mathcal{B}$ then $a_i \geq {}^{p-1}/_2$. But if we substitute a_i with

$$a_i = -(p - a_i) + p$$

the value of α does not change. Denoting this as $a_i = a_i' + p$, the old $(i+1)$-th coefficient is increased by 1 and the new i-th coefficient $a_i' = -(p - a_i)$ satisfies

$$\begin{array}{ccccc} \dfrac{p-1}{2} & < & a_i & \leq & p-1 \\ \dfrac{-1-p}{2} & < & -(p-a_i) & \leq & -1 \\ -\dfrac{(p-1)}{2} & \leq & -(p-a_i) & \leq & -1 \end{array}$$

Consider for example $\alpha = 2 + 2p + 2p^2$ in $\mathbb{Q}_3$. The first non-zero entry of α is indexed by $\nu_p(\alpha) = 0$ and is $a_0 = 2$. It does not lie in $\mathcal{A} \cap \mathcal{B} = \{0, 1\}$, so we set it to $a_0' = -1$ and increase a_1.

$$\begin{aligned} \alpha &= 2 + 2p + 2p^2 = (-(p-2) + p) + 2p + 2p^2 \\ &= -1 + 3p + 2p^2 = -1 + 3p^2 = -1 + 1p^3 \end{aligned}$$

The steps can be visualised as follows.

a_0	a_1	a_2	a_3
2	2	2	0
–1	0	0	1
-1	**0**	0	1
-1	0	**0**	1
-1	0	0	**1**

Consider $\alpha = 0 + 1p + 2p^2 + 1p^3$. The first non-zero entry has index $\nu_p(\beta) = 1$ but lies in $\mathcal{B}$, so we step over to $a_2 \notin \mathcal{B}$ and iteratively proceed as before.

a_0	a_1	a_2	a_3	a_4
0	1	2	1	0
0	**1**	2	1	0
0	1	**2**	1	0
0	1	**−1**	2	0
0	1	−1	**2**	0
0	1	−1	**−1**	1
0	1	−1	−1	**1**

It is easy to see that the value of α is unchanged. Also notice how we might need an additional element to accommodate an eventual carry-over.

Chapter 2

Continued fractions in $\mathbb{R}$

Mathematics shows up in the most unexpected places. In 1202, Italian mathematician Leonardo Fibonacci proposed a problem in his *Liber Abaci* ("Book of Calculation", [12]), that can be summarised as:

> *"A man placed a pair of rabbits in some place completely surrounded by a wall, find out how many pairs of rabbits would descended from them in one year."*

He famously provided a solution, the (perhaps already known) Fibonacci Sequence $F_n : 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \dots$ where the first three terms are boundary conditions. The ratio F_{n+1}/F_n tends to φ, the **golden ratio**. A surprising amount of mathematics sprouts from this sequence and $\varphi = 1.61803\dots$. We truncate it since φ is irrational, but there is a compact representation also providing excellent approximations and reflecting some of its properties.

A **continued fraction** is the representation of a number x as a (potentially) infinite series of fractions, meaning that for some a_i, b_i in $\mathbb{C}$ we wish to have

$$x = a_0 + \cfrac{b_1}{a_1 + \cfrac{b_2}{a_2 + \cfrac{b_2}{a_3 + \dots}}} = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 & \dots \\ & b_1 & b_2 & b_3 & \end{bmatrix}$$

This is also represented as $[a_0, a_1 : b_1, a_2 : b_2, \dots]$. If all the b_i are required to be 1, the continued fraction is in **canonical form** and is conveniently simplified to $x = [a_0, a_1, a_2, \dots]$. The integers a_i are called **partial quotients**. Interestingly, φ has a periodic expansion. We will prove this and see that it relies some information on φ, and on all real numbers. It is only natural to wish for a generalisation: we will focus on attempts at the definition of p-adic continued fractions, and understand why we called them "attempts".

This chapter is mostly based on personal remarks and rearrangements on the first chapters by Olds [27] and Ikenga [16]. Other contributions will be cited as needed.

2.1 Rational numbers as continued fractions

On the Euclidean algorithm for the expansion of rational numbers.

Definition 2.1 (Canonical continued fraction) Consider $(a_i)_I$ with I index set. A **canonical continued fraction** is a chain of consecutive divisions:

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \dots}}}$$

where each a_i is an integer. If I is finite, the chain terminates and the fraction is said **finite**. If $I = \mathbb{N}$ instead, the fraction is said **infinite**.

Different notations exist for generalised continued fractions. For example, Italian mathematician Pietro Cataldi wrote

$$x = a_0 \cdot \& \frac{b_1}{a_1} \cdot \& \frac{b_2}{a_2} \cdot \& \dots$$

where $(a_i)_I$ and $(b_i)_I$ are integers, while German mathematician Carl F. Gauss used the **Kettenbruch** ("continued fraction") **operator** K

$$x = a_0 + \operatorname*{K}_{i=0}^{+\infty} \frac{b_i}{a_i}$$

which is mostly used by complex analysts, who put $f_n := \operatorname{K}_{i=0}^{n} {}^{b_i}\!/_{a_i}$ for $(a_i)_I$ and $(b_i)_I$ complex rational functions. For canonical continued fractions we use the modern notation $[a_0, a_1, a_2, \dots]$ of uncertain attribution.

Fibonacci's $\varphi = 1.618033988749\dots$ will prove to be a great staging ground for our results. The minimal polynomial of F_n is $f(x) = x^2 - x - 1$ with roots

$$\varphi = \frac{1+\sqrt{5}}{2}, \qquad \psi = \frac{1-\sqrt{5}}{2}$$

The first is conventionally called **golden ratio** and the second is its conjugate. It is not hard to derive Binet's formula for F_n:

$$F_n = \frac{\varphi^n + \psi^n}{\varphi + \psi} = \frac{\varphi^n + \psi^n}{\sqrt{5}}$$

This proves that the quotient of successive terms of F_n tends to φ, just remark that $|\psi| < 1$. More importantly, φ is a root of $x^2 - x - 1$, so $\varphi^2 = \varphi + 1$ and

$$\varphi = 1 + \frac{1}{\varphi} = 1 + \cfrac{1}{1 + \cfrac{1}{\varphi}} = \dots = [1, 1, 1, 1, \dots]$$

Can this procedure be generalised? And to which sets of numbers?
Let us start from a rational, for example $\alpha = {}^{71}\!/_{17}$. We can split the numerator

$$\alpha = \frac{71}{17} = \frac{17 \times 4 + 3}{17} = 4 + \frac{3}{17}$$

and even further

$$\alpha = 4 + \frac{3}{17} = 4 + \frac{1}{\frac{17}{3}} = 4 + \frac{1}{\frac{5\times 3+2}{3}} = 4 + \frac{1}{5+\frac{2}{3}}$$
$$= 4 + \frac{1}{5+\frac{1}{1+\frac{1}{2}}} = [4,5,1,2]$$

For all rationals, this returns a finite continued fraction in canonical form. Notice how the procedure mimics what is done in the Euclidean algorithm.

Lemma 2.2 (Euclidean division) Consider two positive integers a and $b \neq 0$. There exist two unique positive integers q and r ($0 \leq r < b$) such that $a = bq + r$.

Proof. Fix b and proceed by induction on a. The base case is $a = 0$, where we can choose $b = r = 0$. Suppose we have a pair (q, r) for a generic $a > 1$, then

$$a + 1 = qb + r + 1$$

and we need to find an appropriate pair (q', r') for $a' = a + q$. Since $r < b$, we have $r + 1 \leq b$. If $r + 1 = b$ we choose $(q + 1, 0)$, and $(q, r + 1)$ if $r + 1 < b$. Suppose $a = qb + r = q'b + r'$ for distinct $q \neq q'$ and $r \neq r'$, then $b(q - q') = r' - r$ where the right side is not divisible by b but the left side is, so they are both equal to zero and $q = q'$, $r = r'$. □

Euclidean division can be turned into an algorithm for the greatest common divisor of a and b. This might seem unrelated to our reasoning at first, but we will see its ties.
Consider $a = 71$ and $b = 17$, we apply "one step" of Euclidean division

$$71 = 4 \times 17 + 3 \qquad q = 4,\ r = 3$$

and we could go on, albeit with a change of parameters. Let us define as a_k, b_k, q_k, r_k the values at step i. At each step, set $a_{k+1} = b_k$ and $b_{k+1} = r_k$.

$$17 = 5 \times 3 + 2 \qquad q_2 = 5,\ r_2 = 2$$
$$3 = 1 \times 2 + 1 \qquad q_3 = 1,\ r_3 = 1$$
$$2 = 2 \times 1 + 0 \qquad q_4 = 2,\ r_4 = 0$$

We stop at the last positive remainder r, which is exactly the GCD of a and b. This procedure is called **(integral) Euclidean Algorithm**.

Algorithm 2.3 (Integral Euclidean algorithm)

in: positive integers a, b

1. set $a_k \leftarrow a$, $b_k \leftarrow b$
2. set $b_k, r_k \leftarrow$ `euclidean_division`(a_k, b_k)
3. if $r_k = 0$ return r_{k-1}, else set $a_{k+1} \leftarrow b_k$, $b_{k+1} \leftarrow r_k$

Theorem 2.4 The Euclidean Algorithm returns $d = \gcd(a, b)$.

Proof. Consider a single step of Euclidean division on a and b, returning the pair (r, q). Any n dividing both a and b divides $r = a - bq$. For the same reason, any n dividing b and r also divides a.

$$\{\text{divisors of } a \text{ and } b\} = \{\text{divisors of } b \text{ and } r\}$$

Therefore, $d = \gcd(a, b) = \gcd(b, r)$. Consider now k steps of Euclidean division, where $a_1 = a$ and $b_1 = b$. Assume $r_k \neq 0$. The same argument proves

$$\{\text{divisors of } a_1 \text{ and } b_1\} = \{\text{divisors of } a_k \text{ and } b_k\}$$

hence d is also the GCD of a_k and b_k. Suppose we reach $r_{k+1} = 0$, then d is a divisor of $r_k \neq 0$ and $d \leq r_k$. Moreover r_k divides b_k and a_k, since (respectively) $0 = r_{k+1} = a_{k+1} - b_{k+1}q_{k+1} = b_k - r_k q_{k+1}$ and $a_k = b_k q_k + r_k$. But d is the greatest of all common divisors, so $d \geq r_k$ and $d = r_k$. □

Given a positive rational $\alpha = a/b$, we are now able to write its continued fraction expansion: apply the Euclidean algorithm on a and b until $r_{k+1} = 0$, then $\alpha = [q_0, q_1, q_2, \ldots, q_k]$. We cannot include step $k+1$ since $r_{k+1} = 0$ would require dividing by 0. Some remarks before proceeding:

(i) The algorithm must terminate since the r_i are a decreasing sequence of non-negative integers.

(ii) The sequence $(q_k)_k$ is uniquely determined by a and b, so the expansion is unique if we build it this way.

(iii) If both a and b are negative, the algorithm does not change. If only one is negative, some refer to $-\alpha$ as $-[r_0, r_1, r_2, \ldots, r_k]$. Others exploit Euclidean division with a negative q and then proceed. If $a = 0$, then $\alpha = 0$ and the expansion is $\alpha = [0]$. If $b = 0$, α is undefined.

(iv) Due to (iii), all partial quotients a_i are positive integers except for a_0 which can be positive, negative or zero.

Algorithm 2.5 (Rational Continued Fraction expansion)

in: a rational $\alpha = a/b$

1. apply the integral Euclidean algorithm on a, b till completion (i.e. $r_{k+1} = 0$), saving the next quotient in $(q_i)_I$ at each step.
2. $\alpha = [q_0, q_1, q_2, \ldots, q_k]$

Continued fractions are unexpectedly well-equipped to provide information on the real number they represent.

Theorem 2.6 Finite canonical continued fractions are exactly the expansions of rational numbers $\alpha = a/b$.

Proof. Assume without loss of generality a and b to be positive. Of course a finite canonical continued fraction represents a rational number, just proceed backwards. Consider on the other side a rational $\alpha = a/b$. Applying the

Euclidean algorithm on $a = a_0$ and $b = b_0$ returns a couple (q_0, r_0) such that $a = bq_0 + r_0$, which can be rearranged as

$$\frac{a}{b} = q_0 + \frac{r_0}{b}$$

If $r_0 \neq 0$ we proceed with $a_1 = b_0 = b$ and $b_1 = r_0$. This can be done since all the numbers we are dealing with are positive. Again,

$$\frac{a}{b} = q_0 + \frac{r_0}{b} = \frac{a}{b} = q_0 + \frac{1}{\frac{b}{r_0}} = \frac{a}{b} = q_0 + \frac{1}{q_2 + \frac{r_1}{r_0}}$$

The process of successive division ends whenever $r_{k+1} = 0$, and this must happen since $r_0 > r_1 > r_2 > \dots$ is a decreasing sequence of integers. □

Corollary 2.7 The representation from Algorithm 2.5 is not unique.

Proof. First, the last term can be modified to obtain an even or odd number of terms in the expansion. If the last $a_k = 1$,

$$\frac{1}{a_k} = \frac{1}{(a_k + 1) + \frac{1}{1}}$$

and $[a_0, \dots, a_k] = [a_0, \dots, a_k - 1, 1]$. If $a_k \neq 1$, we can do the exact opposite and write $[a_0, \dots, a_k] = [a_0, \dots, a_{k-1} + 1]$. Second, with the same idea, any expansion can be "cut short": $[a_0, \dots, a_{k-1}, a_k] = [a_0, \dots, a_{k-1} + 1/a_k]$. □

Uniqueness is not an intrinsic property of the expansion, but of the algorithm generating it. We implicitly require the last term of a finite expansion to be different from 1 to have uniqueness. However, at times we will make use of non-unicity to get two different expansions of the same number. Remark that this is only meaningful for rationals, as expansions of irrationals are infinite.

Back to our example, $[1, 1, 1, 1, 1, \dots]$ is periodic, hence the number it represents (φ) is irrational by Theorem 2.6. Remark that we calculated it via the minimal polynomial of φ over $\mathbb{Q}$. Can we find an algorithm for any other irrational?

2.2 Irrational numbers as continued fractions

On the generalisation of the Euclidean algorithm via the floor function.

The previous approach only works for rational numbers. Now, φ is not rational. If it was we would also have $2\varphi - 1 = \sqrt{5}$ in $\mathbb{Q}$, which is absurd: by standard arguments, $a/b = \sqrt{5}$ for a reduced quotient a/b in $\mathbb{Q}$ implies $a^2 = 5b^2$ so a is either 5 or 1. This is true for all square roots of non-squares. Furthermore, φ is an algebraic irrational.

Definition 2.8 The **set of irrational numbers** is $\mathbb{R} \setminus \mathbb{Q}$, represented as $\mathbb{P}$ due to the alphabetic succession P, Q, R. They are classified as either

(i) **algebraic irrationals**, roots of a non-zero polynomial in $\mathbb{Z}[x]$

(ii) **transcendental irrationals**, all the others.

Since $\mathbb{Q}$ is countable and $\mathbb{R}$ is not, there are uncountably many elements in $\mathbb{P}$. It is very difficult to prove that a real α is transcendental irrational.

Corollary 2.9 A real number has an infinite continued fraction expansion if and only if it is an irrational.

Proof. Trivial from Theorem 2.6. □

For $\alpha = \frac{a}{b} \in \mathbb{Q}$, Euclidean division iteratively returned the integer closest to α (from below). We can do something similar for irrationals using the floor of α.

Algorithm 2.10 (Real Euclidean algorithm)

in: real number α

1. calculate $a_i = \lfloor x_i \rfloor$ and the error $e_i = x_i - a_i$
2. if $e_i \neq 0$ define $x_{i+1} = 1/e_i$ and go on, else if $e_i = 0$ stop

Lemma 2.11 This is a generalisation of the Euclidean Algorithm to $\mathbb{R}$.

Proof. For a rational $\alpha = a/b$ one step of this is equivalent to one step of the Euclidean Algorithm. With the notation of this theorem,

rational Euclidean Algorithm	real Euclidean Algorithm
$x_0 = \alpha = \frac{a}{b}$	$x_0 = \alpha = a/b$
$a_0 = q$ from $a = qb + r$	$a_0 = \lfloor \alpha \rfloor = q$ from $a = qb + r$
$e_0 = x_0 - a_0 = \frac{a-qb}{b} = \frac{r}{b}$	$e_0 = x_0 - a_0 = \frac{a-qb}{b} = \frac{r}{b}$
$x_1 = \frac{b}{r}$	$x_1 = \frac{1}{e_0} = \frac{b}{r}$

□

For rationals nothing changes: properties like Theorem 2.6 and Corollary 2.9 still hold. But the algorithm cannot be adapted to output a gcd (of which numbers?). Remark that irrationals also introduce all kind of errors. Consider $\pi = 3.14159265\ldots$ and try applying the algorithm,

i	x_i	a_i	true a_i	e_i
0	3.141592653589793...	3	3	0.141592653589793...
1	7.062513305931052...	7	7	0.062513305931052
2	15.996594406684103...	15	15	0.996594406684103...
⋮				
12	14.300419599222613...	14	14	0.300419599222613...
13	3.328677631511632...	**3**	**2**	0.328677631511632...

and for $i = 13$ our algorithm starts misbehaving[1]. This is due to the floating point errors adding up and slowly poisoning our calculations.

[1]We tested the above algorithm on a two-core 11th Gen Intel(R) Core(TM) i7-11370H 3.30GHz and 3.30 GHz, Python 3.9 for Windows 11.

Algorithm 2.12 (Real Continued Fraction expansion)

in: real number α

1. apply the real Euclidean algorithm on α till completion (i.e. $e_i = 0$), saving the next a_i in $(a_i)_I$ at each step.
2. $\alpha = [a_0, a_1, a_2, a3, \dots]$

Theorem 2.13 The algorithm returns the continued fraction expansion of α.

$$\alpha = [a_0, a_1, a_2, \dots]$$

This also works for rationals and provides a generalised algorithm for all real numbers. In the next Section we will develop the tools to prove Theorem 2.13.

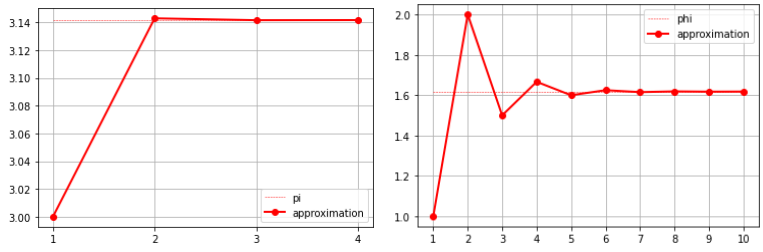
2.3 The convergents

On the properties of convergents. Diophantine approximation of real numbers.

Consider the continued fraction expansions of π and φ. It is a fair question to consider what happens when we study the initial segments of $[a_0, a_1, a_2 \dots]$, i.e. the $C_i = [a_0, \dots, a_i]$. We already know they are rational numbers since they have a finite expansion.

	π		φ
$[3]$	$C_0 = {}^3/_1 = 3$	$[1]$	$C_0 = {}^1/_1 = 1$
$[3,7]$	$C_1 = {}^{22}/_7 = 3.1428\dots$	$[1,1]$	$C_1 = {}^2/_1 = 2.0000$
$[3,7,15]$	$C_2 = {}^{333}/_{106} = 2.8584\dots$	$[1,1,1]$	$C_2 = {}^3/_2 = 1.5000$
$[3,7,15,1]$	$C_3 = {}^{355}/_{113} = 3.1415\dots$	$[1,1,1,1]$	$C_3 = {}^5/_3 = 1.6666\dots$

For irrational numbers, the C_i act as a gradual approximation. Observe how fast the segments converge to the value of α in the two cases $\alpha = \pi$ and $\alpha = \varphi$. They both converge, but the approximation of π at a faster pace.



(a) approximation of π (b) approximation of φ

Figure 2.1: Convergence of the C_i for irrational numbers.

This is somewhat trivial for rationals, as the algorithm terminates with a rational input. They actually provide the *best* approximation for any irrational.

Definition 2.14 (Convergents) Consider a real number α with continued fraction expansion $[a_0, a_1, a_2, a_3, \dots]$, not necessarily finite. We define $C_i = [a_0, a_1, \dots, a_i]$ as the ***i*-th convergent of α**. If $I = [0, 1, \dots, k]$, then C_{k+1} is undefined and the sequence $(C_i)_I$ is finite.

Convergents are a powerful tool that allow to prove a variety of results. For example, they construct a sequence of approximations.

> **Problem 3** (Diophantine approximation) Given a real (irrational) α, provide a "good" approximation via rationals.

This problem is not very relevant for our scenario, however while studying it we will develop the tools to study others of our interest.

Lemma 2.15 Consider an infinite continued fraction. Recursively define two sequences $(p_i)_I$ and $(q_i)_I$ such that

$$\begin{cases} p_{-2} = 0,\ p_{-1} = 1 \\ p_k = a_k p_{k-1} + p_{k-2} \quad \text{for } k \geq 0 \end{cases} \qquad \begin{cases} q_{-2} = 1,\ q_{-1} = 0 \\ q_k = a_k q_{k-1} + q_{k-2} \quad \text{for } k \geq 0 \end{cases}$$

then $C_k = [a_0, a_1, a_2, \dots, a_k] = \frac{p_k}{q_k}$ for $k \geq 0$. This justifies defining them as (respectively) **partial numerators** and **partial denominators**.

Proof. This holds for C_0 since $p_0 = a_0$ and $q_0 = 1$. Consider a generic $k > 0$, we know that the continued fraction representation of C_{k+1} is not unique and

$$\begin{aligned} C_{k+1} = [a_0, a_1, a_2, a_3, \dots, a_k, a_{k+1}] &= \left[a_0, a_1, a_2, a_3, a_4, \dots, a_k + \frac{1}{a_{k+1}}\right] \\ &= \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} = \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} \\ &= \frac{a_{k+1} p_k + p_{k-1}}{a_{k+1} q_k + q_{k-1}} = \frac{p_{k+1}}{q_{k+1}} \end{aligned}$$

□

Consider $\alpha = [a_0, a_1, a_2, \dots]$. We wish to study the properties of the sequence $(C_i)_I$ in $(\mathbb{R}, |\,|_\infty)$. This requires some short lemmas on the properties of these newly defined sequences.

Lemma 2.16 For $k \geq 0$,

$$\begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix}$$

Proof. Easy to prove by induction. The base case $k = 0$ is trivial, and

$$\begin{aligned} \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix} &= \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix} \cdot \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_k p_{k-1} + p_{k-2} & p_{k-2} \\ a_k q_{k-1} + q_{k-2} & q_{k-2} \end{pmatrix} \end{aligned}$$

which is the recursive relation. □

Corollary 2.17 For $k \geq 0$,

$$p_k q_{k-1} - q_k p_{k-1} = (-1)^{k+1}$$

Proof. The matrices defined by the a_j in the previous lemma have all determinant -1 and there are $k+1$. □

Corollary 2.18 For $k \geq 0$,

$$C_k - C_{k-1} = \frac{(-1)^{k+1}}{q_k q_{k-1}}$$

It also follows that $|C_k - C_{k-1}| = 1/q_k q_{k-1}$.

Proof. Consider the previous corollary and divide by $q_k q_{k-1}$. □

Theorem 2.19 (C_k) is a Cauchy sequence converging to α, meaning that

$$\alpha = \lim_{k \to \infty} C_k$$

Proof. Given an $\varepsilon > 0$, by Corollary 2.18 we can always find an N such that for $n, m \geq N$ and $n < m$ the following is upper-bounded by ε:

$$|C_m - C_n| \leq |C_m - C_{m-1}| + \cdots + |C_{n+1} - C_n| = \sum_{k=n}^{m} |C_k - C_{k-1}| = \sum_{k=n}^{m} \frac{1}{q_k q_{k-1}}$$

so the sequence is Cauchy. Since $\mathbb{R}$ is a complete space (C_k) converges to a limit, it remains to show it is α. By definition $\alpha = [a_0, a_1, \ldots, a_k, x_{k+1}]$, where $x_{k+1} = [a_{k+1}, a_{k+2}, a_{k+3}, \ldots]$. Hence for $k \geq 1$

$$\alpha = \frac{x_{k+1} p_k + p_{k-1}}{x_{k+1} q_k + q_{k-1}}$$

$$\alpha(x_{k+1} q_k + q_{k-1}) = x_{k+1} p_k + p_{k-1}$$

$$x_{k+1}(x q_k - p_k) = -(x q_{k-1} - p_{k-1})$$

$$x_{k+1} q_k \left(\alpha - \frac{p_k}{q_k}\right) = -q_{k-1} \left(\alpha - \frac{p_{k-1}}{q_{k-1}}\right)$$

$$\alpha - \frac{p_k}{q_k} = \left(-\frac{q_{k-1}}{x_{k+1} q_k}\right) \left(\alpha - \frac{p_{k-1}}{q_{k-1}}\right)$$

$$\alpha - \frac{p_k}{q_k} = \left(-\frac{q_{k-1}}{x_{k+1} q_k}\right) \left(\alpha - \frac{p_{k-1}}{q_{k-1}}\right)$$

All terms defining q_k are positive, so $q_k > q_{k-1} > 0$. Moreover $x_{k+1} \geq 1$, otherwise the continued fraction would not be infinite. Therefore

$$|\alpha - C_k| = \left|-\frac{q_{k-1}}{x_{k+1} q_k}\right| \; |\alpha - C_{k-1}| < |\alpha - C_{k-1}|$$ □

This proves proves Theorem 2.13. Corollary 2.18 states that the approximation error is $1/q_k q_{k-1}$ and since the q_k are increasing

$$|\alpha - C_k| < 1/q_k^2$$

The convergents of a continued fraction seem to solve Problem 3, but are they a good approximation? Can we find one better?

We can provide some results on the approximation quality.

Theorem 2.20 Every odd C_{2m+1} is an upper bound for every even C_{2n}.

Proof. We can prove that odd convergents strictly increase and even convergents strictly decrease:

$$\begin{aligned} C_k - C_{k-2} &= C_k - C_{k-1} + C_{k-1} - C_{k-2} = \frac{(-1)^{k+1}}{q_k q_{k-1}} - \frac{(-1)^k}{q_{k-1} q_{k-2}} \\ &= \frac{(-1)^k (q_k - q_{k-2})}{q_k q_{k-1} q_{k-2}} = \frac{(-1)^k a_k q_{k-2}}{q_k q_{k-1} q_{k-2}} = \frac{(-1)^k a_k}{q_k q_{k-1}} \end{aligned}$$

where all are positive integers except eventually $(-1)^k$. Thus

$$\begin{aligned} C_0 < C_2 < C_4 < C_6 < C_8 < \dots \\ C_1 > C_3 > C_5 > C_7 > C_9 > \dots \end{aligned}$$

We already know that the sign of $C_k - C_{k-1}$ is dictated by $(-1)^{k+1}$. Pairing the two results, we get that for any m

(i) $C_{2m+1} > C_{2m}$

(ii) $C_{2m+1} > C_{2m+2}$

or in other words that any odd convergent is greater than both its predecessor and its successor. Finally, assume there is an even convergent C_{2n} such that $C_{2m+1} \leq C_{2n}$. If $n < m$ then $C_{2m+1} \leq C_{2n} < C_{2m}$, and if $n > m$ then instead $C_{2n+1} < C_{2m+1} \leq C_{2n}$. Both are absurd due to (i) and (ii). □

Corollary 2.21 C_k is the best approximation of α with denominator at most q_k.

Proof. Suppose p/q is the best rational approximation of α with denominator at most q_k, this property is evaluated with its distance from α.
We know that $q_k > q_{k-1}$, so p_k/q_k and p_{k-1}/q_{k-1} are rationals of denominator at most q_k. Moreover odd convergents are increasing, even convergents are decreasing, and α lies between them due to Corollary 2.18. Then also p/q lies between them. We can prove that

(i) $\left|\frac{p}{q} - \frac{p_{k-1}}{q_{k-1}}\right| = \left|\frac{pq_{k-1} - p_{k-1}q}{q_{k-1}q}\right| \geq \frac{1}{q_{k-1}q}$

(ii) $\left|\frac{p}{q} - \frac{p_{k-1}}{q_{k-1}}\right| \leq \left|\frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}}\right| = \frac{1}{q_{k-1}q_k}$

(iii) $\frac{1}{q_{k-1}q} \leq \left|\frac{p}{q} - \frac{p_{k-1}}{q_{k-1}}\right| \leq \frac{1}{q_{k-1}q_k}$

where (iii) comes from (i) and (ii). Finally, since $q < q_k$ by hypothesis, we get that the inequalities in (iii) are actually equalities. This implies $q = q_k$, and from (iii) $p = p_k$. □

Theorem 2.22 If a/b satisfies

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}$$

then it is among the convergents of α.

Proof. Assume it is not a convergent. By the properties of $(q_i)_I$ we can pick an index k such that $q_k < b < q_{k+1}$ and

$$|\alpha q_k - p_k| \leq |\alpha b - a| = |b|\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b}$$
$$\left|\frac{a}{b} - \frac{p_k}{q_k}\right| \leq \left|\frac{a}{b} - \alpha\right| + \left|\alpha - \frac{p_k}{b_k}\right| < \frac{1}{2b^2} + \frac{1}{2q_k b}$$

The leftmost numerator, $aq_k - p_k b$, is a nonzero integer since $a/b \neq p_k/q_k$. Then

$$\left|\frac{a}{b} - \frac{p_k}{q_k}\right| \geq \frac{1}{q_k b}$$

which returns $q_k > b$. But this contradicts our choice of k. □

Theorem 2.23 (Hurwitz) Any irrational number α has an infinity of rational approximations p/q with $q \geq 1$ which satisfy the inequality

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

Proof. See Olds [27] or LeVeque [19]. □

A crucial step in the proof, which we will not get into, is that if the a_i get very large very fast we get good approximations of α. Back to our example, φ is often called the "simplest form" for an irrational: remark that $a_1, a_2, \ldots$ must be positive (not a_0) in an irrational continued fraction. However, this heuristically implies that φ is one of the hardest irrationals to approximate: its convergents keep a distance from φ close to the boundary by Hurwitz.

2.4 Linear fractional transformations

On a convenient functional representation of the chain division operation.

We saw that the continued fraction $\alpha = [a_0, a_1, a_2, \ldots]$ is the result of a chain of consecutive divisions. This usual representation via square or triangular brackets conveniently hides the repeated operation, which has form

$$a_j \mapsto \alpha_{j-1} + \frac{1}{a_j} = \frac{\alpha_{j-1}a_j + 1}{a_j} =: \alpha_j$$

for $\alpha_{j-1} = [a_0, \ldots, a_{j-1}]$. We can introduce a class of functions representing it. This general overview comes from personal remarks on Pollack's introduction [30].

Definition 2.24 Consider a, b, c, d complex numbers. A **linear fractional (complex) transformation** is a $\mathbb{C}$-to-$\mathbb{C}$ function

$$z \longmapsto L(z) = \frac{az+b}{cz+d}$$

when defined.

This is often called **Möbius Transform** in complex analysis, with the implicit requirement that L can be extended to a $\mathbb{C}_\infty$-to-$\mathbb{C}_\infty$ bijection on the Riemann sphere. If $c \neq 0$ this is done defining

$$\begin{aligned} L: \quad \infty &\longmapsto {}^{a}\!/_{c} \\ -{}^{d}\!/_{c} &\longmapsto \infty \end{aligned}$$

while if $c = 0$

$$L : \infty \longmapsto \infty$$

which is a bijection if we require $ad - bc \neq 0$. This will usually hold for us. The function L is associated to a matrix m depending on its parameters

$$m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

and we can remark it with the notation L_m. The condition $ad - bc \neq 0$ becomes $\det(m) \neq 0$. Consider for example the case $a = b = c = 1$, $d = 0$ and fix $z_0 = 1$, the concept of "chain of operations" resembles

$$\begin{aligned} z_0 &= 1 \\ z_1 &= L(z_0) = 2 \\ z_2 &= L(z_1) = L^2(z_0) = 1.5 \\ z_3 &= L(z_2) = L^3(z_0) = 1.\overline{6} \end{aligned}$$

What we are doing here is by all means

$$\begin{aligned} z_1 &= \frac{1+1}{1} = 1 + \frac{1}{1} \\ z_2 &= \frac{\left(1+\frac{1}{1}\right)+1}{\left(1+\frac{1}{1}\right)} = 1 + \frac{1}{1+\frac{1}{1}} \end{aligned}$$

and so on, meaning that $z_k = L^k(1)$ is the k-th convergent of φ. This is due to the choice of $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ as m, and can be formally proved.

Lemma 2.25 Consider L_m and L_n. Then the matrix associated to their composition $L_m \circ L_n$ is mn, whenever all three are defined.

Proof. By definition,

$$\begin{aligned} (L_m \circ L_n)(z) &= L_m\left(L_n(z)\right) \\ &= \frac{L_n(z)a_m + b_m}{L_n(z)c_m + d_m} = \frac{\left(\frac{za_n+b_n}{zc_n+d_n}\right)a_m + b_m}{\left(\frac{za_n+b_n}{zc_n+d_n}\right)c_m + d_m} \\ &= \frac{(a_m a_n + b_m c_n)z + (a_m b_n + b_m d_n)}{(c_m a_n + b_m c_n)z + (c_m b_n + d_m d_n)} = L_{mn}(z) \end{aligned}$$

□

In our previous example, the k-th power of m is

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^k = \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{pmatrix}$$

where the $(p_i)_I = (1,2,3,4,8,\dots)$ and $(q_i)_I = (1,1,2,3,5,\dots)$ are partial numerators and denominators of $\varphi = [1,1,1,1,\dots]$, since we are exponentiating matrices of the form $\left(\begin{smallmatrix} a_i & 1 \\ 1 & 0 \end{smallmatrix}\right)$ for $a_i = 1$. Due to the previous Lemma,

$$L^k(x) = L_{\left(\begin{smallmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{smallmatrix}\right)}(x) = \frac{p_k x + p_{k-1}}{q_k x + q_{k-1}}$$

$$\begin{aligned} L^1(1) &= \frac{p_1 + p_0}{q_1 + q_1 0} = 2 \\ L^2(1) &= \frac{p_2 + p_1}{q_2 + q_1} = \frac{3}{2} \\ L^3(1) &= \frac{p_3 + p_2}{q_3 + q_2} = 1.\overline{6} \end{aligned}$$

For a less trivial example, pick $\alpha = [4,5,1,2] = {}^{71}/_{17}$ instead. Define the matrices

$$A_k = \begin{pmatrix} a_k & 1 \\ 1 & 0 \end{pmatrix}$$

We already know they can be used to iteratively construct the sequences $(p_i)_I$ and $(q_i)_I$ from their initial values and the $(a_i)_I$. Here $I = \{0,1,2,3\}$, and

$$A_0 = \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix} \quad A_1 = \begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix} \quad A_2 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \quad A_3 = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}$$

This becomes more interesting if we set $L_k(a_k) = L_{A_k - 1}\left(L_{A_{k-2}}\left(\dots L_{A_0}(a_k)\right)\right)$ for $k \geq 0$, which is an immediate generalisation of the previous Lemma.

$$\begin{aligned} L_1(a_1) &= L_{A_0}(a_1) = \frac{4a_1 + 1}{1a_1} = 4 + \frac{1}{5} = C_1 \\ L_2(a_2) &= L_{A_0 A_1}(a_2) = L_{\left(\begin{smallmatrix} 21 & 4 \\ 5 & 1 \end{smallmatrix}\right)}(a_2) = \frac{21a_2 + 4}{5a_2 + 1} = C_2 \\ L_3(a_3) &= L_{A_0 A_1 A_2}(a_3) = L_{\left(\begin{smallmatrix} 25 & 21 \\ 6 & 5 \end{smallmatrix}\right)}(a_3) = \frac{25a_3 + 21}{6a_3 + 5} = C_3 = \alpha \end{aligned}$$

One could also reasonably set $A_{-1} = \left(\begin{smallmatrix} p_{-1} & p_{-2} \\ q_{-1} & q_{-2} \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ to define $L_0(a_0)$ as

$$L_0(a_0) = \frac{a_0}{1} = 4 = C_0$$

and none of the other L_i are varied since A_{-1} is the identity matrix.

Lemma 2.26 Consider $F_n = A_0 \cdot A_{n-1}$ for $n > 0$. Then $L_{F_n}(a_n) = C_n$.

Proof. Remark that $F_n = A_0 \cdots A_{n-1} = \left(\begin{smallmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{smallmatrix}\right)$, therefore

$$\begin{aligned} L_{F_n}(a_n) &= L_{\left(\begin{smallmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{smallmatrix}\right)}(a_n) \\ &= \frac{a_n p_{n-1} + p_{n-2}}{a_n q_{n-1} + q_{n-2}} = \frac{p_n}{q_n} = C_n \end{aligned}$$

□

We can also justify the requirement that $\det(m) \neq 0$.

Lemma 2.27 For $m = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, if L_m is defined in x and y then

$$L_m(x) - L_m(y) = \frac{\det(m)(x-y)}{(cx+d)(cy+d)}$$

Proof. By direct computation,

$$\begin{aligned} L_m(x) - L_m(y) &= \frac{ax+b}{cx+d} - \frac{ay+b}{cy+d} = \frac{(ax+b)(cy+d) - (ay+b)(cy+d)}{(cx+d)(cy+d)} \\ &= \frac{ad(x-y) - bc(x-y)}{(cx+d)(cy+d)} = \frac{\det(m)(x-y)}{(cx+d)(cy+d)} \end{aligned}$$

□

Most of the properties we described can be rearranged with linear fractional transformations in mind. Consider for example the following.

Proposition 2.28 Odd and even convergents tend to the same limit.

Proof. Consider $|C_{2n} - C_{2n+1}|$ for $n \to +\infty$. Then

$$\begin{aligned} |C_{2n} - C_{2n+1}| &= \left|L_{F_{2n}}(a_{2n}) - L_{F_{2n+1}}(a_{2n+1})\right| \\ &= \left|L_{F_{2n}}(a_{2n}) - L_{F_{2n}}\left(L_{A_{2n}}(a_{2n+1})\right)\right| \\ &= \left|L_{F_{2n}}(a_{2n}) - L_{F_{2n}}\left(a_{2n} + \frac{1}{a_{2n+1}}\right)\right| \\ &= \left|\frac{\det(F_{2n})(-1/a_{2n+1})}{(q_{2n}a_{2n} + q_{2n-1})\left(q_{2n}\left(a_{2n} + \frac{1}{a_{2n+1}}\right) + q_{2n-1}\right)}\right| \\ &\leq \frac{|\det F_{2n}|}{|a_{2n+1}||q_{2n}q_{2n-1}|} = \frac{1}{|a_{2n+1}|\left|q_{2n-1}^2\right|} \leq \frac{1}{|q_{2n}q_{2n-1}|} = \frac{1}{q_{2n}q_{2n-1}} \end{aligned}$$

since $|\det F_{2n}| = 1$ and the q_i are positive. □

This also provides an exact analogue for the approximation quality bound of Corollary 2.18.

2.5 Quadratic irrationals and periodicity

On their representation and Lagrange's algorithm for efficient computation. Relation with periodic expansions.

A quadratic irrational is a real number that is both irrational and a root of a degree-two polynomial in $\mathbb{Z}[x]$. An example is φ, which we know is a root of $f(x) = x^2 - x - 1 \in \mathbb{Z}[x]$.

Lemma 2.29 Any α is quadratic irrational if and only if it can be expressed as

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

satisfying the properties

(i) P is an integer

(ii) D is a positive integer and not a perfect square

(iii) Q is a non-zero integer dividing $P^2 - D$

This is unique if D is squarefree: in such case, an α is in **canonical form**.

Proof. Consider a quadratic irrational. The degree-two polynomial it is root of has form $ax^2 + bx + c$. Its determinant is non-zero, else its roots would not be irrational. It cannot be negative either, else its root would be complex.

$$x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \qquad x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a}$$

$$Q = 2a,\ P = -b,\ D = b^2 - 4ac \qquad Q = -2a,\ P = b,\ D = b^2 - 4ac$$

From the above $D > 0$ and D is not a square, otherwise α would be rational. Assume instead to have an α satisfying (i), (ii) and (iii), then

$$\alpha = \frac{P + \sqrt{D}}{Q}$$
$$\alpha Q = P + \sqrt{D}$$
$$\alpha^2 Q^2 + P^2 - 2\alpha PQ = D$$
$$\alpha^2 Q^2 + \alpha(-2PQ) + (P^2 - D) = 0$$

Then α is root of $x^2Q^2 + x(-2PQ) + (P^2 - D)$, which is a polynomial of degree two and coefficients in $\mathbb{Z}$. Its roots are exactly the

$$\frac{2PQ \pm \sqrt{4P^2Q^2 - 4Q^2(P^2 - D)}}{2Q^2} = \frac{P \pm \sqrt{D}}{Q}$$

and its determinant is $\Delta = {}^{4D}/_{Q^2}$, therefore it cannot be zero due to (ii) and the polynomial does not split. □

For example, both roots of $x^2 - x - 1$ we presented (φ and ψ) are already in canonical form. An example of a rational not in canonical form is

$$\frac{2 + \sqrt{20}}{4}$$

because while $Q = 4$ divides $P^2 - D = 4 - 20 = -16$, $D = 20$ is a square.
We have an efficient algorithm to compute the continued fraction expansions of quadratic irrationals.

Lemma 2.30 If x is a quadratic irrational and the linear fractional transformation L is defined in x, then $L(x)$ is also a quadratic irrational.

Proof. Assume x is in canonical form, then it is a matter of calculations to show that $L(x)$ is also a quadratic irrational in $\sqrt{D}$. □

Theorem 2.31 (Lagrange's algorithm) If α is a quadratic irrational in canonical form, we can define three infinite sequences of integers (P_k), (Q_k), (a_k) and an infinite sequence of irrationals (x_k) as

$$\begin{cases} P_0 = P \\ P_{k+1} = a_k Q_k - P_k \quad \text{for } k \geq 0 \end{cases} \qquad \begin{cases} Q_0 = Q \\ Q_{k+1} = \dfrac{D - P_{k+1}^2}{Q_k} \quad \text{for } k \geq 0 \end{cases}$$

$$\begin{cases} x_0 = \alpha \\ x_{k+1} = \dfrac{P_{k+1} + \sqrt{D}}{Q_{k+1}} \quad \text{for } k \geq 0 \end{cases} \qquad \begin{cases} a_0 = \lfloor x_0 \rfloor \\ a_{k+1} = \lfloor x_{k+1} \rfloor \quad \text{for } k \geq 0 \end{cases}$$

such that

(i) $\alpha = [a_0, a_1, a_2, a_3, \dots]$

(ii) $Q_k \neq 0$ for $k \geq 0$

(iii) both Q_k and Q_{k+1} divide $D - P_{k+1}^2$

Proof. We can prove by induction (ii), (iii) and that they are sequences of integers. Consider the base case, here a_0, P_0 and Q_0 are integers by definition. Moreover $Q_0 \neq 0$ and Q_0 divides $D - P_0^2$ since α is in canonical form, thus

$$Q_1 = \frac{D - P_1^2}{Q_0} = \frac{D - a_0^2 Q_0^2 - P_0^2 + 2a_0 Q_0 P_0}{Q_0} = \frac{(D - P_0^2) + Q_0(a_0^2 Q_0 - 2a_0 P_0)}{Q_0}$$

and Q_1 is an integer with $Q_0 Q_1 = D - P_1^2$, proving Q_0 and Q_1 divide $D - P_{k+1}^2$. Then P_1 is also an integer. Consider a generic k. We immediately get that P_{k+1} is an integer by the $(k-1)$-th step. Assume by absurd $Q_{k+1} = 0$, then by construction $D - Q_{k+1} = 0$ and D is a square which is impossible. Also

$$\begin{aligned} Q_{k+1} &= \frac{D - P_{k+1}^2}{Q_k} = \frac{D - a_k^2 Q_k^2 - P_k^2 + 2a_k Q_k P_k}{Q_k} = \frac{(D - P_k^2) + Q_k(a_k Q_k^2 - 2Q_k P_k)}{Q_k} \\ &= \frac{Q_{k-1} Q_k + Q_k(a_k^2 Q_k - 2a_k P_k)}{Q_k} \end{aligned}$$

so Q_{k+1} is an integer, and we get again $Q_k Q_{k+1} = D - P_{k+1}^2$.
We need to prove that the (x_k) are irrationals and the (a_k) form the simple continued fraction expansion of α. It is easier to prove that one step of this algorithm is equivalent to one step of the algorithm from Theorem 2.13,

$$\begin{aligned} x_k - a_k &= \frac{P_k + \sqrt{D}}{Q_k} - a_k = \frac{P_k + \sqrt{D} - a_k Q_k}{Q_k} = \frac{\sqrt{D} - P_{k+1}}{Q_k} \\ &= \frac{\sqrt{D} - P_{k+1}}{Q_k} \frac{\left(\sqrt{D} + P_{k+1}\right)}{\left(\sqrt{D} + P_{k+1}\right)} = \frac{D - P_{k+1}^2}{Q_k\left(\sqrt{D} + P_{k+1}\right)} = \frac{Q_{k+1}}{\sqrt{D} + P_{k+1}} = \frac{1}{x_{k+1}} \end{aligned}$$

and with the notation of Theorem 2.13 we get $e_k = x_k - a_k$, $x_{k+1} = 1/e_k$. □

Algorithm 2.32 (Quadratic irrational Continued Fraction expansion)

in: quadratic irrational α in canonical form

1. fix $P_0 \leftarrow P$, $Q_0 \leftarrow Q$, $x_0 \leftarrow \alpha$, $a_0 \leftarrow \lfloor x_0 \rfloor$
2. iteratively calculate P_{k+1}, Q_{k+1}, x_{k+1}, a_{k+1}
3. $\alpha = [a_0, a_1, a_2, a_3, \dots]$

Consider for example the quadratic irrational

$$\alpha = \frac{3 + \sqrt{11}}{2}$$

It is easy to see that α is in canonical form, so we can apply Lagrange's algorithm with $P_0 = 3$, $Q_0 = 2$, $x_0 = \alpha$, $a_0 = 3$.

	Lagrange's algorithm				irrational algorithm		
i	P_i	Q_i	x_i	a_i	x_i	e_i	a_i
0	3	2	3.15831…	3	3.1583…	-	3
1	3	1	6.31662…	6	6.31662…	0.31662…	6
2	3	2	3.15831…	3	6.31662…	0.15831…	3
⋮							
12	3	1	6.31662…	6	3.07595…	0.32510…	6
13	3	2	3.15831…	3	13.16698…	0.07595…	3
14	3	1	6.31662…	**6**	5.98863…	0.16698…	**13**
15	3	2	3.15831…	**3**	1.01150…	0.98863…	**5**

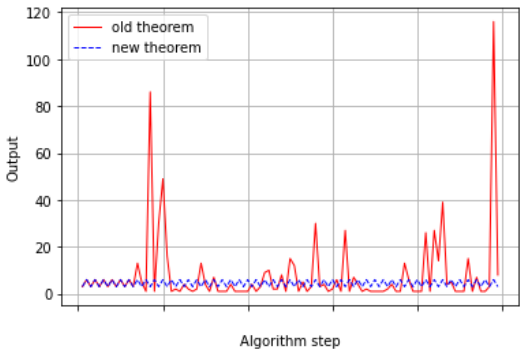


Figure 2.2: Comparison of the a_i from the two algorithms.

We can see that the new algorithm provides a remarkable stability for quadratic irrationals thanks to the three integer sequences. Being theoretically equivalent to the "classical" irrational algorithm[2], it also gives an easier approach for proofs involving quadratic irrationals.

[2]It is indeed theoretically equivalent, but not computationally. This is due to floating point arithmetic slowly poisoning the results, as we saw above

Problem 4 (Periodicity) When is the continued fraction expansion of a real number α periodic?

Quadratic irrationals have a close relation with periodic continued fractions. We will borrow the terminology used for the periodicity of p-adic expansions: a continued fraction is **purely periodic** if its terms have no pre-period, and **(eventually) periodic** if they have periodic behaviour after some pre-period.

Theorem 2.33 (Euler) If a real number α has an eventually periodic continued fraction expansion, then α is a quadratic irrational.

Proof. Assume $\alpha = [a_0, a_1, \dots, a_{j-1}, \overline{a_j, a_{j+1}, \dots, a_{j+k-1}}]$, fix $x_j = [a_j, a_{j+1}, a_{j+2}, \dots]$.

$$\begin{aligned} x_j = [a_j, a_{j+1}, a_{j+2}, \dots] &= [\overline{a_j, a_{j+1}, \dots, a_{j+k-1}}] = [a_j, a_{j+1}, \dots, a_{j+k-1}, x_{j+k}] \\ &= [a_j, a_{j+1}, \dots, a_{j+k-1}, x_j] = \frac{x_j p_n + p_{n-1}}{x_j q_n + q_{n-1}} \end{aligned}$$

so x_j is root of $x^2 q_n + x(q_{n-1} - p_n) - q_{n-1}$ and a quadratic irrational. If the pre-period is non-zero (i.e. $j - 1 \neq 0$), then remark that α is the image of the linear fractional transformation L applied on x_j

$$x_j \longmapsto L(x_j) = \frac{x_j p_{j-1} + p_{j-2}}{x_j q_{j-1} + q_{j-2}}$$

This is well-defined if $p_{j-1}q_{j-2} - p_{j-2}q_{j-1} \neq 0$, which is 1 in our case. More importantly, L is defined in x_j since $x_j q_{j-1} + q_{j-2} = 0$ would imply $x_j \in \mathbb{Q}$. Finally, due to Lemma 2.30 α is a quadratic irrational. □

Theorem 2.34 (Lagrange) If α is a quadratic irrational, then it has a periodic continued fraction expansion.

Proof. We will exploit the sequences arising from Theorem 2.31.

Step 1. If k is large enough, $Q_k > 0$. Consider $\alpha = [a_0, a_1, \dots, a_n, x_k]$ as before for some $n \geq 1$. We can consider x_k as a partial quotient and write

$$\alpha = \frac{x_k p_{k-1} + p_{k-2}}{x_k q_{k-1} + q_{k-2}}$$

where both α and x_k are quadratic irrationals with the same radical term $\sqrt{D}$.

$$\overline{\alpha} = \overline{\left(\frac{x_k p_{k-1} + p_{k-2}}{x_k q_{k-1} + q_{k-2}}\right)} = \frac{\overline{x_k}\,\overline{p_{k-1}} + \overline{p_{k-2}}}{\overline{x_k}\,\overline{q_{k-1}} + \overline{q_{k-2}}} = \frac{\overline{x_k} p_{k-1} + p_{k-2}}{\overline{x_k} q_{k-1} + q_{k-2}}$$

Therefore, if we search for the closed form of $\overline{x_k}$,

$$\begin{gathered} \overline{\alpha}\,(\overline{x_k} q_{k-1} + q_{k-2}) = \overline{x_k} p_{k-1} + p_{k-2} \\ \overline{x_k}\,(\overline{\alpha} q_{k-1} - p_{k-1}) = p_{k-2} - \overline{\alpha} q_{k-1} \\ \overline{x_k} = \frac{p_{k-2} - \overline{\alpha} q_{k-1}}{\overline{\alpha} q_{k-1} - p_{k-1}} = \frac{\frac{-1}{q_{k-2}}\left(\overline{\alpha} - \frac{p_{k-2}}{q_{k-2}}\right)}{\frac{1}{q_{k-1}}\left(\overline{\alpha} - \frac{p_{k-1}}{q_{k-1}}\right)} = -\frac{q_{k-2}}{q_{k-1}} \frac{\overline{\alpha} - \frac{p_{k-2}}{q_{k-2}}}{\overline{\alpha} - \frac{p_{k-1}}{q_{k-1}}} \\ \overline{x_k} \xrightarrow[k \to +\infty]{} -\frac{q_{k-2}}{q_{k-1}} \frac{\overline{\alpha} - \alpha}{\overline{\alpha} - \alpha} = -\frac{q_{k-2}}{q_{k-1}} \end{gathered}$$

where the last step holds because $\overline{\alpha} \neq \alpha$ for a quadratic irrational. Since the q_k are positive for a large k, $\overline{x_k}$ is eventually negative. But $x_k > 0$, so $x_k - \overline{x_k} > 0$ so

$$0 < x_k - \overline{x_k} = \frac{P_k + \sqrt{D}}{Q_k} - \frac{P_k - \sqrt{D}}{Q_k} = \frac{2\sqrt{D}}{Q_k}$$

implying $Q_k > 0$.

Step 2. If k is large enough, Q_k only assumes finitely many values.
From the algorithm $Q_k Q_{k+1} = D - P_{k+1}^2 \leq D$, but for a large enough k we have $Q_{k+1} \geq 1$ and $Q_k > 0$. Then

$$D \geq Q_k Q_{k+1} \geq Q_k > 0$$

so Q_k eventually lies in $[0, D]$.

Step 3. If k is large enough, P_k only assumes finitely many values.
Remark that eventually $Q_{k-1} Q_k > 0$, hence

$$P_k^2 < P_k^2 + Q_{k-1} Q_k = D$$

and P_k lies in $[0, \sqrt{D}]$.

Step 4. The pair (P_k, Q_k) can only assume finitely many values. We will sooner or later reach two distinct indices $i < j$ with $(P_i, Q_i) = (P_j, Q_j)$, in which case $x_i = x_j$ and $a_i = a_j$. All successive pairs will be equal by construction. □

There is something more we can say for the expansion of a particular class of quadratic irrationals. See Olds [27] for a proof.

Proposition 2.35 (Galois) A quadratic irrational α is called **reduced** if both $\alpha > 1$ and $\overline{\alpha} \in (-1, 0)$. The expansion of a quadratic irrational α is purely periodic if and only if α is reduced.

One can actually exploit the theorem of Galois to prove Lagrange's. Our "standard" approach proved there is a finite number of quadratic irrationals the complete quotients can go through, which is equivalent to them reaching a reduced quotient at a certain step: the algorithm then starts being periodic.

Chapter 3

Continued fractions in $\mathbb{Q}_p$

We are already familiar with p-adic numbers. They were first formally introduced by Kurt Hensel (1897) in his article *Über eine neue Begründung der Theorie der algebraischen Zahlen* [15] while trying to expand the analytical theory of complex (Laurent) power series to algebraic number theory.

At this point, we are also very familiar with continued fractions and their core properties. It is just natural to attempt a generalisation in $\mathbb{Q}_p$: by our standards it is just a sinister twin of $\mathbb{R}$, but we will find out that this is more than enough to set us back. Remark that defining any algorithm cfrac returning some sequence $(b_i)_I \leftarrow \text{cfrac}(\alpha)$ is not enough: it must first be well-posed,

(P0) **Convergence.** The algorithm converges, i.e. if $(b_i)_I \leftarrow \text{cfrac}(\alpha)$ then in the normed space $(\mathbb{Q}_p, |\cdot|_p)$ we have $\lim_{n\to\infty} b_n = \alpha$.

and secondly, while not mandatory, it would be nice to also achieve those properties that we found useful in $\mathbb{R}$. For instance those describing α:

(P1) **Finiteness for rationals.** The algorithm terminates with a rational input α, i.e. if α is in $\mathbb{Q}$ and $(b_i)_I \leftarrow \text{cfrac}(\alpha)$ then $I = \{0, 1, 2, \ldots, n\}$. This is well-posed since $\mathbb{Q}_p$ contains a copy of $\mathbb{Q}$.

(P2) **Periodicity.** The algorithm satisfies an analogue of Euler's and Lagrange's theorems (respectively Theorems 2.33 and 2.34), i.e. $(b_i)_I$ is periodic if and only if α is a quadratic irrational. Euler's side always holds, the proof uses universal arguments. We focus on Lagrange's side.

Here we used the notation of canonical continued fractions, but this can be effortlessly extended to generalised continued fractions. For the sequences of partial quotients, we will use the author's notation in each algorithm. For example, Browkin uses $(b_i)_I$ and Schneider $(c_i : b_i)_I$ instead.

The contents on p-adic continued fractions are based on the articles by Browkin [5, 6], Ruban [37], Schneider [39] and a survey by Romeo [36]. Others will be cited as needed.

3.1 A tale of floor functions

A small summary of the first most notable algorithms.

Notation 3.1 When describing $\mathbb{Z}/p\mathbb{Z}$ as being **adjoined to a set $\mathcal{S}$**, we implicitly mean that $\mathcal{S}$ is chosen as complete set of representatives for $\mathbb{Z}/p\mathbb{Z}$.

In 1940, Kurt Mahler questioned whether a p-adic analogue to the continued fraction algorithm in $\mathbb{R}$ was possible ([24], *On a geometrical representation of p-adic numbers*) and provided some generic properties. Many attempts came after.

The year 1969 was most profitable for humanity: we witnessed the Moon Landing, and Schneider provided in his article *Über p-adische Kettenbruche* [39] a continued fraction algorithm for $\mathbb{Z}_p$.

Schneider used $\{0, 1, \dots, p-1\}$ as representative set for $\mathbb{Z}_p$ and exploited the ultrametric distance to gradually approximate α. This procedure mimics the inverse limit definition of $\mathbb{Z}_p$. His algorithm does **not** return a canonical continued fraction.

Modern attempts focus on Lagrange's universal structure: iteratively set

$$\begin{cases} b_i = \text{floor}(\alpha_i) \\ \alpha_{i+1} = \frac{1}{\alpha_i - b_i} \end{cases}$$

This algorithm requires an analogue of the real floor function in $\mathbb{Q}_p$.
Let us see some examples.

(A) In $\mathbb{R}$, we are used to having $\lfloor 7.3 \rfloor = \lfloor 3 \times 10^{-1} + 7 \cdot 10^{1} \rfloor = 7$. One can see this as "returning the positive powers in the series", which represent the integer part. In $\mathbb{Q}_p$, this becomes

$$\text{floor}_A : \sum_{i=-k}^{+\infty} a_i p^i \longmapsto \sum_{i=0}^{+\infty} a_i p^i$$

Consider $p = 3$ for example, fix $\alpha = 2p^{-1} + p^0 + 2p^1 + p^2 = {}^{50}/_{3}$,

$$\text{floor}_A\left(2p^{-1} + p^0 + 2p^1 + p^2\right) = p^0 + 2p^1 + p^2 = 16$$

(B) Intuitively, the real floor can also be seen as "returning the part of integral norm". Remark that in $\mathbb{Q}_p$ a positive norm $|\alpha|_p = p^{-\nu_p(\alpha)}$ corresponds to a negative valuation, so it is reasonable to write

$$\text{floor}_B : \sum_{i=-k}^{+\infty} a_i p^i \longmapsto \sum_{i=-k}^{0} a_i p^i$$

With the same example,

$$\text{floor}_B\left(2p^{-1}+p^0+2p^1+p^2\right)=2p^{-1}+p^0=\frac{5}{3}$$

which has norm $|5/3|_p = 3$.

(C) We can proceed exactly as in (B), but ignore the element of null valuation. This returns again something of positive norm.

$$\text{floor}_C:\sum_{i=-k}^{+\infty}a_ip^i\longmapsto\sum_{i=-k}^{-1}a_ip^i$$

$$\text{floor}_C\left(2p^{-1}+p^0+2p^1+p^2\right)=2p^{-1}=\frac{2}{3}$$

The first notable attempt was by A.A. Ruban in his 1970 article Некотоые метрицеские свойства p-адических йисед (*Certain metric properties of the p–adic numbers*) [37], only found in Russian. Fixing $\{0,1,\dots,p-1\}$ as representative set for $\mathbb{Z}/p\mathbb{Z}$, he defined the following floor function.

Definition 3.2 (Ruban's r function) Fix $\alpha=\sum_i a_ip^i\in\mathbb{Q}_p$ for coefficients a_i in $\{0,1,\dots,p-1\}$. **Ruban's *r* function** is

$$r:\mathbb{Q}_p\longrightarrow\mathbb{Q}$$
$$\alpha=\sum_{i=-k}^{+\infty}a_ip^i\longmapsto r(\alpha)=\sum_{i=-k}^{0}a_ip^i$$

Remark how this is exactly the intuitive generalisation floor_B from (B).
In 1978, Jerxy Browkin defined a similar function in *Continued Fractions in Local Fields I* [5] only differing in the choice of representative set.

Definition 3.3 (Browkin's s function) Fix $\alpha=\sum_i a_ip^i\in\mathbb{Z}_p$ for coefficients a_i in $\{-(p-1)/2,\dots,(p-1)/2\}$. **Browkin's *s* function** is

$$s:\mathbb{Q}_p\longrightarrow\mathbb{Q}$$
$$\alpha=\sum_{i=-k}^{+\infty}a_ip^i\longmapsto s(\alpha)=\sum_{i=-k}^{0}a_ip^i$$

Again, this follows the intuitive idea from (B). Remark how Browkin's s only differs from Ruban's r in the choice of representatives for $\mathbb{Z}/p\mathbb{Z}$. Theorem 1.52 states that this only affects the representation of α in $\mathbb{Q}_p$. We will prove that it has heavy implications in the properties of the sequence $(b_i)_I$, and so does having a floor function such that the set $\text{floor}(\mathbb{Q}_p)$, in which lie the b_i, only contains elements of integral norm.

In his 2001 article "*Continued Fractions in Local Fields II*" [6], Browkin famously provided another one [6], which is the one from example (C).

Definition 3.4 (Browkin's t function) Fix $\alpha=\sum_i a_ip^i\in\mathbb{Q}_p$ for coefficients a_i in $\{-(p-1)/2,\dots,(p-1)/2\}$. **Browkin's *t* function** is

$$t:\mathbb{Q}_p\longrightarrow\mathbb{Q}$$
$$\alpha=\sum_{i=-k}^{+\infty}a_ip^i\longmapsto t(\alpha)=\sum_{i=-k}^{-1}a_ip^i$$

These two choices result in two algorithms called (respectively) "Browkin I" and "Browkin II". Browkin II is more complex than its predecessor due to the use of the sign function, the dependence on n and a convoluted use of both s and t, motivated by the convergence requirement (P0):

$$\text{floor}(\alpha_n) = \begin{cases} s(\alpha_n) & \text{if } n \text{ even} \\ t(\alpha_n) & \text{if } n \text{ odd and } \nu_p(\alpha_n - t(\alpha_n)) = 0 \\ t(\alpha_n) - \text{sign}(t(\alpha_n)) & \text{if } n \text{ odd and } \nu_p(\alpha_n - t(\alpha_n)) \neq 0 \end{cases}$$

In the next sections, we will see how these algorithms perform. All satisfy the strong requirement (P0). Browkin I and Browkin II are the only ones satisfying the soft requirement (P1) and without counterexamples to (P2), therefore most modern approaches start from them. This is represented in Table 3.1. A recent survey by Romeo [36] addressed proving (P2) for Browkin I and II as one of the most challenging open problems in this field.
Some authors recently generalised continued fractions to $\mathfrak{P}$-adic continued fractions for prime ideals $\mathfrak{P}$, see Capuano, Murru, Terracini [8].

property	**Schneider**	**Ruban**	**Browkin I**	**Browkin II**
convergence (P0)	✓	✓	✓	✓
finiteness in $\mathbb{Q}$ (P1)	×	×	✓	✓
periodicity (P2)	×	×	?	?

Table 3.1: The main algorithms and their properties.

We conclude with some examples of all algorithms except Schneider's, which is more complex and will be presented in Section 3.8. Consider $2/3$ in $\mathbb{Q}_7$, the steps in Ruban's algorithm are

$$\begin{cases} \alpha_0 = \alpha = \frac{2}{3} = 3 + 2p + 2p^2 + 2p^3 + \dots \\ b_0 = 3 \end{cases}$$

$$\begin{cases} \alpha_1 = \frac{1}{\alpha_0 - b_0} = 4p^{-1} + 6 + 6p + 6p^2 + 6p^3 + \dots \\ b_1 = 4p^{-1} + 6 = \frac{46}{7} \end{cases}$$

$$\begin{cases} \alpha_2 = \frac{1}{\alpha_1 - b_1} = 6p^{-1} + 6 + 6p + 6p^2 + 6p^3 + \dots \\ b_2 = 6p^{-1} + 6 = \frac{48}{7} \end{cases}$$

$$\begin{cases} \alpha_3 = \frac{1}{\alpha_2 - b_2} = 6p^{-1} + 6 + 6p + 6p^2 + 6p^3 + \dots \\ b_3 = 6p^{-1} + 6 = \frac{48}{7} \end{cases}$$

which loops, returning the expansion $[3, {}^{46}/_{7}, \overline{{}^{48}/_{7}}]$. The steps for Browkin I are almost identical, we just need to adapt to the new set of representatives $\{-3, -2, -1, 0, +1, +2, +3\}$ in each calculation.

$$\begin{cases} \alpha_0 = \alpha = \frac{2}{3} = 3 + 2p + 2p^2 + 2p^3 + \dots \\ b_0 = 3 \end{cases}$$

$$\begin{cases} \alpha_1 = \frac{1}{\alpha_0 - b_0} = 4p^{-1} + 6 + 6p + 6p^2 + 6p^3 + \dots \\ \quad = -3p^{-1} + 0 + 0p + 0p^2 + 0p^3 + \dots \\ b_1 = -3p^{-1} = -\frac{3}{7} \end{cases}$$

since $\alpha_1 = b_1$ the algorithm terminates, returning $[3, -3/7]$. Browkin II has a convoluted floor function which depends on n and the sign function.

$$\begin{cases} \alpha_0 = \alpha = \frac{2}{3} = 3 + 2p + 2p^2 + 2p^3 + \dots \\ b_0 = s(\alpha_0) = 3 \end{cases}$$

$$\begin{cases} \alpha_1 = \frac{1}{\alpha_0 - b_0} = 4p^{-1} + 6 + 6p + 6p^2 + 6p^3 + \dots \\ \quad = -3p^{-1} + 0 + 0p + 0p^2 + 0p^3 + \dots \\ t(\alpha_1) = -3p^{-1} = -\frac{3}{7} \\ b_1 = -3p^{-1} - \operatorname{sign}(t(\alpha_1)) = \frac{4}{7} \end{cases}$$

$$\begin{cases} \alpha_2 = \frac{1}{\alpha_1 - b_1} = 6p^{-1} + 6 + 6p + 6p^2 + 6p^3 + \dots \\ \quad = -1 + 0p + 0p^2 + 0p^3 + \dots \\ b_2 = s(\alpha_2) = -1 \end{cases}$$

and again the algorithm stops, having reached $\alpha_2 = b_2$. The expression is $[3, 4/7, -1]$. It is a general fact that all odd b_i are rationals and even b_i are integers [36]. Below, some further examples. With the notation $\alpha = [b_0, b_1, b_2, \dots]_p$, we implicitly mean that the algorithm is in $\mathbb{Q}_p$ with the appropriate defining set. For example, a Ruban-type $\alpha = [b_0, b_1, b_2, \dots]_p$ requires $\{0, \dots, p-1\}$.

α	**Schneider**	**Ruban**	**Browkin I**	**Browkin II**
$\frac{71}{17}$	$\begin{bmatrix} 27 & 3 & 3 & 3 & 3 & 3 & \overline{3} \\ 1 & 1 & 1 & 1 & 1 & 1 & 2 \end{bmatrix}_3$	$\left[1, \frac{49}{27}, \frac{7}{3}, \overline{\frac{8}{3}}\right]_3$	$\left[1, -\frac{32}{27}, \frac{2}{3}\right]_3$	$\left[1, -\frac{5}{27}, -1, -\frac{2}{3}, 1\right]_3$
$\frac{2}{3}$	$\begin{bmatrix} 11 & 11 & 11 & \overline{11} \\ 8 & 4 & 9 & 10 \end{bmatrix}_{11}$	$\left[8, \frac{59}{11}, \frac{58}{11}, \overline{\frac{120}{11}}\right]_{11}$	$\left[-3, \frac{3}{11}\right]_{11}$	$\left[-3, -\frac{8}{11}, 1\right]_{11}$

These are of course chosen to put an emphasis on their properties. Remark how all but Browkin I and Browkin II have periodical expansions for rationals.

3.2 Generalised continued fractions

On the properties of their associated sequences.

In $\mathbb{R}$, the theory can be naturally extended from rational continued fractions (Algorithm 2.5), which conveniently meant they were in canonical form. We had no need to work with the general object.
There is no reason to assume their form a priori in $\mathbb{Q}_p$, so we will provide some results on generalised continued fractions and their associated sequences.

Consider a *generalised continued fraction*, which is an object of form

$$b_0 + \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \cfrac{a_3}{b_3 + \dots}}}$$

for two sequences $(a_i)_{I^*}$ and $(b_i)_I$ of numerators and denominators in $\mathbb{Q}_p$, where $I^* = I \setminus \{0\}$. If one index set is finite, the other is also finite. This notation is usually shortened to

$$\begin{bmatrix} a_1 & a_2 & a_3 & \dots & \\ b_0 & b_1 & b_2 & b_3 & \dots \end{bmatrix}$$

or simply $[b_0, a_1 : b_1, a_2 : b_2, a_3 : b_3, \dots]$. The following few results are an exact analogue to generalised continued fractions in $\mathbb{R}$.

Definition 3.5 (generalised convergents) Consider a continued fraction expansion $[b_0, a_1 : b_1, a_2 : b_2, a_3 : b_3, \dots]$, not necessarily finite. We define

$$C_i = [b_0, a_1 : b_1 \dots, a_i : b_i] = b_0 + \cfrac{a_1}{b_1 + \ddots \cfrac{a_{i-1}}{b_{i-1} + \cfrac{a_i}{b_i}}}$$

as its ***i*-th convergent**. If $I = [0, 1, \dots, k]$ is finite, then C_{k+1} is undefined and the sequence $(C_i)_I$ is finite.

We define two sequences $(A_n)_I$, $(B_n)_I$ of elements $A_n = A_n(b_0, \dots, a_n, b_n)$ and $B_n = B_n(b_0, \dots, a_n, b_n)$ satisfying the following recursions:

$$\begin{cases} A_0 = b_0 \\ A_1 = b_0 b_1 + a_1 \\ A_{n+2} = b_{n+2} A_{n+1} + a_{n+2} A_n \quad \text{for } n \geq 0 \end{cases} \qquad \begin{cases} B_0 = 1 \\ B_1 = b_1 \\ B_{n+2} = b_{n+2} B_{n+1} + a_{n+2} B_n \quad \text{for } n \geq 0 \end{cases}$$

Lemma 3.6 The recursive definitions above are equivalent to

$$\begin{pmatrix} A_n & A_{n-1} \\ B_n & B_{n-1} \end{pmatrix} = \begin{pmatrix} b_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} b_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 1 & 0 \\ 0 & a_n \end{pmatrix} \begin{pmatrix} b_n & 1 \\ 1 & 0 \end{pmatrix}$$

Proof. By induction,

$$\begin{pmatrix} A_1 & A_0 \\ B_1 & B_0 \end{pmatrix} = \begin{pmatrix} b_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} b_1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b_0 b_1 + a_1 & b_0 \\ b_1 & 1 \end{pmatrix}$$

and the inductive step for $n \geq 2$ is

$$\begin{aligned} \begin{pmatrix} A_n & A_{n-1} \\ B_n & B_{n-1} \end{pmatrix} &= \begin{pmatrix} b_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} b_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 1 & 0 \\ 0 & a_n \end{pmatrix} \begin{pmatrix} b_n & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} A_{n-1} & A_{n-2} \\ B_{n-1} & B_{n-2} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & a_n \end{pmatrix} \begin{pmatrix} b_n & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} b_n A_{n-1} + a_n A_{n-2} & A_{n-1} \\ b_n B_{n-1} + a_n B_{n-2} & B_{n-1} \end{pmatrix} \end{aligned}$$

□

Corollary 3.7 If $(A_n)_I$ and $(B_n)_I$ satisfy the recursive definitions above,

$$\det\begin{pmatrix} A_n & A_{n-1} \\ B_n & B_{n-1} \end{pmatrix} = (-1)^{n+1} a_1 \cdots a_n$$

Proof. The determinant of these matrices is -1 if they contain any b_i and a_i if they contain any a_i. There are respectively $n+1$ and n of them. □

Lemma 3.8 $C_n = {}^{A_n}/_{B_n}$, this justifies defining the A_n as **partial numerators** and the B_n as **partial denominators**.

Proof. Similar to the proof in the real case. The base case is

$$C_0 = \frac{A_0}{B_0} = \frac{b_0}{1}$$

For the inductive step we exploit again non-unicity in the representation:

$$\begin{aligned} C_{n+1} &= [b_0, a_1 : b_1, \ldots, a_n : b_n, a_{n+1} : b_{n+1}] \\ &= \left[b_0, a_1 : b_1, \ldots, a_n : \left(b_n + \frac{a_{n+1}}{b_{n+1}}\right)\right] \\ &= \frac{\left(b_n + \frac{a_{n+1}}{b_{n+1}}\right) A_{n-1} + a_n A_{n-2}}{\left(b_n + \frac{a_{n+1}}{b_{n+1}}\right) B_{n-1} + a_n B_{n-2}} \\ &= \frac{b_{n+1}(b_n A_{n-1} + A_{n-2}) + a_{n+1} A_{n-1}}{b_{n+1}(b_n B_{n-1} + B_{n-2}) + a_{n+1} B_{n-1}} \\ &= \frac{b_{n+1} A_n + a_{n+1} A_{n-1}}{b_{n+1} B_n + a_{n+1} B_{n-1}} = \frac{A_{n+1}}{B_{n+1}} \end{aligned}$$

□

If the continued fraction is simple, we showed in Section 2.3 that some variations of these results hold. They only rely on the recurrent formulas, so they are (mostly) universal and hold in $\mathbb{Q}_p$. But we cannot assume that all b_i are positive: this makes arguments based on signs not transferable in $\mathbb{Q}_p$.

3.3 Partial quotients of negative valuation

On their importance in the construction of an algorithm.

We can provide some further results when the b_i have negative valuation (except eventually the first b_0). This implies that their p-adic norms are integral: this reasoning lead in Section 3.1 to floor functions $\text{floor}_B(\cdot)$ and $\text{floor}_C(\cdot)$. We will prove it is a sensible requirement and $\text{floor}_A(\cdot)$ was not a good candidate.

First, consider what happens under these conditions.

Lemma 3.9 If $b_1, b_2, b_3 \ldots$ have negative valuation, for all $n \geq 1$

$$\nu_p(B_n) = \nu_p(b_1) + \cdots + \nu_p(b_n)$$

Proof. The inductive base is $\nu_p(B_1) = \nu_p(b_1)$. For a generic $n > 1$,

$$\nu_p(b_{n+2}B_{n+1}) = \nu_p(b_{n+2}) + \nu_p(B_{n+1}) = \nu_p(b_{n+2}) + \nu_p(b_1) + \cdots + \nu_p(b_{n+1})$$

$$\nu_p(B_{n+2}) = \nu_p(b_{n+2}B_{n+1} + B_n) = \min\left\{\nu_p(b_{n+2}B_{n+1}), \nu_p(B_n)\right\} = \nu_p(b_{n+2}B_{n+1})$$

where $\nu_p(b_{n+2}B_{n+1}) < \nu_p(B_n)$ being them respectively the sum of $n+1$ and n strictly negative terms. □

Lemma 3.10 If $b_1, b_2, b_3 \ldots$ have negative valuation and $b_0 \neq 0$, for all $n \geq 0$

$$\nu_p(A_n) = \nu_p(b_0) + \nu_p(b_1) + \cdots + \nu_p(b_n)$$

and if $b_0 = 0$ then for all $n \geq 2$

$$\nu_p(A_n) = \nu_p(b_2) + \nu_p(b_3) + \cdots + \nu_p(b_n)$$

Proof. Assume $b_0 \neq 0$. This is similar to the previous lemma, but with $A_0 = b_0$. If $\nu_p(b_0) = 0$, then $b_0 = 1$ and the result still follows. If $\nu_p(b_0) < 0$ the results follows exactly as before. Finally, $\nu_p(b_0) > 0$,

$$\begin{aligned}
&\nu_p(A_0) = \nu_p(b_0) \\
&\nu_p(A_1) = \nu_p(b_0b_1 + 1) = \min\left(\nu_p(b_0b_1), \nu_p(1)\right) = \nu_p(b_0) + \nu_p(b_1)
\end{aligned}$$

and induction follows as above. If $b_0 = 0$ then $\nu_p(b_0) = +\infty$, but recursively

$$\begin{aligned}
A_0 &= b_0 = 0 \\
A_1 &= b_1b_0 + 1 = 1 \\
A_2 &= b_2b_1b_0 + b_2 + b_0 = b_2 \\
&\vdots
\end{aligned}$$

so we can proceed in the same way, just with b_2 instead of b_0 as first element in the dominating term of any A_n. □

Corollary 3.11 If $b_1, b_2, b_3 \ldots$ have negative valuation and $b_0 \neq 0$, for all $n \geq 0$

$$|A_n|_p = \prod_{k=0}^{n} |b_k|_p \qquad\qquad |B_n|_p = \prod_{k=1}^{n} |b_k|_p$$

Corollary 3.12 Under these assumptions, if $b_0 \neq 0$ all A_n and B_n are non-zero. If $b_0 = 0$, this still holds but with $n \geq 2$ for the A_n.

Proof. This is trivial for the B_n. If $A_n = 0$ instead, then $\nu_p(A_n) = +\infty$ by definition but this is impossible due to the formula in Lemma 3.10. □

Browkin [5] proves that under this condition the algorithm is well-defined, i.e. if the expansion $[b_0, b_1, b_2, \ldots]$ of α dictated by the $(b_i)_I$ converges then it converges to α. This means that the algorithm is well-posed.

Theorem 3.13 (Browkin's convergence I) If $(b_i)_I$ consists of elements with negative valuation except b_0, then the sequence $(C_n)_I$ converges to a $\beta \in \mathbb{Q}_p$ such that $\nu_p(\beta - C_n) = \nu_p(B_nB_{n+1})$ for $n \geq 0$.

Proof. Concerning the difference of consecutive terms,

$$\begin{aligned} C_{n+1} - C_n &= \frac{A_{n+1}}{B_{n+1}} - \frac{A_n}{B_n} = \frac{A_{n+1}B_n - A_nB_{n+1}}{B_nB_{n+1}} \\ &= \frac{b_{n+1}\left(A_nB_n - A_nB_n\right) + \left(B_nA_{n-1} - A_nB_{n-1}\right)}{B_nB_{n+1}} \\ &= \frac{(-1)\left(A_nB_{n-1} - B_nA_{n-1}\right)}{B_nB_{n+1}} = \frac{(-1)^n}{B_nB_{n+1}} \end{aligned}$$

$$\nu_p\left(C_{n+1} - C_n\right) = \nu_p\left(\frac{A_{n+1}}{B_{n+1}} - \frac{A_n}{B_n}\right) = \nu_p\left(\frac{(-1)^n}{B_nB_{n+1}}\right) = -\nu_p\left(B_nB_{n+1}\right)$$

which is greater than zero and increasing due to Lemma 3.9. This proves that $(C_i)_I$ is a Cauchy sequence in p-adic norm. Moreover for $m > n$

$$\begin{aligned} \nu_p\left(C_m - C_n\right) &= \nu_p\left(C_m - C_{m-1} + C_{m-1} - C_{m-2} + C_{m-2} \cdots - C_n\right) \\ &= \nu_p\left(C_m - C_{m-1} + C_{m-1} - C_{m-2} + C_{m-2} \cdots - C_n\right) \\ &= \min\left[\nu_p\left(C_m - C_{m-1}\right), \ldots \nu_p\left(C_{n+1} - C_n\right)\right] \\ &= \nu_p\left(C_{n+1} - C_n\right) = -\nu_p\left(B_nB_{n+1}\right) \end{aligned}$$

and if we define $\beta \in \mathbb{Q}_p$ as its limit we get the thesis. □

In particular, this also means that

$$|C_1 - C_0|_p = p^{\nu_p(B_1B_0)} < 1$$

since $\nu_p(B_1B_0) = \nu_p(b_1) < 0$, and at the n-th step

$$|C_{n+1} - C_n|_p = p^{\nu_p(B_{n+1}B_n)} < 1$$

and the sequence $(B_{n+1}B_n)_I$ provides a approximation quality bound.

Theorem 3.14 (Browkin's convergence II) If the algorithm does not terminate (i.e. I is infinite) with input α, then $(C_i)_I$ converges in $\mathbb{Q}_p$ and its limit is α.

Proof. Consider again $\alpha = \alpha_0 = [b_0, b_1, b_2, b_3, \ldots, b_n, \alpha_{n+1}]$. Then

$$\alpha = \frac{A_{n+1}(b_0, b_1, \ldots, \alpha_{n+1})}{B_{n+1}(b_0, b_1, \ldots, \alpha_{n+1})} = \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}}$$

$$\alpha - C_n = \frac{\alpha_{n+1}A_n + A_{n-1}}{\alpha_{n+1}B_n + B_{n-1}} - \frac{A_n}{B_n} = \frac{A_{n-1}B_n - A_nB_{n-1}}{\left(\alpha_{n+1}B_n + B_{n-1}\right)B_n} = \frac{(-1)^n}{\left(\alpha_{n+1}B_n + B_{n-1}\right)B_n}$$

and since

$$\nu_p(\alpha_{n+1}B_n + B_{n-1}) = \nu_p(b_{n+1}B_n + B_{n-1}) = \nu_p(B_{n+1})$$

we have that

$$\nu_p\left(\alpha - C_n\right) = \nu_p\left(\frac{(-1)^n}{\left(\alpha_{n+1}B_n + B_{n-1}\right)B_n}\right) = -\nu_p(B_{n+1}) - \nu_p(B_n)$$

which tends to infinity, therefore $|\alpha - C_n|_p$ tends to 0. □

All the above proves that it is desirable for an algorithm to have partial quotients of negative valuation. This requirement is not too restrictive: Ruban, Browkin I and Browkin II all satisfy this property.

Fix $p \neq 2$ a prime. Consider the localisation of $\mathbb{Z}$ at its prime ideal $\mathcal{P} =< p >$. Such ring is usually denoted as $\mathbb{Z}_{\mathcal{P}}$, $\mathcal{P}^{-1}\mathbb{Z}$ or $\mathbb{Z}\left[1/p\right]$. We will use the latter for convention and convenience.

Definition 3.15 The **ring of s-integers** is

$$\mathbb{Z}\left[1/p\right] = \left\{ \frac{a}{p^k} \text{ such that } a \in \mathbb{Z}, k \in \mathbb{N} \right\}$$

The name is justified by an analogous construction in number fields which we will not investigate further.

Lemma 3.16 $\mathbb{Z}\left[1/p\right]$ is a subring of $\mathbb{Q}_p$.

Proof. It is a ring under the same operations. Consider now any $\alpha = a/p^k$ in $\mathbb{Z}\left[1/p\right]$, writing a as a power series in $\mathbb{Z}_p$ we get

$$\frac{a}{p^k} = \frac{\sum_{i=0}^{+\infty} a_i p^i}{p^k} = \sum_{i=0}^{+\infty} a_i p^{i-k} = \sum_{j=-k}^{+\infty} b_j p^j$$

with $b_j = a_{i-k}$, so α lies in the field of fractions of $\mathbb{Z}_p$ which is $\mathbb{Q}_p$. □

Browkin's choices have $s(\alpha) \in \mathbb{Z}\left[1/p\right]$ and $t(\alpha) \in \mathbb{Z}\left[1/p\right]$ for any α in $\mathbb{Q}_p$. Further, due to the choice of representatives, the following holds.

Lemma 3.17 For any α in $\mathbb{Q}_p$,

(i) $r(\alpha)$ lies in $\mathbb{Z}\left[1/p\right] \cap [0, p)$

(ii) $s(\alpha)$ and $t(\alpha)$ lie in $\mathbb{Z}\left[1/p\right] \cap (-p/2, +p/2)$

Proof. Consider Ruban's r, we have $r(\alpha) = \sum_{i=-k}^{0} a_i p^i$ and due to the choice of representatives this is lower-bounded by 0 and upper-bounded by

$$\sum_{i=-k}^{0} (p-1)p^i = (p-1)\sum_{i=0}^{k} p^{-i} = (p-1)\frac{1-p^{-k}}{1-p^{-1}} = (p-1)\frac{p^k-1}{p^k-p^{k-1}} = p - \frac{1}{p^{k-1}}$$

Browkin's s is easier to treat with the Euclidean norm,

$$|s(\alpha)|_\infty = \left| \sum_{i=-k}^{0} a_i p^i \right|_\infty \leq \sum_{i=-k}^{0} \left| a_i p^i \right|_\infty < \frac{p-1}{2} \sum_{i=-k}^{0} p^i = \frac{p-1}{2} \sum_{i=0}^{k} p^{-i} = \frac{p}{2} - \frac{1}{2p^{k-1}}$$

and the same holds for Browkin's t. □

An immediate consequence is that Ruban and Browkin I all return partial quotients b_i which are either null or negatively valued. Moreover, since s is such that $\nu_p(\alpha - s(\alpha)) > 0$,

$$\nu_p(\alpha_{n+1}) = \nu_p\left(\frac{1}{\alpha_n - s(\alpha_n)}\right) = -\nu_p\left(\frac{1}{\alpha_n - s(\alpha_n)}\right) < 0$$

If $b_0 \neq 0$ all partial quotients b_i have negative valuation. If $b_0 = 0$ instead, this means that $\nu_p(\alpha_0) > 0$, but then $\nu_p(\alpha_1) = \nu_p(1/\alpha_0)$ is negative: all next b_i have negative valuation. This also holds for Ruban's algorithm, which uses r instead.

Corollary 3.18 Ruban and Browkin I return partial quotients $(b_i)_I$ such that for $i \geq 1$ their norms are $|b_i|_p \geq 1$ and $|b_i|_\infty < p/2$.

The reasoning is more complex for Browkin II, since Browkin's t is used in combination with s and the floor function. This was proved by Browkin in [6].

Lemma 3.19 Browkin II returns partial quotients $(b_i)_I$ such that

$$\nu_p(b_{2i}) = \nu_p(\alpha_{2i}) = 0$$
$$\nu_p(b_{2i+1}) = \nu_p(\alpha_{2i+1}) < 0$$

Proof. Recall that in Browkin II

$$\text{floor}(\alpha_n) = \begin{cases} s(\alpha_n) & \text{if } n \text{ even} \\ t(\alpha_n) & \text{if } n \text{ odd and } \nu_p(\alpha_n - t(\alpha_n)) = 0 \\ t(\alpha_n) - \text{sign}(t(\alpha_n)) & \text{if } n \text{ odd and } \nu_p(\alpha_n - t(\alpha_n)) \neq 0 \end{cases}$$

For an odd n, $\nu_p(b_n) < 0$ holds by construction since the sign function does not change the valuation, $\nu_p(\pm 1) = 0$ but $\nu_p(\alpha_n) < 0$. For an even n, notice how $\alpha_{n-1} - b_{n-1}$ in step $n-1$ is constructed to have null valuation, implying that at the n-th step $\nu_p(\alpha_n) = -\nu_p(\alpha_{n-1} - b_{n-1}) = 0$ and $s(\alpha_n)$ is a non-zero element of the representative set $\{-(p-1)/2, \ldots, +(p-1)/2\}$. □

This also implies what we remarked in Section 3.1: all partial quotients are by construction a fraction with just a power of p at the denominator, so even partial quotients are integers.

3.4 P0, convergence property

A necessary and sufficient condition for output convergence in $\mathbb{Q}_p$.

Property P0 is the first meaningful requisite for any well-behaving continued fraction algorithm in $\mathbb{Q}_p$.

(P0) If $(b_i)_I \leftarrow \text{cfrac}(\alpha)$, then $(b_i)_I$ converges in $\mathbb{Q}_p$ to α.

Since we are studying algorithms with negatively valued partial quotients, from the results of the previous Section (Theorem 3.14) this property can be reduced to the following:

(P0′) If $(b_i)_I \leftarrow \text{cfrac}(\alpha)$, then $(b_i)_I$ converges in $\mathbb{Q}_p$.

Theorem 3.20 Consider the partial numerators and denominators $(A_n)_I$ and $(B_n)_I$ uniquely defined by the partial quotients $(b_i)_I$ of the algorithm. The algorithm converges in $\mathbb{Q}_p$, i.e. (P0) holds, if and only if

$$\lim_{n \to +\infty} \nu_p \left(B_n B_{n+1} \right) = -\infty$$

Proof. We need to prove that the convergents $(C_n)_I$ are a Cauchy sequence in the ultrametric space $\mathbb{Q}_p$. From Lemma 1.25, we know that this is equivalent to requiring

$$\lim_{n\to+\infty} |C_{n+1} - C_n| = 0$$

which can be written as

$$\lim_{n\to+\infty} \nu_p\left(\frac{A_{n+1}B_n - A_nB_{n+1}}{B_{n+1}B_n}\right) = \lim_{n\to+\infty} \nu_p\left(\frac{(-1)^n}{B_{n+1}B_n}\right) = +\infty$$

and is exactly the thesis. □

In the algorithms constructed following Lagrange's, we put $b_i = \text{floor}(\alpha_i)$ for a chosen function $\text{floor}(\cdot)$ posing as the real $\lfloor\cdot\rfloor$. Theorem 3.20 justifies our previous remarks on the "trivial choice" for $\text{floor}(\cdot)$ returning only the positive powers of p in the expression of α,

$$\begin{aligned}\nu_p(B_nB_{n+1}) &= \nu_p(B_n) + \nu_p(B_{n+1}) \\ &= \big[\nu_p(b_1) + \cdots + \nu_p(b_n)\big] + \big[\nu_p(b_1) + \cdots + \nu_p(b_n) + \nu_p(b_{n+1})\big] \\ &= 2\nu_p(b_1) + \cdots + 2\nu_p(b_n) + \nu_p(b_{n+1})\end{aligned}$$

which for $n \to +\infty$ diverges to $+\infty$, proving this function to be a poor choice. Consider instead the case $\nu_p(b_i) < 0$ for $i = 1, 2, 3, \ldots$, arising from Ruban's and Browkin's functions r and s. From the equation of Lemma 3.9,

$$\nu_p(B_n) = \nu_p(b_1) + \cdots + \nu_p(b_n) < 0 \quad \text{for } n \geq 1$$

and the same reasoning proves the following sufficient condition.

Lemma 3.21 If $b_1, b_2, b_3, \ldots$ have negative valuation, the algorithm converges. This does not depend on the valuation of b_0.

Remark how this is a sufficient criterion, not a necessary one. For example, it could be relaxed to the following.

Corollary 3.22 If the $(b_i)_I$ eventually (i.e. from a certain $N \in \mathbb{N}$) satisfy Lemma 3.21, the algorithm converges.

Corollary 3.23 If the $(b_i)_I$ satisfy Lemma 3.21 except for a subsequence of negative valuation, the algorithm converges.

Having an algorithm satisfying either Theorem 3.20 or one of Corollaries 3.22 and 3.23 completes the study of convergence in $(\mathbb{Q}_p, |\cdot|_p)$.
These results, however, tell us nothing about convergence of $(b_i)_I$ in $(\mathbb{R}, |\cdot|_\infty)$. If the sequence satisfies it, the condition only states that we will slowly factor out all powers of p from $B_{n+1}B_n$, but we know nothing about other factors. This gives rise to the following open problem.

Problem 5 (Convergence problem) Consider a p-adic continued fraction algorithm satisfying convergence property (P0) in $\mathbb{Q}_p$.
Does its output $(b_i)_I$ also converge in $\mathbb{R}$?

3.5 P1, finiteness property

A short remark on finite continued fraction expansions.

Property P0 is an implicit requirement for any well-posed algorithm.
Properties P1 and P2, respectively finiteness on rationals and periodicity on quadratic irrationals are not compulsory, but desirable for an analogue to the algorithm in $\mathbb{R}$.

(P1) **Finiteness for rationals.** If α is in $\mathbb{Q} \subseteq \mathbb{Q}_p$ and $(b_i)_I \leftarrow \mathrm{cfrac}(\alpha)$, then $I = \{0, 1, 2, \dots, n\}$ is finite.

This is a reasonable requirement: remark again that both $\mathbb{R}$ and $\mathbb{Q}_p$ contain a copy of $\mathbb{Q}$, so when dealing with the immersion $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ we can consider its domain as the usual rationals.

If $I = \{0, \dots, k\}$, then $[b_0, b_1, \dots, b_k]$ represents a rational: just backtrace the consecutive divisions to a fraction. This only uses universal arguments. Since the other side of property P1 always holds, we can only concern ourselves with the given implication.
P1 was proved in $\mathbb{R}$ using the fact that remainders $(r_i)_I$ from Euclidean division formed a decreasing sequence of integers. A similar strategy has been used by Browkin [5] and Barbero, Cerruti, Murru [4] for Browkin I and Browkin II, albeit on different sequences.

3.6 Real and p-adic quadratic irrationals

On a number theoretical approach to real quadratic irrationals and to their p-adic analogue.

This is an introduction to p-adic quadratic irrationals based on personal remarks on the book by Robert [35, Section 6.6] and Browkin's article [5].

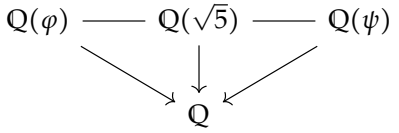
Let us first recall what happens in $\mathbb{R}$.
Real quadratic irrationals are irrational roots of an irreducible quadratic polynomial f of integral coefficients, meaning that they lie in $\mathbb{P} \coloneqq \mathbb{R} \setminus \mathbb{Q}$. If we consider $\mathbb{Q}$ as a field and

$$\mathbb{Q}(\alpha) \coloneqq \{a + b\alpha \text{ for } a, b \in \mathbb{Q}\}$$

as a $\mathbb{Q}$-vector field, this is equivalent to $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. For example, we know $f(x) = x^2 - x - 1$ has irrational roots φ and ψ. Since f is quadratic, irreducible and monic, it is also their minimal polynomial and $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ is both a field extension of order 2 and a $\mathbb{Q}$-vector space of power base $\{1, \varphi\}$. These two are

$$v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad\qquad v_\varphi = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$$

if represented with basis $\{1, \sqrt{5}\}$. Something similar happens if we try $\{1, \psi\}$, therefore the are the same vector space and our extension has the following structure.



$$\mathbb{Q}\left(\sqrt{5}\right) = \mathbb{Q}\left(\frac{1+\sqrt{5}}{2}\right) = \mathbb{Q}(\varphi)$$
$$= \mathbb{Q}\left(\frac{1-\sqrt{5}}{2}\right) = \mathbb{Q}(\psi)$$

Pick $\alpha = \varphi$. Being a finite extension of $\mathbb{Q}$, then $\mathbb{Q}(\alpha)$ is also a **number field**. One usually exploits algebraic number theory to study the properties of such extensions in a more general setting, where $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$. We will see why the case $n = 2$ is of our interest.

Each $\beta \in \mathbb{Q}(\varphi)$ has some basis-invariant properties: one of them is the minimal polynomial, others are norm and trace, descending from matrices. We can associate a matrix $M(\beta)$ to β representing multiplication by it in $\mathbb{Q}(\varphi)$. In our degree-two extension, one basis is $\{e_1, e_2\} = \{1, \sqrt{5}\}$ and $\beta = a + b\sqrt{5}$. The entries of row i are the components of βe_i in order.

$$M(\beta) = \begin{pmatrix} a & b \\ 5b & a \end{pmatrix}$$

We define **trace of β** and **(algebraic) norm of β** as respectively trace and determinant of $M(\beta)$, which are basis-invariant.

$$\text{trace}(\beta) = 2a = (a + \sqrt{b}) + (a - \sqrt{b})$$
$$\text{norm}(\beta) = a^2 - 5b^2 = (a + \sqrt{b}) \cdot (a - \sqrt{b})$$

Finally, if we pick $\sigma \in G(\mathbb{Q}(\alpha)/\mathbb{Q})$ such that

$$\sigma\left(\sqrt{D}\right) = -\sqrt{D}$$
$$\sigma(q) = q \quad \text{for } q \in \mathbb{Q}$$

then $\overline{\beta}$ conjugate of β is defined as $\sigma(\beta)$. If we focus on f_β minimal polynomial of β over $\mathbb{Q}$, norm and trace can be written in terms of β and its conjugate:

$$f_\beta(x) = x^2 + (\beta + \overline{\beta})x + (\beta \cdot \overline{\beta})$$
$$= x^2 + \text{trace}(\beta)x + \text{norm}(\beta)$$

Taking $\beta = \varphi$ as an element of $\mathbb{Q}(\varphi) = \mathbb{Q}(\sqrt{5})$, then $\text{norm}(\varphi) = -1$ and $\text{trace}(\varphi) = 1$. With φ in canonical form,

$$\text{norm}(\varphi) = \frac{P + \sqrt{D}}{Q} \cdot \frac{P - \sqrt{D}}{Q} = \frac{P^2 - 5}{Q^2}$$
$$\text{trace}(\varphi) = \frac{P + \sqrt{D}}{Q} + \frac{P - \sqrt{D}}{Q} = \frac{2P}{Q}$$

Consider now $\mathbb{Q}_p$.
We wish to extend the theory of real quadratic irrationals to p-adic quadratic irrationals, and understand whether (and when) they are ill-defined.

Definition 3.24 An α in $\mathbb{Q}_p$ is **quadratic irrational** (or ***p*-adic quadratic irrational**) if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ as a field extension.

Most properties transfer, allowing us to define norm and trace in $\mathbb{Q}(\alpha)$.

Lemma 3.25 If α is a p-adic quadratic irrational, then it is root of an irreducible degree-two polynomial of coefficients in $\mathbb{Z}$.

Proof. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$, we can consider $\mathbb{Q}(\alpha)$ as a $\mathbb{Q}$-vector space isomorphic to $\mathbb{Q} \oplus \mathbb{Q}$ with power base $\{1, \alpha\}$. The set $\{1, \alpha, \alpha^2\}$ is linearly dependent, so there are $c_0, c_1, c_2 \in \mathbb{Q}$ such that $c_0(1) + c_1(\alpha) + c_2(\alpha^2) = 0$. This means that α is root of $f(x) = c_2x^2 + c_1x + c_0$ whose coefficients can be assumed integers without loss of generality. The polynomial is irreducible, otherwise it would split in linear factors and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 1$. □

A p-adic quadratic irrational α is therefore associated to an irreducible quadratic polynomial $f(x) = a_2x^2 + a_1x + a_0$ such that $f(\alpha) = 0$ and the a_i are in $\mathbb{Z}$. We know that α is one among

$$x_1, x_2 = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0a_2}}{2a_2}$$

allowing us to find explicit expressions for conjugate, norm and trace.
Conversely, an irreducible quadratic polynomial of determinant $D = a_1^2 - 4a_0a_2$ over $\mathbb{Z}$ can be associated to a p-adic quadratic irrational, but we must require that $\sqrt{D}$ is defined in $\mathbb{Q}_p$. From Section 1.10, this is equivalent to D being a square modulo p. We shall always assume this is the case.

An analogue of Lemma 2.29 conveniently holds, allowing to write quadratic irrationals in a canonical form. This is a direct consequence of Lemma 3.25.

Corollary 3.26 Any α is a p-adic quadratic irrational if and only if it can be expressed as

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

satisfying the properties

(i) P is an integer

(ii) D is a positive integer

(iii) D is a square in $\mathbb{Q}_p$, but not a perfect square

(iv) Q is a non-zero integer dividing $P^2 - D$

This is unique if D is squarefree: in such case, an α is in **canonical form**.

Proof. If α is a p-adic quadratic irrational, i.e. if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$, then considering its minimal polynomial $f(x) = a_2x^2 + a_1x + a_0$

$$\alpha = \frac{-a_1 + \sqrt{a_1^2 - 4a_0a_2}}{2a_2}$$

Therefore (i) and (ii) are trivial, the first and second part of (iii) are required respectively for it to exist and the extension to have degree two, and (iv) can

be assumed without loss of generality. Of course all calculations have to be immersed in $\mathbb{Q}_p$.
On the other hand, an α satisfying all (i), (ii), (iii) and (iv) has a well-defined conjugate $\overline{\alpha}$ in $\mathbb{Q}_p$ such that

$$f(x) = x^2 + (\alpha + \overline{\alpha})x + (\alpha \cdot \overline{\alpha})$$

is quadratic and irreducible, otherwise we would have

$$\begin{aligned}\Delta &= (\alpha + \overline{\alpha})^2 - 4(\alpha \cdot \overline{\alpha}) \\ &= \left(\frac{2P}{Q}\right)^2 - 4\left(\frac{P^2 - D}{Q^2}\right) = \frac{4D}{Q^2} = 0\end{aligned}$$

but this cannot be if D satisfies (iii). □

We can always assume a quadratic irrational α in such form. The only nuisance is defining which of the two roots we need to consider according to the representative set of $\mathbb{Z}/p\mathbb{Z}$ (recall $\mathcal{S}$ in Notation 3.1).
If D is a positive integer with $\left(\frac{D}{p}\right) = 1$, Hensel's lemma (Theorem 1.46) provides an algorithm to find its two roots d_1 and d_2 as zeroes of $x^2 - D$, and tells us they are p-adic integers. Write

$$\begin{aligned}d_1 &= a_0 + a_1 p + a_2 p^2 + a_3 p^3 + a_4 p^4 + \dots \\ d_2 &= b_0 + b_1 p + b_2 p^2 + b_3 p^3 + b_4 p^4 + \dots\end{aligned}$$

If we fix $\{0, 1, \dots, p-1\}$, then we choose the smallest between a_0 and b_0 and pick the corresponding d_j. If we fix $\{-(p-1)/2, \dots, +(p-1)/2\}$ instead, we choose the positive one. Since a_0 and b_0 are roots of D modulo p, only one is positive. This d_j is the canonical root of D, and we write $\sqrt{D} = d_j$.

Consider the example from Section 1.10. We provided two solutions of

$$f(x) = x^2 - 2 \in \mathbb{Z}_7[x]$$

as p-coherent sequences. This is equivalent to finding $\sqrt{2}$ in $\mathbb{Z}_7$. As p-adic numbers, they are (in the two representation systems)

$$\begin{aligned}d_1 &= 3 + 1p + 2p^2 + 6p^3 + \dots = +3 + 1p + 2p^2 - 1p^3 + \dots \\ d_2 &= 4 + 5p + 4p^2 + 0p^3 + \dots = -3 - 1p - 2p^2 + 1p^3 + \dots\end{aligned}$$

Under the representative set $\{0, 1, \dots, p-1\}$, the leftmost expansion, we pick d_1. Under $\{-(p-1)/2, \dots, +(p-1)/2\}$, we pick d_1 again. Here $\sqrt{2} = d_1$ in all cases.

A final remark and warning.
Both real and p-adic quadratic irrationals are roots of an irreducible quadratic polynomial with integral coefficients, but it is important to recall that we work in $\mathbb{Q}_p$ and there is no "nice" correspondence between it and $\mathbb{R}$.

Aperiodic p-adic series are divergent real series[1] , and some real numbers[2] do not exist at all in $\mathbb{Q}_p$. One should think of them as vastly different structures. An exception is $\mathbb{Q}$, which is contained in both: its two copies can be identified one to the other.

3.7 P2, periodicity property

A preliminary analysis and comparison with $\mathbb{R}$.

We unknowingly worked with field extensions while proving Euler's and Lagrange's theorems (Theorems 2.33 and 2.34) in $\mathbb{R}$. Periodicity property P2 for a generic continued fraction algorithm cfrac on $\mathbb{Q}_p$ can be rephrased as

(P2′) The output $(b_i)_I \leftarrow \text{cfrac}(\alpha)$ is periodic if and only if $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$.

Again, this is reasonable since both $\mathbb{R}$ and $\mathbb{Q}_p$ contain a copy of $\mathbb{Q}$. Euler's proof only uses universal arguments, therefore his side also holds in $\mathbb{Q}_p$.

Theorem 3.27 (Euler in $\mathbb{Q}_p$) If a p-adic number α has an eventually periodic continued fraction expansion, then α is a p-adic quadratic irrational.

Sketch of proof. Exactly like we did for Theorem 2.33.
If cfrac satisfies (P0), consider its partial numerators and denominators. Assume α has a purely periodic expansion, then we can represent it as a quadratic irrational via some partial quotient α_j. If α has an (eventually) periodic expansion, it is the image of a quadratic irrational via a linear fractional operator and thus a quadratic irrational itself. □

This suggests a natural correlation between periodic continued fractions and degree-two equations. Studying property (P2′), Theorem 3.27 leaves us with the following problem to address.

Problem 6 (Periodicity problem) Fix a p-adic number α such that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ and a continued fraction algorithm on $\mathbb{Q}_p$. Does α have a periodic continued fraction expansion?

In $\mathbb{R}$, Lagrange's algorithm provided a closed form for complete quotients α_n. We can give a similar structure to $\mathbb{Q}_p$. Writing $\alpha = \alpha_0$ in canonical form, we can define two sequences $(Q_n)_I$ and $(P_n)_I$ such that

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

If the partial quotients returned from the algorithm are $(b_i)_I$, these two sequences can be recursively defined as

$$\begin{cases} P_0 = P \\ P_{n+1} = b_n Q_n - P_n \end{cases} \qquad \begin{cases} Q_0 = Q \\ Q_{n+1} = \frac{D - P_{n+1}^2}{Q_n} \end{cases}$$

[1] Formally evaluate the formal power series: this usually diverges in $\mathbb{R}$. Theorem 1.44 states that rationals are exactly those elements in $\mathbb{Q}_p$ with periodic (formal) series expansion upon allowing an infinite series of zeroes to be "periodic" - otherwise integers would not be periodic.

[2] Consider the square root of 5 in $\mathbb{Q}_3$, 5 is not a square modulo 3 since $2 \equiv 5 \mod 3$.

Lemma 3.28 If α is a quadratic irrational, then every complete quotient α_n can be written as

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

with P_n and Q_n satisfying the recurrence relation above.

Proof. We proceed by induction. For $n = 0$ we have $\alpha_0 = \alpha$ already in such form, and from α we inherit P_0 and Q_0. For the inductive step,

$$\begin{aligned}
\alpha_{n+1} &= \frac{1}{\alpha_n - b_n} = \frac{1}{\left(\frac{P_n+\sqrt{D}}{Q_n}\right) - b_n} \\
&= \frac{Q_n}{(P_n - b_n Q_n) + \sqrt{D}} = \frac{Q_n(P_n - b_n Q_n - \sqrt{D})}{(P_n - b_n Q_n)^2 - D} \\
&= \frac{Q_n(-P_{n+1} - \sqrt{D})}{P_{n+1}^2 - D} = \frac{Q_n(P_{n+1} + \sqrt{D})}{D - P_{n+1}^2} = \frac{P_{n+1} + \sqrt{D}}{Q_{n+1}}
\end{aligned}$$

where in the last row we simply substituted the recurrence relations. □

A first difference from real continued fraction is that the partial quotients in $\mathbb{R}$ are integers, while in $\mathbb{Q}_p$ they are rationals[3]. We cannot say a priori if this form is canonical since P_n and Q_n could be rationals, but due to Corollary 3.26 it can indeed be reduced to a canonical form. See the analysis in Capuano, Veneziano and Zannier [9, Section 4] for more results.

The conjugate of α_n satisfies a similar formula, just with the opposite sign on the square root. This is easy to prove, apply the usual $\sigma \in G(\mathbb{Q}(\alpha)/\mathbb{Q})$ such that $\sigma(\sqrt{D}) = -\sqrt{D}$ to α_n.

Remark that for general continued fractions the following formulas hold:

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

$$\begin{cases} P_0 = P \\ P_{n+1} = b_n Q_n - P_n \end{cases} \qquad \begin{cases} Q_0 = Q \\ Q_{n+1} = \frac{D - P_{n+1}^2}{a_n Q_n} \end{cases}$$

where we already inherit the assumption $a_n \neq 0$ from the definition.

Sadly, knowing the recurrence relations is not enough to prove (P2') in the general case. A crucial step in the proof of Lagrange's side in $\mathbb{R}$ was having positive partial quotients, which we are not always guaranteed to have.

3.8 Schneider's p-adic algorithm

A brief overview on the algorithm and its properties.

[3] Being a finite formal series in p, they are rationals.

In 1969, Schneider provided the first continued fraction algorithm for p-adic integers. Its structure does not follow Lagrange's algorithm and returns a generalised continued fraction.
This section is a short overview mainly based on de Poorten [42] and Romeo [36]: while not too relevant for our case, this algorithm is worthwhile to study due to it being the first. The results are simple enough to show in a few pages.

Schneider fixed $\{0, 1, \dots, p-1\}$ as representative set for $\mathbb{Z}/p\mathbb{Z}$ and considered the following result.

Lemma 3.29 All $a \in \mathbb{Z}_p$ satisfying $0 \leq |\alpha - a|_p < 1$ are congruent modulo p.

Proof. Consider two distinct a_1, a_2 such that $0 \leq |\alpha - a_i|_p < 1$, then

$$\begin{aligned} |a_1 - a_2|_p &= |a_1 + \alpha - \alpha - a_2|_p \\ &\leq \max\left\{|a_1 - \alpha|_p, |\alpha - a_2|_p\right\} < 1 \end{aligned}$$

since $\mathbb{Q}_p$ is ultrametric. This implies $\nu_p(a_1 - a_2) > 0$. □

Remark that the condition is equivalent to

$$\nu_p(\alpha - a) > 0$$

We denote by $[\beta]_{(j)}$ the j-th coefficient in the expansion of the p-adic integer β for convenience. The lemma states the following: if given any $\alpha \in \mathbb{Z}_p$ we are able to find an $a \in \mathbb{Z}_p$ such that $\nu_p(\alpha - a) > 0$, then they are congruent modulo p. But we could have $\alpha \neq a$, i.e. some j such that $[\alpha - a]_{(j)} \neq 0$. We need to pick such index j and repeat the process, mimicking the inherent inverse limit structure of $\mathbb{Z}_p$ given by the ring isomorphism from Theorem 1.14,

$$\begin{aligned} \varphi : \mathbb{Z}_p &\longrightarrow \prod_{n=0}^{+\infty} \mathbb{Z}/p^n\mathbb{Z} \\ \sum_{i=0}^{+\infty} a_i p^i &\longmapsto (\alpha_0, \alpha_1, \alpha_2, \dots) \end{aligned}$$

Algorithm 3.30 (Schneider's Continued Fraction expansion for $\mathbb{Z}_p$)
Fix $\alpha = \sum_i c_i p^i \in \mathbb{Z}_p$ for $c_i \in \{0, 1, \dots, p-1\}$. Set $\alpha_0 = \alpha$ and $b_0 = [\alpha_0]_{(0)}$,

$$\begin{cases} e_{n+1} = \nu_p(\alpha_n - b_n) \\ a_{n+1} = p^{e_{n+1}} \\ \alpha_{n+1} = \frac{a_{n+1}}{\alpha_n - b_n} \\ b_{n+1} = \left[p^{e_{n+1}} \alpha_{n+1}\right]_{(0)} \end{cases}$$

If at any step $\alpha_i = b_i$, the algorithm terminates and I is finite.

This returns a continued fraction expansion in general form

$$b_0 + \cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \cfrac{a_3}{b_3 + \dots}}}$$

such that the b_i take by construction value in $\{1, 2, \ldots, p-1\}$ and the a_i are positive powers of p. The only exception is b_0 which can be zero: remark that

$$\begin{aligned}\nu_p\left(p^{e_{n+1}}\alpha_{n+1}\right) &= e_{n+1} + \nu_p\left(\alpha_{n+1}\right) = e_{n+1} + \nu_p\left(a_{n+1}\right) - \nu_p\left(\alpha_n - b_n\right) \\ &= e_{n+1} + e_{n+1} - e_{n+1} = e_{n+1}\end{aligned}$$

Theorem 3.31 Schneider's algorithm satisfies property (P0).

Proof. This is trivial if the continued fraction is finite. For an infinite expression, consider the generalised formula

$$\begin{pmatrix} A_n & A_{n-1} \\ B_n & B_{n-1} \end{pmatrix} = \begin{pmatrix} b_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & a_1 \end{pmatrix}\begin{pmatrix} b_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 1 & 0 \\ 0 & a_n \end{pmatrix}\begin{pmatrix} b_n & 1 \\ 1 & 0 \end{pmatrix}$$

Taking its determinant, we showed that

$$\begin{aligned} A_n B_{n-1} - B_n A_{n-1} &= (-1)^{n+1} a_1 \cdots a_n \\ \frac{A_n}{B_n} &= \frac{A_{n-1}}{B_{n-1}} + \frac{(-1)^{n+1} a_1 \cdots a_n}{B_n B_{n-1}} \end{aligned}$$

where the a_i are positive powers of p. As $n \to +\infty$, we have that

$$\begin{aligned}\left|\frac{A_n}{B_n} - \frac{A_{n-1}}{B_{n-1}}\right|_p &= \left|(-1)^{n+1}\frac{p^{e_1+\cdots+e_n}}{B_n B_{n-1}}\right|_p \\ &= \left|\frac{p^{e_1+\cdots+e_n}}{B_n B_{n-1}}\right|_p \longrightarrow 0\end{aligned}$$

We can also use these equations to find an expression for the limit,

$$C_n = \frac{A_n}{B_n} = [b_0] + \left[\frac{p^{e_1}}{B_0 B_1}\right] + \left[-\frac{p^{e_1+e_2}}{B_1 B_2}\right] + \cdots + \left[(-1)^{n+1}\frac{p^{e_1+\cdots+e_n}}{B_n B_{n-1}}\right]$$

which again converges in p-adic norm. □

Sadly, Schneider's algorithm does not satisfy property (P1). We can find various counterexamples: for example $71/17$ in $\mathbb{Q}_3$ returns

$$\left[\begin{array}{cccccccc} 27 & 3 & 3 & 3 & 3 & 3 & \overline{3} \\ 1 & 1 & 1 & 1 & 1 & 1 & 2 \end{array}\right]$$

where

$$\begin{aligned}(a_i)_{I^*} &= (27, \overline{3}) \\ (b_i)_I &= (1, 1, 1, 1, 1, 1, \overline{2})\end{aligned}$$

We are given the following effective criterion for the determination of its period by Pejkovic [29].

Theorem 3.32 Schneider's algorithm on a reduced rational $\alpha = a/b$ either terminates or we can detect a period within $O(\log^2 H(\alpha))$ steps, where the rational height is $H(\alpha) = \max\{|a|, |b|\}$.

In our example, $H(\alpha) = 71$ and $\log(71) = 6.149\ldots$

Schneider's algorithm doesn't satisfy property (P1) either. One of the first criteria was given by de Weger [43] starting from a challenge by Bundschuh [7] to showh whether

$$\sqrt{-1} \in \mathbb{Q}_5\,, \quad \sqrt{2} \in \mathbb{Q}_7\,, \quad \sqrt{5} \in \mathbb{Q}_{11}\,, \quad \sqrt{3} \in \mathbb{Q}_{13}$$

were periodic. Remark that we already used challenge 2 in some examples.

Theorem 3.33 If for some index n the sign of P_n and Q_n are different and $P_{n+1}^2 > D$, then the (Schneider) continued fraction of $\sqrt{D} \in \mathbb{Q}_p$ is not periodic.

Proof. Consider the recurrence formulas for $(P_n)_I$ and $(Q_n)_I$ in the general case. It follows immediately that $P_{n+1} = a_n Q_n - P_n$ has a different sign from P_n and the same of Q_n. This also holds for Q_n and $Q_{n+1} = {}^{(D-P_{n+1}^2)}/_{(a_n Q_n)}$, which have different signs, therefore P_{n+1} and Q_{n+1} also have different sign. Moreover,

$$|P_{n+2}|_\infty = |P_{n+1}|_\infty + b_{n+1}|Q_{n+1}|_\infty > |P_{n+1}|_\infty$$

implying $P_{n+2}^2 > D$. By induction, $|P_{n+1}|_\infty$ tends to infinity, but periodicity of the continued fraction (in $\mathbb{Q}_p$) implies periodicity of the P_n (in both $\mathbb{Q}_p$ and $\mathbb{R}$), which cannot be if they are unbounded. □

Corollary 3.34 If $D < 0$, the continued fraction of $\sqrt{D}$ is not periodic in $\mathbb{Q}_p$.

Proof. If $c < 0$, we immediately satisfy the conditions of the Theorem: $P_n^2 > D$ always holds and $P_1 = b_0 > 0$, $Q_1 = {}^{(D-P_1^2)}/_{a_0} < 0$ by definition. □

De Weger proved that the challenges by Bundschuh are not periodic: the first satisfies the Corollary, and the others all satisfy the Theorem with $n = 1$. For example $\sqrt{2} \in \mathbb{Q}_7$ goes through the following iterations (also from de Weger [43], albeit with a different notation):

n	P_n	Q_n	a_n	b_n
0	0	1	49	3
1	2	–1	7	1
2	–3	2	49	3

Table 3.2: Sequences associated to $\sqrt{2} \in \mathbb{Q}_7$ [43, page 114].

Starting from $n = 1$, the hypotheses of Theorem 3.32 are satisfied.

3.9 Ruban's p-adic algorithm

A brief overview on the algorithm and its properties.

Since the article by Ruban can only be found in Russian, we will need to base this Section on references by Browkin [5, 6], Murru [26], Romeo [36].

Consider Lagrange's algorithm. Its structure, apart from the "integer part" (or floor) operation, is universal. Ruban made an attempt to the definition of a p-adic floor function.

Definition 3.35 (Ruban's r function) Fix $\alpha = \sum_i a_i p^i \in \mathbb{Z}_p$ for a_i in $\{0, 1, \dots, p-1\}$. **Ruban's r function** is

$$r : \mathbb{Q}_p \longrightarrow \mathbb{Q}$$
$$\alpha = \sum_{i=-k}^{+\infty} a_i p^i \longmapsto r(\alpha) = \sum_{i=-k}^{0} a_i p^i$$

Once this is fixed, the algorithm follows the same structure. Ruban's algorithm is worth studying for its close similarity with Browkin I, which has many open problems to offer.

Algorithm 3.36 (Ruban's Continued Fraction expansion for $\mathbb{Q}_p$) Set $\alpha_0 = \alpha$ and $b_0 = r(\alpha_0)$. Iteratively define

$$\begin{cases} \alpha_{i+1} = \frac{1}{\alpha_i - b_i} \\ b_{i+1} = r(\alpha_{i+1}) \end{cases}$$

If at any step $\alpha_i = b_i$, α_{i+1} is undefined and the two sequences $(b_i)_I$, $(\alpha_i)_I$ terminate (i.e. I is finite).

Remark that Ruban's floor function r maps a p-adic number into a rational number of negative p-adic valuation, except eventually the first whenever $b_0 = 0$. This allows us to prove the following.

Lemma 3.37 Ruban's continued fraction algorithm satisfies property (P0).

Proof. Corollary 3.22 holds for $n \geq N$ with starting index $N = 1$ since all $b_1, b_2, b_3, \dots$ have negative valuation. □

Laohakosol [18] proved that Ruban does not satisfy property P1.

Theorem 3.38 (Theorem 2 [18]) Let α be a nonzero element of $p\mathbb{Z}_p$. Then α is rational if and only if its Ruban expansion is either finite or periodic with all partial quotients of form $b_i = p - 1/p$ from a certain index i onwards.

Sketch of proof. If the expansion is finite, this is trivial. If the partial quotients are $b_i = p - 1/p$ from $i \geq N$, N fixed, Laohakosol provides a rational expression for the periodical segment. The other side requires building an associated generalised continued fraction $[0, a_1 : b_1, a_2 : b_2, \dots]$ and proving the two are "equivalent" - in the sense that they have the same convergents. Then Laohakosol introduces some auxiliary x_i such that

$$\alpha = \frac{a_1}{x_0/x_1} = \frac{a_1}{b_1 + a_2 x_2/x_1} = \frac{a_1}{b_1 + \dfrac{a_2}{b_3 + a_3 x_3/x_2}} = \dots$$

and proves they are eventually constant in absolute value. The catch is that they are either non-zero or the fraction terminates. □

A recent result by Capuano, Veneziano and Zannier [9] provides a characterisation from the point of view of the prime p.

Theorem 3.39 For any α in $\mathbb{Q} \subset \mathbb{Q}_p$,

(i) if $\alpha < 0$, for every prime p Ruban's algorithm does not terminate for α.

(ii) if $\alpha \geq 0$ and $\alpha \in \mathbb{Z}$, there are only finitely many primes p such that Ruban's algorithm does not terminate for α.

(iii) if $\alpha \geq 0$ and $\alpha \notin \mathbb{Z}$, there are only finitely many primes p such that Ruban's algorithm terminates for α.

The proof is very convoluted and exploits results we did not introduce (e.g. real embeddings). See the article for more details.

We also know that Ruban's algorithm does not satisfy (P2). Ooto [28] exploits arguments similar to those of de Weger.

Theorem 3.40 If for some n we have $P_nQ_n \leq 0$ and $P_{n+1}^2 > D$, then Ruban's algorithm is not ultimately periodic for α.

Proof. Assume $P_nQ_n < 0$. Since the b_n are always positive,

$$P_nP_{n+1} = P_n(b_nQ_n - P_n) = P_nb_nQ_n - P_n^2 < 0$$

and by hypothesis

$$Q_nQ_{n+1} = Q_n\left(\frac{D - P_{n+1}^2}{Q_n}\right) = D - P_{n+1}^2 < 0$$

therefore $P_{n+1}Q_{n+1} < 0$. Similarly to Theorem 3.32,

$$|P_{n+2}|_\infty = |b_{n+1}|_\infty|Q_{n+1}|_\infty + |P_{n+1}|_\infty > |P_{n+1}|_\infty$$

which diverges, making it impossible for $(P_n)_I$ to be periodic. □

This allows for the creation of an arbitrary number of counterexamples to (P2) for Ruban's continued fractions. The analogy with de Weger's approach ends with the following:

Corollary 3.41 If $D < 0$, Ruban's algorithm is not ultimately periodic on $\sqrt{D}$.

Proof. Here $P_0Q_0 = 0$ and $P_1^2 = 1$, so we can apply the Theorem for $n = 0$. □

Interestingly, in the same article by Capuano, Veneziano and Zannier [9] mentioned above, they also provide an effective criterion for the determination of the period.

Proposition 3.42 Let α be a p-adic quadratic irrational. Ruban's continued fraction of α is periodic if and only if there exists an unique real embedding $j : \mathbb{Q}(\alpha) \to \mathbb{R}$ such that the image of each α_n under j is positive.
There exists an effectively computable constant N_α such that either

(i) an $n \leq N_\alpha$ does not have a positive real embedding, therefore the expansion is not periodic, or

(ii) $\alpha_{n_1} = \alpha_{n_2}$ for some $n_1 < n_2 \leq N_\alpha$, therefore the expansion is periodic.

3.10 A p-adic Euclidean algorithm

On a generalisation of the Euclidean algorithm to $\mathbb{Q}_p$.

J. Browkin [5] proposes what is perhaps the most natural definition of floor function in $\mathbb{Q}_p$: we will introduce it from the perspective of Lager [17].

Theorem 3.43 (p-adic Euclidean division) Given any $a, b \in \mathbb{Q}_p$, $b \neq 0$, there exist two unique $q \in \mathbb{Z}[1/p]$ with $|q|_\infty < p/2$ and $r \in \mathbb{Q}_p$ with $|r|_p < |b|_p$ such that

$$a = qb + r$$

Proof. Remark that q can also be seen as an element of $\mathbb{R}$, so $|q|_\infty$ is well-defined. If $|a|_p < |b|_p$ set $q = 0$ and $r = a$. Otherwise write

$$a = up^{\nu_p(a)} \qquad\qquad b = vp^{\nu_p(b)}$$

for u and v invertible according to Theorem 1.39. Find an integer $\overline{q}$ such that

$$\overline{q} \equiv uv^{-1} \mod p^{\nu_p(b)-\nu_p(a)+1}$$

and $|\overline{q}| \leq p^{\nu_p(b)-\nu_p(a)+1}$. This is possible because u and v are invertible in $\mathbb{Z}_p$, hence $\nu_p(u)$ and $\nu_p(v)$ are zero and they are invertible in every $\mathbb{Z}/p^k\mathbb{Z}$. If we define $q = \overline{q}p^{\nu_p(a)-\nu_p(b)}$ we get an element of $\mathbb{Z}[1/p]$ with $|q|_\infty \leq 1/p$. Then

$$r = a - qb = up^{\nu_p(a)} - \left(\overline{q}p^{\nu_p(a)-\nu_p(b)}\right) vp^{\nu_p(b)} = (u - \overline{q}v)p^{\nu_p(b)}$$

therefore $\nu_p(r) \geq \nu_p(b) + 1$ and $|r|_p < |b|_p$. As for uniqueness, consider two couples (r, q) and (r', q') satisfying the equation. Write $q = m/p^k$ and $q' = m'/p^k$.

$$b(q - q') = (r' - r)$$
$$|b|_p|q - q'|_p = |b(q - q')|_p = |r' - r|_p = \max\left\{|r|_p, |r'|_p\right\} < |b|_p$$

which implies $|q - q'|_p < 1$, so $p \mid q - q' = m - m'/p^k$ and $p^{k+1} \mid m - m'$. But $|q - q'|_\infty < p$, so $|m - m'|_p < p^{k+1}$. The only possibility is $m - m' = 0$, so $m = m'$, $q = q'$ and finally $r = r'$. □

It is only natural to compare its properties to "usual" Euclidean division.

Theorem 3.44 (p-adic Euclidean algorithm) Consider two p-adic numbers a and b with $b \neq 0$. Set $a_0 = a$ and $b_0 = b$. Iteratively find q_i and r_i according to Theorem 3.43 such that

$$a_i = q_i b_i + r_i$$

and for each step set $a_i = b_{i-1}$ and $b_i = r_{i-1}$. Stop when $r_i = 0$.

(i) Assume a and b are rationals $a = p_a/q_a p^{\nu_p(a)}$ and $b = p_b/q_b p^{\nu_p(b)}$ in reduced form. Then for each r_i resulting from the algorithm

$$r_i \cdot \operatorname{lcm}(q_a, q_b) \in \mathbb{Z}[1/p]$$

(ii) This process has a finite number of steps for rational inputs.

Proof. Consider (i). Fix $l = \operatorname{lcm}(q_a, q_b)$. From $a_0 = q_0 b_0 + r_0$, we get

$$l\frac{p_a}{q_a}p^{\nu_p(a)} = lq_0\frac{p_b}{q_b}p^{\nu_p(b)} + lr_0$$

and lr_0 lies in $\mathbb{Z}[1/p]$. The result for all the r_i follows by induction with the same reasoning.

Consider (ii) instead. For any couple (a_i, b_i) with $b_i \neq 0$ write them as

$$r_i = u_i p^{\nu_p(r_i)} = u_i p^{\epsilon_i} \qquad\qquad q_i = v_i p^{\nu_p(q_i)} = v_i p^{\delta_i}$$

according to Theorem 1.39. Some remarks on them:

(a) In Theorem 3.43 we set $q = \overline{q}p^{\nu_p(a)-\nu_p(b)}$ with $\nu_p(a) \leq \nu_p(b)$. If $q \neq 0$, then p does not divide it and $|q|_p \geq 1$. In our setting we have $\nu_p(q_i) = \nu_p(a_i) - \nu_p(b_i) = \nu_p(r_{i-2}) - \nu_p(r_{i-1})$, hence $\delta_i = \epsilon_{i-2} - \epsilon_{i-1}$.

(b) In the same proof we saw $\epsilon_i \geq \epsilon_{i-1} + 1$, therefore $\epsilon_i \geq \epsilon_{i-1} + 1 \geq \epsilon_{i-2} + 2$ and $\epsilon_i > \epsilon_{i-2}$.

(c) We have that $\left|v_i p^{\delta_i}\right|_\infty < \frac{p-1}{2}$, hence $|v_i|_\infty < \frac{p^{1-\delta_i}}{2}$.

(d) Both v_i and u_i are rationals.

Since $r_i = a_i - q_i b_i = r_{i-2} - q_i r_{i-1}$, we conclude that

$$\begin{aligned} u_i p^{\epsilon_i} &= u_{i-2}p^{\epsilon_{i-2}} - \left(v_i p^{\delta_i}\right)\left(u_{i-1}p^{\epsilon_{i-1}}\right) \\ &= u_{i-2}p^{\epsilon_{i-2}} - v_i u_{i-1} p^{\epsilon_{i-1}+\delta_i} \\ &= p^{\epsilon_{i-2}}(u_{i-2} - v_i u_{i-1}) \end{aligned}$$

$$\begin{aligned} |u_i|_\infty &\leq p^{\epsilon_{i-2}-\epsilon_i}\left(|u_{i-2}|_\infty + |v_i|_\infty |u_{i-1}|_\infty\right) \\ &< p^{\epsilon_{i-2}-\epsilon_i}\left(|u_{i-2}|_\infty + \frac{1}{2}p^{1-\delta_i}|u_{i-1}|_\infty\right) \\ &= p^{\epsilon_{i-2}-\epsilon_i}\left(|u_{i-2}|_\infty + \frac{1}{2}p^{1-\epsilon_{i-2}+\epsilon_{i-1}}|u_{i-1}|_\infty\right) \\ &= p^{\epsilon_{i-2}-\epsilon_i}|u_{i-2}|_\infty + \frac{1}{2}p^{1+\epsilon_{i-1}-\epsilon_i}|u_{i-1}|_\infty \\ &= p^{\epsilon_{i-2}-\epsilon_i}|u_{i-2}|_\infty + \frac{1}{2}p^{1+\epsilon_{i-1}-\epsilon_i}|u_{i-1}|_\infty \\ &< \frac{1}{2}|u_{i-2}|_\infty + \frac{1}{2}|u_{i-1}|_\infty \end{aligned}$$

If we consider the sequence of elements $s_i = |u_{i-1}|_\infty + 2|u_i|_\infty \geq 1$, we get that

$$\begin{aligned} s_i &= |u_{i-1}|_\infty + 2|u_i|_\infty \\ &< |u_{i-1}|_\infty + |u_{i-2}|_\infty + |u_{i-1}|_\infty = s_{i-1} \end{aligned}$$

and the sequence (s_i) is decreasing. By property (i) we also know that if l is the least common multiple of the reduced denominators of a and b then

$$l \cdot s_i = l\left(|u_{i-1}|_\infty + 2|u_i|_\infty\right) \in \mathbb{Z}$$

since the u_i have unitary norm. So the sequence $(l \cdot s_i)$ is not only decreasing, but of integers ≥ 1. It must terminate for rational inputs. □

We conclude showing how this algorithm ties to Browkin's s.

Corollary 3.45 The quotient q resulting from the p-adic Euclidean division of a and b in $\mathbb{Q}_p$ is exactly $s\left(a/b\right)$.

Proof. Browkin's s applied on a p-adic number x outputs some $s(x)$ such that

(i) $s(x)$ lies in $\mathbb{Z}\left[1/p\right]$.

(ii) $|x - s(x)|_p = \left|\sum_{i=1}^{+\infty} a_i p^i\right|_p < 1 = |1|_p$

(iii) $|s(x)|_\infty < \frac{p}{2}$

For $x = a/b$ we can write

$$\frac{a}{b} = s\left(\frac{a}{b}\right) + \left(\frac{a}{b} - s\left(\frac{a}{b}\right)\right)$$

This would work for any choice of $s\left(a/b\right)$, but we can exploit uniqueness of the couple (q, r) from Theorem 3.43 to prove that $q = s\left(a/b\right)$ and $r/b = a/b - s\left(a/b\right)$. By remarks (iii) and (i), $|a/b|_\infty < p/2$ and $s\left(a/b\right) \in \mathbb{Z}\left[1/p\right]$ respectively. Moreover $r = a - bs\left(a/b\right)$, so by remark (ii)

$$|r|_p = \left|a - bs\left(\frac{a}{b}\right)\right|_p = |b|_p \left|\frac{a}{b} - s\left(\frac{a}{b}\right)\right|_p < |b|_p$$

By uniqueness in Theorem 3.43, $q = s(a/b)$. □

Consider for example $\mathbb{Z}_3$ with representatives $\{-1, 0, +1\}$, the division between

$$a = 2 = -1 + 1p$$
$$b = 26 = -1 + 0p + 0p^2 + 1p^3$$

returns a quotient q that can be calculated as

$$s\left(\frac{a}{b}\right) = s\left(\frac{-1+1p}{-1+1p^3}\right) = s\left(1 + 2p + 2p^2 + 0p^3 + 2p^4 + \dots\right) = 1$$

The result can be verified with formal division between a and b. The choice of s by Browkin is justified a posteriori by this algorithm.

3.11 Continued fractions in local fields

On a general setting for a Lagrange analogue.

Before proceeding, it is relevant to remark that in his article Browkin [5] works with a more general setting. In fact, the title we chose is that of [5]. We will provide a small introduction so that the theory is well understood, and refer to Ramakrishnan and Valenza [33], Artin [2], or the notes by Sutherland [41] for more details.

This Section will show the reasoning behind most of the theory we need for Browkin I and will become useful for a conjecture.
The overwhelmed reader can skip it and only consider $\mathbb{Q}_p$.

Definition 3.46 A **discrete valuation** on a field $\mathbb{K}$ and group Γ is a map $\nu : \mathbb{K} \to \Gamma \cup \{\infty\}$ such that

(i) $\nu(xy) = \nu(x) + \nu(y)$

(ii) $\nu(x+y) \geq \min[\nu(x), \nu(y)]$

(iii) $\nu(x) = \infty$ if and only if $x = 0$

usually written in additive notation. If $\Gamma = (\mathbb{Z}, +)$ this is an integral valuation. Written multiplicatively, ν yields an ultrametric absolute value $|\cdot|_\nu$ on $\mathbb{K}$.

Definition 3.47 A field $\mathbb{K}$ is called **local field** if it has a non-trivial absolute value $|\cdot|$ and is locally compact under the topology induced by it.

From Gouvea [13], $\mathbb{Q}_p$ is locally compact. The norm induced by the multiplicative formulation of ν_p is $|\cdot|_p$, and the idea is that any open set is actually clopen, so open neighbourhood of any $a \in \mathbb{Q}_p$ are also closed.

Proposition 3.48 (Classification of local fields) Let $\mathbb{K}$ be a local field. If $\mathbb{K}$ is archimedean, it is either $\mathbb{C}$ or $\mathbb{R}$. If $\mathbb{K}$ is non archimedean, it is a finite extension of $\mathbb{Q}_p$ if it has characteristic zero or $\mathbb{F}_q((t))$ for t trascendental over $\mathbb{F}_q$ if it has prime characteristic. This holds up to isomorphism.

One can also provide more general results that further the link with $\mathbb{Q}_p$ and $\mathbb{Z}_p$. For example, every DVR $\mathcal{R}$ can be extended to a local field $\mathbb{K} = \mathrm{Quot}(\mathcal{R})$. Further, Hensel's Lemma can be generalised to any complete DVR. However, we are mainly interested in the following.

Lemma 3.49 The ring of integers $\mathcal{O}_\nu$ of a local field $\mathbb{K}$ is a DVR, moreover $\mathcal{O}_\nu = \{x \in \mathbb{K} \text{ with } |x| \leq 1\}$. The unique non-zero prime ideal m_ν of $\mathcal{O}_\nu$ as DVR is $m_\nu = \{x \in \mathbb{K} \text{ with } |x| = 1\}$. Then $\mathbb{K}_\nu = {}^{\mathbb{K}}/_{\mathcal{O}_\nu}$ is the **residue field of** $\mathbb{K}$ **under** ν.

In order to define continued fractions in local fields, we need a final ingredient.

Definition 3.50 Consider a local field $\mathbb{K}$ closed under valuation ν.
Define ι the canonical homomorphism of additive groups $\iota : \mathbb{K} \to {}^{\mathbb{K}}/_{m_\nu}$. An additional mapping $s : \mathbb{K} \to \mathbb{K}$ is $\mathbb{K}$**-compatible** if

(i) $s(0) = 0$

(ii) $\iota s = \iota$

(iii) $s(a) = s(b)$ if $a - b \in m_\nu$

We denote by S the field generated by $s(\mathbb{K})$.

Choosing an adequate $\mathbb{K}$-compatible s will generalise the choice of a floor function for Lagrange's algorithm. Consider the following examples.

(A) The field $\mathbb{K} = \mathbb{F}((x))$ of formal power series over the field $\mathbb{F}$ is closed under the norm induced by $\nu(f) = \mathrm{ord}(f)$. Then $\mathcal{O}_\nu = \mathbb{Z}_p$, m_ν contains formal series of order 1 and the residue field is $\mathbb{F}$. The mapping s can be chosen as

$$s\left(\sum_{n=r}^{+\infty} a_n x^n\right) = \sum_{n=r}^{0} a_n x^n$$

where $a_n \in \mathbb{F}$. Then $s(\mathbb{K}) = \mathbb{F}[x^{-1}]$.

(B) The field $\mathbb{K} = \mathbb{Q}$ of rational numbers is not closed under the norm induced by $v(r) = v_p(r)$. We can still define $\mathcal{O}_v = \mathbb{Z}[1/p]$, m_v as the set of elements of valuation 1, the residue field as $\mathbb{Z}$.

(C) The field $\mathbb{K} = \mathbb{Q}_p$ of p-adic numbers is closed under the norm induced by $v(\alpha) = v_p(\alpha)$. Here $\mathcal{O}_v = \mathbb{Z}_p$, m_v is the set of elements of valuation 1 and the residue field is $\mathbb{Z}$. The mapping s can be chosen as Browkin's s function

$$s\left(\sum_{n=r}^{+\infty} a_n p^n\right) = \sum_{n=r}^{0} a_n p^n$$

where $a_n \in \mathbb{Z}/p\mathbb{Z}$. Then $s(\mathbb{K}) = \mathbb{Z}[1/p]$.

Browkin defines a general continued fraction algorithm for local fields as follows. Pick $\zeta \in \mathbb{K}$, set $\zeta_0 = \zeta$,

$$\begin{cases} b_n = s(\zeta_n) \\ \zeta_{n+1} = \frac{1}{\zeta_n - b_n} \end{cases}$$

stopping whenever $\zeta_n = b_n$. This returns two sequences $(\zeta_n)_I$ and $(b_n)_I$ upon which we can define all structures related to continued fractions (for example convergents C_n, or the A_n and B_n).

The algorithm depends on the choice of s, which is not canonical.

3.12 Browkin's first p-adic algorithm

Construction and first properties of "Browkin I".

The algorithm in Theorem 3.44 is only known to terminate for the set of representatives $\{-(p-1)/2, \dots, (p-1)/2\}$ of $\mathbb{Z}_p$. Browkin I assumes any p-adic integer in such form. If $p = 2$, this set is ill-defined.
A natural approach is trying $\{0, 1\}$ instead, but that degradates Browkin I to Ruban's algorithm, which lacks both properties (P1) and (P2). Moreover, most proofs by Browkin would need to be adapted. It is usually implied that Browkin continued fractions assume p odd.

Algorithm 3.51 (Browkin I) Consider a non-zero $\alpha \in \mathbb{Q}_p$, fix $\alpha_0 = \alpha$ and $b_0 = s(\alpha_0)$. Iteratively define the $(b_i)_I$ and $(\alpha_i)_I$ as

$$\begin{cases} \alpha_{i+1} = \frac{1}{\alpha_i - b_i} \\ b_{i+1} = s(\alpha_{i+1}) \end{cases}$$

If at any step $\alpha_i = b_i$, α_{i+1} is undefined and the two sequences $(b_i)_I$, $(\alpha_i)_I$ terminate (i.e. I is finite).

Let us start with a complete example. For $p = 3$, Browkin I requires $\{-1, 0, +1\}$ as set of representatives. With $a = -1 + p$ and $b = -1 + p^3$, define $\alpha = a/b$ in $\mathbb{Q}_3$.

$$\begin{cases} \alpha_0 = a/b = 1 + 2p + 2p^2 + 0p^3 + 2p^4 + \dots \\ \quad = 1 - 1p + 0p^2 + 1p^3 - 1p^4 + \dots \\ b_0 = 1 \end{cases}$$

$$\begin{cases} \alpha_1 = \frac{1}{\alpha_0 - b_0} = 2p^{-1} + 2 + 1p + 0p^2 + 2p^3 + 0p^4 + \dots \\ \quad = -1p^{-1} - p + 1p^2 - 1p^3 + 1p^4 + \dots \\ b_0 = -1p^{-1} = -\frac{1}{3} \end{cases}$$

$$\begin{cases} \alpha_2 = \frac{1}{\alpha_1 - b_1} = 2p^{-1} + 1 + 2p + 2p^2 + 2p^3 + 2p^4 + \dots \\ \quad = -1p^{-1} - 1 + 0p^2 - 0p^3 + 0p^4 + \dots = -\frac{4}{3} \\ b_0 = -1p^{-1} - 1 = -\frac{4}{3} \end{cases}$$

and the algorithm terminates. This is good news: α is rational in $\mathbb{Q}_3$ and we desire to achieve finiteness property (P1). The continued fraction is in canonical form

$$\alpha = 1 + \cfrac{1}{-1/3 + \cfrac{1}{-4/3}}$$

This converges both in $\mathbb{Q}_3$ and in $\mathbb{R}$, it suffices to backtrack the calculations:

$$\alpha = 1 + \cfrac{1}{-1/3 + \cfrac{1}{-4/3}} = 1 + \frac{1}{-1/3 - 3/4} = 1 - \frac{12}{13} = \frac{1}{13} = \frac{a}{b}$$

This is meaningful since we are in the copy of $\mathbb{Q}$ contained in both $\mathbb{R}$ and $\mathbb{Q}_3$. Of course, one can check that $\alpha = 2/26$ has the same Browkin I expansion as the reduced $\alpha = 1/13$, given by[4]

$$(b_i)_I = (1, -1/3, -4/3)$$
$$(\alpha_i)_I = (2/26, -13/12, -4/3)$$

greatly differing from the real case, where the expansion is $[0, 13]$, clearly representing $1/13$. Back to $\mathbb{Q}_3$, the convergents are

$$C_0 = [b_0] = 1$$
$$C_1 = [b_0, b_1] = b_0 + \frac{1}{b_1} = \frac{b_0 b_1 + 1}{b_1} = -2$$
$$C_2 = [b_0, b_1, b_2] = b_0 + \frac{1}{b_1 + \frac{1}{b_2}} = \frac{2}{26} = \frac{a}{b}$$

equivalently defined by the sequences

$$(A_i)_I = (1, 2/3, 1/9)$$
$$(B_i)_I = (1, -1/3, 13/9)$$

We can provide some nice results on the valuation of the two sequences $(\alpha_n)_I$ and $(b_n)_I$. Consider the following, which will become relevant later.

Lemma 3.52 For $n \geq 1$, $\nu_p(\alpha_n) = \nu_p(b_n)$. If $b_0 \neq 0$, this holds for all n.

[4] It is not hard to write $\alpha_2 = -13/12$ exploiting the proof of Theorem 1.44: period and pre-period are respectively $k = 2$ and $j = 3$, so the equation becomes $(2p^{-1} + 2 + p) + p^3 \frac{2}{1-p^2} = 17/3 - 27/4 = -13/12$.

Proof. Remark that

$$\nu_p(b_0) = \nu_p(s(\alpha_0)) = \begin{cases} \nu_p(\alpha_0) & \text{if } \nu_p(\alpha_0) \leq 0 \\ \nu_p(0) & \text{else} \end{cases}$$

Of course $\nu_p(\beta - s(\beta)) > 0$ for any β, therefore $\nu_p(\alpha_n) = -\nu_p(\alpha_n - s(\alpha_n)) < 0$ and

$$\begin{aligned} \nu_p(b_n) &= \nu_p(s(\alpha_n)) = \nu_p(\alpha_n + s(\alpha_n) - \alpha_n) \\ &= \min\left[\nu_p(\alpha_n), \nu_p(s(\alpha_n) - \alpha_n)\right] = \nu_p(\alpha_n) \end{aligned}$$ □

Remark that all partial quotients b_i (except sometimes the first) always have negative valuation, so previous results from Section 3.2 on the two sequences $(A_i)_I$, $(B_i)_I$ still hold.

Corollary 3.53 Browkin I satisfies property (P0).

Proof. Corollary 3.22 holds for $n \geq N$ with starting index $N = 1$ since all $b_1, b_2, b_3, \ldots$ lie in $\mathbb{Z}[1/p]$ and have negative valuation. □

Having partial quotients in $\mathbb{Z}[1/p]$ is a crucial property for convergence. While not a necessary condition, we possess a great deal of theorems that make it desirable. This adds some constraints to the floor function we can use.

Proposition 3.54 (Unicity) Assume that two sequences $(b_i)_I$ and $(b'_i)_I$ satisfy

(i) the terms lie in $s(\mathbb{Q}_p) = \mathbb{Z}[1/p]$

(ii) they have strictly negative valuation, except eventually the first term

If they are element-wise different, then their limits β, β' are different.

Proof. Assume that they only differ in the first element. By Convergence Theorem I 3.13, $\nu_p(\beta - b_0) > 0$ and $\nu_p(\beta' - b'_0) > 0$ for two well-defined limits β and β'. In particular $b_0 \neq \beta$, $b'_0 \neq \beta'$. If $\beta = \beta'$, b_0 and b'_0 are congruent modulo p and therefore $b_0 = b'_0$, which is absurd. □

The following proves that Browkin I is an ideal candidate for the generalisation of real condinued fractions. Schneider's and Ruban's algorithms algorithms, satisfies finiteness property (P1) and is an ideal candidate for further study into periodicity property (P2).

Theorem 3.55 Browkin I satisfies property (P1).

Proof. Consider $\alpha \in \mathbb{Q} \subset \mathbb{Q}_p$. In Browkin I, the n-th step is defined if and only if $s(\alpha_n) \neq \alpha_n$. Consider the sequences $(b_i)_i$ and $\alpha_i)_i$ and remark that

$$\begin{aligned} \alpha_{n+1} &= (\alpha_n - b_n)^{-1} \\ \alpha_n &= b_n + \alpha_{n+1}^{-1} \end{aligned}$$

where $b_n \in \mathbb{Z}[1/p] \cap (-p/2, p/2)$. We can factor out the power of p at the denominator and write $b_n = c_n p^{-k}$ such that

(i) $|c_n| \leq \frac{1}{2} p^{k+1}$

(ii) $c_n \in \mathbb{Z}$

(iii) $k = -\nu_p(b_n) = -\nu_p(\alpha_n) > 0$

We can also write $\alpha_n = {}^{\gamma_n}/_{p^k\beta_n}$ with γ_n, β_n such that

(iv) the fraction is reduced, i.e. $\gcd(\gamma_n, \beta_n) = 1$

(v) $\gamma_n, \beta_n \in \mathbb{Z}$

(vi) $p \nmid \gamma_n$ and $p \nmid \beta_n$

Similarly, $\alpha_{n+1} = {}^{\gamma_{n+1}}/_{p^m\beta_{n+1}}$ where γ_{n+1} and β_{n+1} still satisfy (iv), (v), (vi) and $m \geq 1$. Combining all these we get that

$$\begin{aligned}\alpha_{n+1} &= (\alpha_n - b_n)^{-1} = p^k\beta_n(\gamma_n - c_n\beta_n)^{-1} \\ &= \frac{\gamma_{n+1}}{p^m\beta_{n+1}}\end{aligned}$$

$$\gamma_{n+1}(\gamma_n - c_n\beta_n) = p^{k+m}\beta_n\beta_{n+1}$$

Due to (iv) and (vi), necessarily $\gamma_{n+1} = \pm\beta_n$ and $\beta_{n+1} = \pm p^{-k-m}(\gamma_n - c_n\beta_n)$. We can provide some bounds on their dimension,

$$|\beta_{n+1}| \leq p^{-k-m}\left(|\gamma_n| + \frac{1}{2}p^{k+1}|\beta_n|\right) < \frac{1}{2}|\gamma_n| + \frac{1}{2}|\beta_n|$$

$$|\gamma_{n+1}| + 2|\beta_{n+1}| < |\beta_n| + (|\gamma_n| + |\beta_n|) = |\gamma_n| + 2|\beta_n|$$

We know from (v) that the sequence $(|\gamma_n| + 2|\beta_n|)_n$ is of natural numbers. It is decreasing and therefore finite. □

An interesting remark is that Lager [17] stated they were strongly motivated in their work on a p-adic Euclidean algorithm by Browkin's proof. In fact, the two are based on the same calculations and idea.

Browkin I is in a strong position for property (P2). Remark that the simplest quadratic irrationals have form $\sqrt{D}$, and both Schneider and Ruban failed on some simple quadratic irrationals (Theorems 3.33 and 3.40). Their study is still open for Browkin I, but Browkin [5] manages to prove a positive result in the case of a finite local field (see the previuos Section for an introduction).

Maintaining the naming conventions we had before, consider the local field $\mathbb{K}$ with valuation ν on it and the field S closure of $s(\mathbb{K})$. Pick an element D in S such that $\sqrt{D} \in \mathbb{K}$ and is irrational over S, i.e. $(S(\sqrt{D}) : S) = 2$. Consider the algorithm Browkin I in this local setting. We will need some preliminary lemmas.

Lemma 3.56 For $\alpha = \sqrt{D}$ irrational in $\mathbb{K}$, $\nu_p(\overline{\alpha}_{n+1}) = -\nu_p(\alpha_n)$ $(n = 0, 1, 2, \dots)$.

Proof. Suppose $\nu_p(\sqrt{D}) \leq 0$. By construction, $b_0 = \alpha_0 - \alpha_1^{-1}$ and

$$\overline{\alpha}_1 = \frac{1}{\overline{\alpha}_0 - b_0} = \frac{1}{\overline{\alpha}_0 - \alpha_0 - \alpha_1^{-1}} = \frac{1}{-2\alpha_0 - \alpha_1^{-1}}$$

and since $\nu\left(\alpha_1^{-1}\right) = \nu\left(b_0 - \alpha_0\right) > 0$ we get

$$\begin{aligned}\nu\left(\overline{\alpha}_1\right) &= \nu\left(\frac{1}{-2\alpha_0 - \alpha_1^{-1}}\right) = -\nu\left(-2\alpha_0 - \alpha_1^{-1}\right) \\ &= -\min\left[\nu\left(-2\alpha_0\right), \nu\left(-\alpha_1^{-1}\right)\right] = -\nu\left(\alpha_0\right)\end{aligned}$$

where $\nu(2) = 0$ (in $\mathbb{Q}_p$ this would be the requirement $p \neq 2$), and

$$\begin{aligned}\nu\left(\overline{\alpha}_2\right) &= \nu\left(\frac{1}{-2\alpha_1 - \alpha_2^{-1}}\right) = -\nu\left(-2\alpha_1 - \alpha_2^{-1}\right) \\ &= -\min\left[\nu\left(-2\alpha_1\right), \nu\left(-\alpha_2^{-1}\right)\right] = -\nu\left(\alpha_1\right)\end{aligned}$$

Assume $\nu(\sqrt{D}) > 0$ instead, then $b_0 = s(\alpha) = 0$, $\alpha_1 = \alpha_0^{-1}$ and $\overline{\alpha}_1 = -\alpha_0^{-1}$. Since $b_1 = \alpha_1 - \alpha_2^1$, where $\nu\left(\alpha_2^{-1}\right) = \nu\left(b_1 - \alpha_1\right) > 0$, we get as before

$$\overline{\alpha}_2 = \frac{1}{\overline{\alpha}_1 - b_1} = \frac{1}{\overline{\alpha}_1 - \alpha_1 - \alpha_2^{-1}} = \frac{1}{-2\alpha_1 - \alpha_2^{-1}}$$

$$\nu\left(\overline{\alpha}_2\right) = \nu\left(\frac{1}{-2\alpha_1 - \alpha_2^{-1}}\right) = -\nu\left(\alpha_1\right)$$

This proves $n = 1$ and $n = 2$. For the inductive step, regardless of $\nu(\sqrt{D})$,

$$\begin{aligned}\nu\left(\overline{\alpha}_{n+1}\right) &= \nu\left(\frac{1}{\overline{\alpha}_n - b_n}\right) = -\nu\left(\overline{\alpha}_n - b_n\right) \\ &= -\min\left[\nu\left(\overline{\alpha}_n\right), \nu\left(b_n\right)\right] \\ &= -\min\left[-\nu\left(\alpha_{n-1}\right), \nu\left(\alpha_n\right)\right] = -\nu\left(\alpha_n\right)\end{aligned}$$ □

In $\mathbb{Q}_p$ we know how to write α_n and $\overline{\alpha_n}$ in canonical form. This still holds in the generic local field, and the two sequences $(P_n)_I$ and $(Q_n)_I$ defining them satisfy the following recursion laws:

$$\begin{cases} P_0 = 0 \\ P_{n+1} = b_n Q_n - P_n \end{cases} \qquad \begin{cases} Q_0 = 1 \\ Q_{n+1} = \frac{D - P_{n+1}^2}{Q_n} \end{cases}$$

Lemma 3.57 For $n \geq 2$,

(i) $\nu(P_n) = \nu(Q_b b_n) = \nu(\sqrt{D})$

(ii) $\nu(P_n - \sqrt{D}) = \nu(\sqrt{D}) - \nu(b_n b_{n+1})$

Proof. Since $\nu(\overline{\alpha}_n) = -\nu(\alpha_n) > 0$ for $n \geq 2$,

$$\nu\left(\frac{2P_n}{Q_n}\right) = \nu\left(\alpha_n + \overline{\alpha}_n\right) = \min\left[\nu\left(\alpha_n\right), \nu\left(\overline{\alpha}_n\right)\right] = \nu(b_n)$$

$$\nu\left(\frac{2\sqrt{D}}{Q_n}\right) = \nu\left(\alpha_n - \overline{\alpha}_n\right) = \min\left[\nu\left(\alpha_n\right), \nu\left(\overline{\alpha}_n\right)\right] = \nu(b_n)$$

which immediately proves (i). For the second part,

$$\nu\left(\frac{P_n+\sqrt{D}}{Q_n}\right) = -\nu(\alpha_n) = -\nu(\alpha_{n-1}) = -\nu(b_{n-1})$$
$$\nu(P_n+\sqrt{D}) - \nu(Q_n) = -\nu(b_{n-1})$$
$$\nu(P_n+\sqrt{D}) = \nu(Q_n) - \nu(b_{n-1}) + \nu(b_n) - \nu(b_n)$$
$$\nu(P_n+\sqrt{D}) = \nu(b_nQ_n) - \nu(b_nb_{n-1}) = \nu(\sqrt{D}) - \nu(b_nb_{n-1})$$ □

In this general setting, Browkin [5] provides a positive result.

Theorem 3.58 If $\mathbb{K}(x)$ is the field of power series over a finite field $\mathbb{K}$, then every element $\sqrt{D} \in \mathbb{K} \setminus S$ such that $D \in s(\mathbb{K}(x))$ has a periodic continued fraction expansion.

Proof. Here quadratic irrationals are those α such that $(S(\alpha) : S) = 2$. We can associate to α two sequences P_n and Q_n defined with the same recursion. Since $s(\mathbb{K}(x)) = \mathbb{K}[x^{-1}]$ and $S = \mathbb{K}(x)$, P_n and Q_n can still be described as before, and $D \in s(\mathbb{K}(x))$ implies $P_n, Q_n \in s(\mathbb{K}(x))$ since $s(\mathbb{K}(x))$ is a ring. Moreover $P_n, Q_n \in \mathbb{K}[x^{-1}]$, so they are polynomials in x^{-1}. They have the same degree due to Lemma , since in our setting ν assigns to each element its index as formal power series. If $\mathbb{K}$ is finite, they can only assume a finite number of values and so do the couples (P_n, Q_n). □

It is clear how Browkin uses the idea behind Lagrange's theorem. However, this result still remains undecided in $\mathbb{Q}_p$ since the last step does not hold and the number of values the couple (P_n, Q_n) can assume is unbounded.

3.13 Browkin's second p-adic algorithm

A brief overview on the algorithm and its properties.

We conclude with Browkin II [6], a further development born from the need to have (empirically) more periodic expansions than Browkin I[5]. The latter is the algorithm of our interest, so this Section will only be a short overview based on remarks on Browkin [6] and Romeo [36].

Consider Browkin's t function,

$$t : \mathbb{Q}_p \longrightarrow \mathbb{Q}$$
$$\alpha = \sum_{i=-k}^{+\infty} a_i p^i \longmapsto t(\alpha) = \sum_{i=-k}^{-1} a_i p^i$$

Like what we did for Browkin's s, the fact that its image is contained in $\mathbb{Z}[1/p]$ will be crucial for convergence.

Lemma 3.59 For all α in $\mathbb{Q}_p$, $t(\alpha)$ lies in $\mathbb{Z}[1/p]$.

[5]This does not mean that Browkin I does not return periodic expansions, but that the period has not been observed yet. The pre-period is also an unknown, making this harder to approach.

Algorithm 3.60 (Browkin II) Set $\alpha_0 = \alpha$ and $b_0 = a_0$.

$$\begin{cases} b_n = s(\alpha_n) & \text{if } n \text{ even} \\ b_n = t(\alpha_n) & \text{if } n \text{ odd and } \nu_p(\alpha_n - t(\alpha_n)) = 0 \\ b_n = t(\alpha_n) - \operatorname{sign}(t(\alpha_n)) & \text{if } n \text{ odd and } \nu_p(\alpha_n - t(\alpha_n)) \neq 0 \\ \alpha_{n+1} = \frac{1}{\alpha_n - b_n} \end{cases}$$

The structure of the algorithm is slightly more complex. As we mentioned above, the properties of t are crucial for convergence. Browkin [6] proves the following relaxation of the requirements from Corollaries 3.22 and 3.23.

Lemma 3.61 Consider $(b_n)_n$ sequence of elements in $\mathbb{Z}\left[1/p\right]$ such that $\nu_p(b_n)$ is zero whenever n is even and negative whenever n is odd. Then the sequence converges in $\mathbb{Q}_p$.

Proof. First, we prove that $B_n \neq 0$ and $\nu_p(B_n) \leq \nu_p(B_{n-1})$, where the equality holds if and only if n is even. We know that $B_0 = 1$ and $B_1 = b_1$, then $B_1 \neq 0$ due to its valuation. It also follows that

$$\nu_p(B_0) = 0 > \nu_p(b_1) = \nu_p(B_1)$$

For the inductive step, we have the hypothesis

$$B_{n-1} \neq 0 \text{ and } \nu_p(B_{n-1}) \leq \nu_p(B_{n-2}) \text{ for some } n \geq 2$$

where the equality holds if and only if n is odd. In both cases

$$\begin{aligned} \nu_p(b_n B_{n-1}) = \nu_p(B_{n-1}) < \nu_p(B_{n-2}) \text{ if } n \text{ even} \\ \nu_p(b_n B_{n-1}) < \nu_p(B_{n-1}) = \nu_p(B_{n-2}) \text{ if } n \text{ odd} \end{aligned}$$

therefore

$$\begin{aligned} \nu_p(B_n) &= \nu_p(b_n B_{n-1} + B_{n-2}) \\ &= \min\left[\nu_p(b_n B_{n-1}), \nu_p(B_{n-2})\right] \\ &= \nu_p(b_n B_{n-1}) \begin{cases} = \nu_p(B_{n-1}) < 0 & \text{for } n \text{ even} \\ < \nu_p(B_{n-1}) < 0 & \text{for } n \text{ odd} \end{cases} \end{aligned}$$

meaning again that $B_n \neq 0$ and the claim follows.
Having proved that, we also have that the limit of the sequence $(B_n^{-1})_I$ is zero since $-\nu_p(B_n)$ diverges to $+\infty$. The sequence of convergents $(C_n)_I$ is Cauchy,

$$C_n - C_{n-1} = \frac{A_n}{B_n} - \frac{A_{n-1}}{B_{n-1}} = \frac{(-1)^n}{B_n B_{n-1}} \to 0$$ □

Corollary 3.62 Browkin II satisfies property (P0).

Proof. Recall that due to Lemma 3.19 the partial quotients $(b_i)_I$ from Browkin II satisfy these requirements. □

Browkin conjectured that this algorithm also satisfied (P1), but the problem was left open in [6] and recently proved by Barbero, Cerruti and Murru [4].

Theorem 3.63 Browkin II satisfies property (P1).

Sketch of proof. The proof is similar to that of Browkin I, but adapted to the use of the functions t and sign. The goal is again to reach a bound of the kind

$$2|B_{n+1}|_\infty < |A_n|_\infty + |B_n|_\infty$$

From here we shorten $|\cdot|_\infty$ to $|\cdot|$. Recall that due to Lemma 3.19 the partial quotients $(b_i)_I$ from Browkin II have null valuation if i is even and negative valuation if i is odd. Moreover, a result analogue to Lemma 3.52 holds. Remark that

$$\nu_p(b_0) = \nu_p(s(\alpha_0)) = \begin{cases} \nu_p(\alpha_0) & \text{if } \nu_p(\alpha_0) \le 0 \\ \nu_p(0) & \text{else} \end{cases}$$

and $\nu_p(\beta - t(\beta)) \ge 0$ for any β, then divide by cases. We then proceed like for Browkin I (Theorem 3.55) and write $b_n = c_n p^{\nu_p(b_n)}$. We have

$$|b_{2i}| = |c_{2i}| < \frac{p}{2} \qquad |b_{2i+1}| = |c_{2i+1}| \le p^l\left(1 - \frac{1}{p^l}\right)$$

where $l = -\nu_p(\alpha_{2i+1})$. The case $n = 2i+1$ here required working with the floor function and is proved in [4, Lemma 10, page 2276]. Write $\alpha_n = \gamma_n / p^{-\nu_p(b_n)}\beta_n$ with γ_n, β_n such that (with the same numbering)

(iv) the fraction is reduced, i.e. $\gcd(\gamma_n, \beta_n) = 1$

(v) $\gamma_n, \beta_n \in \mathbb{Z}$

(vi) $p \nmid \gamma_n$ and $p \nmid \beta_n$

then for $n = 2i$ we can substitute in the equation from the algorithm and get

$$\frac{\gamma_{2i+1}}{p^l\beta_{2i+1}} = \alpha_{2i+1} = \frac{1}{\alpha_{2i} - b_{2i}} = \frac{1}{\frac{\gamma_{2i}}{p^0\beta_{2i}} - c_{2i}p^0}$$

$$\beta_{2i}\beta_{2i+1}p^l = \gamma_{2i+1}(\gamma_{2i} - c_{2i}\beta_{2i})$$

implying by construction $\gamma_{2i+1} = \pm\beta_{2i}$ and $\beta_{2i+1} = \pm p^{-l}(\gamma_{2i} - c_{2i}\beta_{2i})$. It follows

$$|\beta_{2i+1}| \le p^{-l}(|\gamma_{2i}| + |c_{2i}|\,|\beta_{2i}|) < p^{-l}\left(|\gamma_{2i}| + \frac{p}{2}|\beta_{2i}|\right)$$

This is not enough for Browkin II: we need to differentiate even and odd indices. If we go one step further,

$$\frac{\gamma_{2i+2}}{p^0\beta_{2i+2}} = \alpha_{2i+2} = \frac{1}{\alpha_{2i+1} - b_{2i+1}} = \frac{1}{\frac{\gamma_{2i+1}}{p^l\beta_{2i+1}} - c_{2i+1}p^{-l}}$$

$$\beta_{2i+2}\beta_{2i+1}p^l = \gamma_{2i+2}(\gamma_{2i+2} - c_{2i+2}\beta_{2i+2})$$

therefore $\gamma_{2i+2} = \pm\beta_{2i+1}$ and $\beta_{2i+1} = \pm p^{-l}(\gamma_{2i+1} - c_{2i+1}\beta_{2i+1})$, from which we get

$$\begin{aligned} |\beta_{2i+1}| &\le p^{-l}(|\gamma_{2i+1}| + |c_{2i+1}|\,|\beta_{2i+1}|) \\ &\le p^{-l}|\gamma_{2i+1}| + \left(1 - \frac{1}{p^l}\right)|\beta_{2i+1}| = p^{-l}|\gamma_{2i+1}| + |\beta_{2i+1}| - \frac{1}{p^l}|\gamma_{2i+2}| \end{aligned}$$

implying

$$\begin{aligned}|\gamma_{2i+2}| + p^l|\beta_{2i+2}| &\leq |\gamma_{2i+1}| + p^l|\beta_{2i+1}| \\ &< |\gamma_{2i+1}| + p^l\left(p^{-l}|\gamma_{2i}| + p^{-l}\frac{p}{2}|\beta_{2i}|\right) \\ &< |\gamma_{2i+1}| + |\gamma_{2i}| + \frac{p}{2}|\beta_{2i}|\end{aligned}$$

In Theorem 3.55 we bounded both $(\gamma_i)_I$ and $(\beta_i)_I$ at the same time. Here we bound the subsequences of even and odd $(\gamma_i)_I$ instead. Substituting above we also get $|\gamma_{2i+3}| = |\beta_{2i+2}|$, moreover $p^l > p/2 + 1$, therefore

$$\begin{aligned}\left(1 + \frac{p}{2}\right)|\gamma_{2i+3}| + |\gamma_{2i+2}| < p^l|\gamma_{2i+3}| + |\gamma_{2i+2}| &= p^l|\beta_{2i+2}| + |\gamma_{2i+2}| \\ &< |\gamma_{2i+1}| + |\gamma_{2i}| + \frac{p}{2}|\beta_{2i}| = \left(1 + \frac{p}{2}\right)|\gamma_{2i+1}| + |\gamma_{2i}|\end{aligned}$$

$$(p+2)|\gamma_{2i+3}| + 2|\gamma_{2i+2}| = (p+2)|\gamma_{2i+1}| + 2|\gamma_{2i}|$$

The sequence $((p+2)|\gamma_{2i+1}| + 2|\gamma_{2i}|)$ is strictly decreasing, and due to (v) is composed by natural numbers. This implies it ends, meaning that both $(|\gamma_i|)$ and $(|\beta_i|) = (|\gamma_{i+1}|)$ also end. The theorem follows. □

Exactly like for Browkin I, where we had a promising result for the case of finite local fields, the problem of satisfying (P2) is still open.

Appendix A

Algorithms

All algorithms are implemented in SageMath, or Python3 if no data structure from SageMath was required. All were tested on a two-core 11th Gen Intel(R) Core(TM) i7-11370H 3.30GHz and 3.30 GHz.

A.1 Chapter 1

Listing A.1: Expansion for irrationals with the "floor algorithm"

```
1 def irrational_cf(x,n):
2         # x real number to be written as CF
3         # n number of steps
4         for i in range(1,n):
5                 a = math.floor(x)
6                 e = x – a
7                 x = 1/e
```

A.2 Chapter 2

Listing A.2: Expansion for irrationals with the "floor algorithm"

```
1 def irrational_cf(x,n):
2         # x real number to be written as CF
3         # n number of steps
4         for i in range(1,n):
5                 a = math.floor(x)
6                 e = x – a
7                 x = 1/e
```

Listing A.3: Expansion for quadratic irrationals with Lagrange's algorithm

```
def lagrange_cf(x,P,Q,D,n):
    # x real number to be written as CF in the form (P+sqrtD)/Q
    # n number of steps
    for i in range(1,n):
        a = math.floor(x)
        P = a*Q-P
        Q = int((D-P**2)/Q)
        x = (P+math.sqrt(D))/Q
```

A.3 Chapter 3

The following are customised or directly taken from the algorithms openly provided by Murru and Romeo [25] for a recent article [26].

Listing A.4: Schneider's algorithm

```
def Schneider(x,lim):
    part_num=[]
    part_den=[]
    b=x[0]
    part_den.append(b)
    e=(x-b).valuation()
    a=p^e
    part_num.append(a)
    if x-b==0:
        flag=0
    else:
        flag=1
    i=0
    while flag==1 and i<lim:
        i=i+1
        x=(p^e)/(x-b)
        b=x[0]
        part_den.append(b)
        e=(x-b).valuation()
        a=p^e
        part_num.append(a)
    return part_num,part_den
```

Listing A.5: Ruban's floor function

```
    def Ruban_floor(x):
    v=x.valuation()
    b=0
    for i in range (v,1):
    b=b+(x[i]*p^i)
    return K(b)
```

Listing A.6: Ruban's algorithm

```
1   def Ruban(x,lim):
2   b=Ruban_floor(x)
3   exp=[Rational(b)]
4   if x–b==0:
5   flag=0
6   else:
7   flag=1
8   i=0
9   while flag==1 and i<lim:
10  i=i+1
11  x=1/(x–b)
12  b=Ruban_floor(x)
13  exp.append(Rational(b))
14  if x–b==0:
15  flag=0
16  else:
17  flag=1
18  return exp
```

Listing A.7: Browkin's s function

```
1   def Browkin_s(x):
2       v=x.valuation()
3       b=0
4       t=x[v]
5       if x[v]>(p–1)/2:
6           t=–(p–x[v])
7           carry=1
8       else:
9           carry=0
10      b=b+(t*p^v)
11      for i in range (v+1,1):
12          t=x[i]+carry
13          if t>(p–1)/2:
14              t=–(p–t)
15              carry=1
16          else:
17              carry=0
18          b=b+(t*p^i)
19      return b
```

Listing A.8: Browkin's first algorithm

```
def BrowkinI(x,lim):
        b=Browkin_s(x)
        exp=[Rational(b)]
        if x-b==0:
                flag=0
        else:
                flag=1
        i=0
        while flag==1 and i<lim:
                i=i+1
                x=1/(x-b)
                b=Browkin_s(x)
                exp.append(Rational(b))
                if x-b==0:
                        flag=0
                else:
                        flag=1
        return exp
```

Bibliography

[1] Joel Abraham. *Introduction to the p-adic Space*. 2017. arXiv: 1710.08835 [math.HO] (see p. 27).

[2] Emil Artin. *Geometric algebra*. Courier Dover Publications, 2016 (see p. 77).

[3] René-Louis Baire. *Sur les fonctions de variables réelles.* 1899 (see p. 22).

[4] Stefano Barbero, Umberto Cerruti, and Nadir Murru. "Periodic representations for quadratic irrationals in the field of p-adic numbers". In: *Mathematics of Computation* 90.331 (2021), pp. 2267–2280 (see pp. 64, 85, 86).

[5] Jerzy Browkin. "Continued Fractions in Local Fields, I". In: *Demonstratio Mathematica* XI.1 (1978), p. 67 (see pp. 52, 54, 59, 64, 72, 75, 77, 82, 84).

[6] Jerzy Browkin. "Continued Fractions in Local Fields, II". In: *Mathematics of Computation* 70.235 (2001), p. 1281 (see pp. 52, 54, 62, 72, 84, 85).

[7] P. Bundschuh. "p-adische Kettenbrüche und Irrationalität p-adischer Zahlen." In: *Elemente der Mathematik* 32 (1977), pp. 36–40. URL: http://eudml.org/doc/141190 (see p. 72).

[8] Laura Capuano, Nadir Murru, and Lea Terracini. *On the finiteness of $\mathfrak{P}$-adic continued fractions for number fields*. 2021 (see p. 55).

[9] Laura Capuano, Francesco Veneziano, and Umberto Zannier. *An effective criterion for periodicity of l-adic continued fractions*. 2018. arXiv: 1801.06214 [math.NT] (see pp. 69, 73, 74).

[10] Keith Conrad. *The p-adic expansion of rational numbers* (see pp. 7, 23).

[11] Jean Dieudonné. "Sur les fonctions continues p-adiques". French. In: *Bull. Sci. Math., II. Sér.* 68 (1944), pp. 79–95. ISSN: 0007-4497 (see p. 19).

[12] Leonardo Fibonacci. *Liber Abaci*. 1202 (see p. 33).

[13] Fernando Gouvea. *p-adic Numbers: An Introduction*. Springer Berlin Heidelberg, 2003 (see pp. 7, 15, 18–20, 26, 78).

[14] P.A. Grillet. *Abstract Algebra*. Graduate Texts in Mathematics. Springer New York, 2007. ISBN: 9780387715681 (see p. 13).

[15] Kurt Hensel. *Über eine neue Begründung der Theorie der algebraischen Zahlen*. 1897 (see pp. 3, 52).

[16] Bruce Ikenaga. *Periodic Continued Fractions*. 2019. URL: https://sites.millersville.edu/bikenaga/number-theory/periodic-continued-fractions/periodic-continued-fractions.html (see p. 33).

[17] Cortney Lager. "A p-adic Euclidean Algorithm". In: *Rose-Hulman Undergraduate Mathematics Journal* 10.235 (2 2009), p. 1281 (see pp. 75, 82).

[18] Vichian Laohakosol. "A characterization of rational numbers by p-adic Ruban continued fractions". In: *Journal of the Australian Mathematical Society. Series A. Pure Mathematics and Statistics* 39.3 (1985), pp. 300–305 (see p. 73).

[19] W.J. LeVeque. *Topics in Number Theory, Volumes I and II*. Dover Books on Mathematics. Dover Publications, 2012 (see p. 43).

[20] I. G. MacDonald M. F. Atiyah. *Introduction to commutative algebra*. Addison-Wesley Publishing Company, 1969 (see p. 17).

[21] S. MacLane. *Categories for the Working Mathematician*. Graduate Texts in Mathematics. Springer New York, 2013 (see p. 13).

[22] David A. Madore. *A First Introduction to p-adic Numbers*. Revised 7th december 2000 (see pp. 7, 10).

[23] K. Mahler. *Introduction to P-Adic Numbers and Their Functions*. Cambridge Tracts in Mathematics. Cambridge University Press, 1973 (see p. 19).

[24] Kurt Mahler. "On a geometrical representation of p-adic numbers". In: *Annals of Mathematics* (1940), pp. 8–56 (see p. 53).

[25] Nadir Murru and Giuliano Romeo. *p-adic continued fractions*. 2023. URL: https://github.com/giulianoromeont/p-adic-continued-fractions (see p. 89).

[26] Nadir Murru and Giuliano Romeo. *A new algorithm for p-adic continued fractions*. 2023 (see pp. 72, 89).

[27] C.D. Olds. *Continued Fractions*. Anneli Lax New Mathematical Library v. 9. Mathematical Association of America, 1963 (see pp. 33, 43, 51).

[28] Tomohiro Ooto. "Transcendental p-adic continued fractions". In: *Mathematische Zeitschrift* 287.3–4 (Feb. 2017), pp. 1053–1064. ISSN: 1432-1823. DOI: 10.1007/s00209-017-1859-2. URL: http://dx.doi.org/10.1007/s00209-017-1859-2 (see p. 74).

[29] T Pejković. "Schneider's p-adic continued fractions". In: *Acta Mathematica Hungarica* 169.1 (2023), pp. 191–215 (see p. 71).

[30] Aaron Pollack. *Continued Fractions*. 2019. URL: https://mathweb.ucsd.edu/~apollack/6_305S_course_notes_continued_fractions.pdf (see p. 43).

[31] Alexa Pomerantz. *An Introduction to the p-adic Numbers*. 2020 (see p. 7).

[32] A.R. Rajwade. *Squares*. Lecture note series / London mathematical society. Cambridge University Press, 1993 (see p. 22).

[33] Dinakar Ramakrishnan and Robert J Valenza. *Fourier analysis on number fields*. Vol. 186. Springer Science & Business Media, 2013 (see p. 77).

[34] Dave Richeson. *A 10-adic number that is a zero divisor*. December 29, 2008. URL: https://divisbyzero.com/2008/12/29/a-10-adic-number-that-is-a-zero-divisor/ (see p. 18).

[35] Alain M. Robert. *A Course in p-adic Analysis*. Graduate Texts in Mathematics. Springer New York, 2000 (see p. 64).

[36] Giuliano Romeo. "Continued fractions in the field of p-adic numbers". In: *arXiv preprint arXiv:2306.14837* (2023) (see pp. 52, 55, 56, 70, 72, 84).

[37] Анатолий Алъбертович Рубан (Anatoly Albertovich Ruban). Некотые метрицеские свойства *p*-адических йисед *(Certain metric properties of the p–adic numbers)* (see pp. 52, 54).

[38] W.H. Schikhof. *Ultrametric Calculus: An Introduction to P-Adic Analysis*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2007 (see pp. 7, 18, 22).

[39] T. Schneider. *Über p-adische Kettenbruche*. 1969 (see pp. 52, 53).

[40] J.P. Serre. *A Course in Arithmetic*. Graduate Texts in Mathematics. Springer New York, 2012 (see pp. 7, 21).

[41] Andrew Sutherland. *Notes on Number Theory no.9*. 2021. URL: `https://math.mit.edu/classes/18.785/2021fa/LectureNotes9.pdf` (see p. 77).

[42] AJ Van der Poorten. "Schneider's continued fraction". In: (2017), pp. 271–281 (see p. 70).

[43] BMM de Weger. "Periodicity of *p*-adic continued fractions." In: *Elemente der Mathematik* 43 (1988), pp. 112–116 (see p. 72).