Continued fractions in local fields and nested automorphisms

Antonino Leonardis

Scuola Normale Superiore

October 2014

Introduction

Goals

- **First aim**: show the various ways (the ones already known and some new one) available to represent p-adic numbers (and more generally the elements of a local field).
- We will see, among others, the p-adic analogue of classical continued fractions as a particular case of *Nested Automorphism* and the *Approximation Lattices*.
- We will also generalize in these cases, when it is possible, the classical theorems for real continued fractions.
- **Second aim**: exploit the structure of the p-adic integers $\mathbb{Z}_p$, more specifically of the torsion part of its multiplicative group, in order to connect the continued fractions, and also the approximation lattices, to the important theory of cyclotomic fields.

Introduction

Previous works

- The classical theory of continued fractions have a wide literature that can be easily found.
- Continued fractions in local fields have been studied in the papers of **J. Browkin**, where he refers to the two main known p-adic definitions: one from **Schneider**, one from **Ruban**.
- Approximation lattices can be found in the work of **De Weger**.
- The part dealing with the continued fractions in function fields refers to three papers with main authors respectively **Alf. J. van Der Poorten**, **T. G. Berry** and **W. M. Schmidt**.

Introduction

Continued fractions: most general definition

- A **Continued Fraction** in a field $\mathbb{K}$, given an element $x \in \mathbb{K}$, is an expression of the form:

$$x = a_0 + \cfrac{b_1}{a_1 + \frac{b_2}{a_2 + \dots}}$$

  where the a_i and b_i are elements of $\mathbb{K}$.
- More specifically $a_i \in A \subset \mathbb{K}$ for some chosen subset A which should give good approximations for the elements of the field.
- In the special case when all $b_i = 1$ one usually writes $x = [a_0, a_1, \dots]$ (this list can be either finite or infinite).

Introduction

Real continued fractions

- The classical real case of continued fractions is when $\mathbb{K} = \mathbb{R}$, $A = \mathbb{Z}$ and all $b_i = 1$; the a_i are > 0 for $i > 0$.
- In this case, finite continued fractions correspond exactly to **rational numbers**.
- There are exactly two different continued fractions for each rational number; we may restrict to finite continued fractions where the last a_i is > 1, with the exception of $x = [1]$, obtaining a **bijection between continued fractions and real numbers** that can be explicitated via **the integral part algorithm**.

Introduction

Real continued fractions

- **Lagrange's theorem:** the continued fraction of $x \in \mathbb{R}$ is infinite periodic if and only if x is an algebraic irrational number of degree 2.
- To every integer $a \in \mathbb{Z}$ one associates a **matrix** $\widehat{a} \in \mathbb{Z}^{2\times 2}$ of determinant -1 so that, considering such matrices as automorphisms of $\mathbb{P}^1(\mathbb{R}) \supset \mathbb{R}$, we have $\widehat{a_0}[a_1, a_2, \ldots] = [a_0, a_1, a_2, \ldots]$.
- Given a positive rational number $d \in \mathbb{Q}$ that is not a square, the continued fraction of $\sqrt{d}$ is of the form $\left[a_0, \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}\right]$. This result is strongly connected with **Pell's equation** $a^2 - b^2 d = \pm 1$.
- The real continued fraction is also related to **diophantine linear equations** and **Euclid's algorithm** for division.

Introduction

Real continued fractions

- We give a simple application of the continued fractions in the real case, using **Dirichlet's lemma** (let $\xi, Q \in \mathbb{R}$, $Q > 1$; then $\exists p, q \in \mathbb{Z}$, $0 < q < Q$ such that $|p - q\xi| \leq \frac{1}{Q}$).
- Let $n \in \mathbb{N}$, $n > 1$ and let also $b \in \mathbb{N}$, $b > 1$; then $\forall m \in \mathbb{N}$ $\exists k_m \in \mathbb{N}$ s.t. n^{k_m} has at least $m + 1$ base b digits, the first ones of which are 1 followed by m zeroes. Moreover k_m can be found via some continued fraction expansion.
- For instance in standard decimal notation $2^{10} = 1024$ which is very close to a power of 10.
- Another less known example is $3^{21} = 10460353203$.

Structure of $\mathbb{Z}_p^\times$
Exponential and Logarithm

- We have the following power series:

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$
$$\log\left(\frac{1}{1-x}\right) = \sum_{n=1}^{\infty} \frac{x^n}{n}.$$

- $\exp(x)$ converges for $x \in q\mathbb{Z}_p$.
- $\log(y)$ converges for $y \in 1 + p\mathbb{Z}_p$.
- The maps $\exp$ and $\log$ are inverse to each other and give a group isomorphism $(q\mathbb{Z}_p)^+ \cong (1 + q\mathbb{Z}_p)^\times$.

Structure of $\mathbb{Z}_p^\times$

- **Hensel's lemma** gives a primitive $\varphi(q)$-th root of unit ξ which modulo q is a generator of $(\mathbb{Z}/q\mathbb{Z})^\times$.
- $\mathbb{Z}_p^\times \cong \mathbb{Z}_p^+ \times \mathbb{Z}/\varphi(q)\mathbb{Z}$.
- $\lfloor x \rfloor = \xi^{\pi_2(x)} = \lim_{k\to\infty} x^{p^k}$.
- The automorphism group of $\mathbb{Z}_p^\times$ is isomorphic to $\mathbb{Z}_p^\times \times (\mathbb{Z}/\varphi(q)\mathbb{Z})^\times \cong \mathbb{Z}_p^+ \times \mathbb{Z}/\varphi(q)\mathbb{Z} \times (\mathbb{Z}/\varphi(q)\mathbb{Z})^\times$.

Number fields

Theory requirements

- We recall the definition of algebraic and finite field extensions and integral ring extensions and their properties.
- A number field $\mathbb{K}$ is a finite extension of $\mathbb{Q}$. Its ring of integers $\mathbb{Z}_{\mathbb{K}}$ is the integral closure of $\mathbb{Z}$ in $\mathbb{K}$.
- We recall the definition of trace, norm and discriminant for a given number field extension and their properties.

Number fields

Classical results

- Let $m \in \mathbb{Z}$, $m \neq 0, 1$ and squarefree. Then we may consider the **quadratic extension** $\mathbb{Q}[\sqrt{m}] \supset \mathbb{Q}$.
- $\mathbb{Z}_{\mathbb{Q}[\sqrt{m}]} = \mathbb{Z}[\omega]$ where $\omega = \sqrt{m}$ for $m \equiv 2, 3 \pmod 4$ and $\omega = \frac{1+\sqrt{m}}{2}$ for $m \equiv 1 \pmod 4$.
- Let $k \in 2\mathbb{Z}$, $k > 0$. Then we may consider the **cyclotomic extension** $\mathbb{Q}[\zeta_k] \supset \mathbb{Q}$, where ζ_k is a primitive k-th root of unity.
- $\mathbb{Z}_{\mathbb{Q}[\zeta_k]} = \mathbb{Z}[\zeta_k]$.

Number fields

Quadratic extensions of cyclotomic fields

- Let $D \in \mathbb{Z}[\zeta_k]$, $D \neq 0$, $D \notin \left(\mathbb{Z}[\zeta_k]^\times\right)^2$ and D squarefree (i.e. not divisible by a non-unit square). Then $\mathbb{Q}\left[\zeta_k, \sqrt{D}\right]$ is the generic quadratic extension of the cyclotomic field $\mathbb{Q}[\zeta_k]$. The element D can be changed multiplying by the square of a unit.
- Let R be any Dedekind domain (for our purposes, R will be $\mathbb{Z}[\zeta_k]$) and $x, y \in R$. Then $x \equiv y \pmod 2$ if and only if $x^2 \equiv y^2 \pmod 4$.
- Let $x \in \mathbb{K} = \mathbb{Q}\left[\zeta_k, \sqrt{D}\right]$. Then $x \in \mathbb{Z}_{\mathbb{K}}$ if and only if $\mathrm{Tr}^{\mathbb{K}}_{\mathbb{Q}[\zeta_k]}(x) \in \mathbb{Z}[\zeta_k]$ and $\mathrm{N}^{\mathbb{K}}_{\mathbb{Q}[\zeta_k]}(x) \in \mathbb{Z}[\zeta_k]$.

Number fields

Quadratic extensions of cyclotomic fields

- **Characterization theorem**: given $x \in \mathbb{K} = \mathbb{Q}\left[\zeta_k, \sqrt{D}\right]$, $x \in \mathbb{Z}_{\mathbb{K}}$ if and only if it is of the form $\frac{a+b\sqrt{D}}{2}$ with $b \in \mathbb{Q}[\zeta_k]$, $a, b^2 D \in \mathbb{Z}[\zeta_k]$ and $a^2 \equiv b^2 D \pmod{4}$. More precisely:
  - If D is also *ideal-squarefree*, i.e., there is no ideal I such that $I^2 | (D)$, then $b^2 D \in \mathbb{Z}[\zeta_k]$ is equivalent to $b \in \mathbb{Z}[\zeta_k]$.
  - If $D \equiv d^2 \pmod{4}$ (or equivalently $\sqrt{D} \equiv d \pmod{2}$) for some $d \in \mathbb{Z}[\zeta_k]$, then $x \in \mathbb{Z}_{\mathbb{K}}$ if and only if it is of the form $\frac{a+b\sqrt{D}}{2}$ with $b \in \mathbb{Q}[\zeta_k]$, $a, b^2 D \in \mathbb{Z}[\zeta_k]$ and $a \equiv bd \pmod{2}$.
  - If $(2, D) = (1)$ and D is not a quadratic residue modulo 4 then $x \in \mathbb{Z}_{\mathbb{K}}$ if and only if it is of the form $a' + b'\sqrt{D}$ with $b' \in \mathbb{Q}[\zeta_k]$, $a', b'^2 D \in \mathbb{Z}[\zeta_k]$.

Number fields

Quadratic extensions of $\mathbb{Q}[i]$

- When $D \equiv 1 \pmod 4$, $\mathbb{Z}_{\mathbb{K}}$ is a free $\mathbb{Z}[i]$-module with basis $\left\langle 1, \frac{1+\sqrt{D}}{2} \right\rangle$.
- When $D \equiv 3 \pmod 4$, $\mathbb{Z}_{\mathbb{K}}$ is a free $\mathbb{Z}[i]$-module with basis $\left\langle 1, \frac{i+\sqrt{D}}{2} \right\rangle$.
- When $D \equiv i, 2+i, 1+2i, 3+2i, 3i, 2+3i \pmod 4$, i.e. D is coprime to 2 and quadratic non-residue modulo 4, and when $D \equiv 1+i, 3+i, 1+3i, 3+3i \pmod 4$, $\mathbb{Z}_{\mathbb{K}}$ is a free $\mathbb{Z}[i]$-module with basis $\left\langle 1, \sqrt{D} \right\rangle$.
- We don't consider the cases $D \equiv 0, 2, 2i, 2+2i \pmod 4$ in which D cannot be squarefree ($(1+i)^2 | D$).

Number fields

Quadratic extensions of $\mathbb{Q}[\omega]$ ($\omega = \zeta_6 = \frac{1+i\sqrt{3}}{2}$)

- When $D \equiv 1 \pmod 4$, $\mathbb{Z}_{\mathbb{K}}$ is a free $\mathbb{Z}[\omega]$-module with basis $\left\langle 1, \frac{1+\sqrt{D}}{2} \right\rangle$.
- When $D \equiv 3+\omega \pmod 4$, $\mathbb{Z}_{\mathbb{K}}$ is a free $\mathbb{Z}[\omega]$-module with basis $\left\langle 1, \frac{\omega+\sqrt{D}}{2} \right\rangle$.
- When $D \equiv 3\omega \pmod 4$, $\mathbb{Z}_{\mathbb{K}}$ is a free $\mathbb{Z}[\omega]$-module with basis $\left\langle 1, \frac{1+\omega+\sqrt{D}}{2} \right\rangle$.
- When $D \equiv 3, \omega, 1+\omega, 2+\omega, 1+2\omega, 3+2\omega, 1+3\omega, 2+3\omega, 3+3\omega \pmod 4$ and when $D \equiv 2, 2\omega, 2+2\omega \pmod 4$, $\mathbb{Z}_{\mathbb{K}}$ is a free $\mathbb{Z}[\omega]$-module with basis $\left\langle 1, \sqrt{D} \right\rangle$.
- We don't consider the case $D \equiv 0 \pmod 4$ in which D cannot be squarefree.

Nested Automorphisms

Definition

- Let ϕ be $\pm$ an automorphism of $\mathbb{Z}_p^\times$.
- Let A be a set of representatives modulo p containing 0 (for instance $0, 1, \dots, p-1$), that we may suppose algebraic over $\mathbb{Q}$ and integral over $\mathbb{Z}$.
- Let $x \in \mathbb{Z}_p^\times$.
- If $x \in A$ we write $x = [a, 0, 0, \dots]$; otherwise we can write uniquely $x = a + p^k\phi(y)$ with $a \in A \setminus \{0\}$, $k \in \mathbb{N}$, $y \in \mathbb{Z}_p^\times$; then we write $x = [a, 0, \dots, 0, y]$ where between a and y there are exactly $k-1$ zeroes.

Nested Automorphisms

Case $\phi(x) = x$

- The case when $\phi(x) = x$ is the usual power series expansion.
- Let's see a simple result in the case of cyclotomic residues.
- Suppose $p > 2$, let $x \in \mathbb{Z}[\omega]$, and let us write $x = [a_0, \ldots]$ as in the former definition, setting $A = \{0\} \cup \{(p-1)\text{-th roots of unity}\}$ and $\phi(x) = x$; then this expression is either finite or non-periodic.
- In the case $p = 2$ the same result holds for positive integers, while negative ones always end with a period $[1, 1, 1, \ldots]$.

Nested Automorphisms

Algorithms

- Let $x \in \mathbb{Z}_p$ and $k \in \mathbb{N}$, suppose $x - y \in p^k\mathbb{Z}_p$ and let ϕ be an automorphism; then $\phi(x) - \phi(y) \in p^k\mathbb{Z}_p$.
- Let $x, y \in \mathbb{Z}_p^\times$ and let us fix A and ϕ as before; then $\forall k \in \mathbb{N}$ $x - y \in p^k\mathbb{Z}_p$ iff $x = [a_0, a_1, \ldots]$, $y = [b_0, b_1, \ldots]$ and $a_0 = b_0, \ldots, a_{k-1} = b_{k-1}$.
- We may use the usual base p algorithms to determine uniquely the first k digits of any such expression knowing the last k digits of the base p expression and vice versa.

Other expressions

- Product expression: $x = \prod_{n=0}^{\infty} (1 + b_n p^{r_n})$.
- Continued Exponentials: $x = a \exp(p^k y)$.
- Approximation Lattices: we'll analyze this in detail.
- Cyclotomic Approximation Lattices: we'll analyze this in detail.

Other expressions

Approximation Lattices

- Let $x = \sum_{i=0}^{\infty} c_i p^i \in \mathbb{Z}_p$ and let $x_k = \sum_{i=0}^{k} c_i p^i$.
- Its **sequence of Approximation Lattices** (AL) $\{\Lambda_k\}_{k\in\mathbb{N}}$ is defined as:

$$\Lambda_k = \left\{(a,b) \in \mathbb{Z}^2 \,|\, v_p(a-bx) \geq k\right\} = \\ = \left\{(a,b) \in \mathbb{Z}^2 \,\middle|\, a \equiv bx \pmod{p^k}\right\}.$$

- The sequence of AL has the following properties:
  - Λ_k is a lattice of rank 2 in $\mathbb{Z}^2$.
  - $\Lambda_0 = \mathbb{Z}^2$, $\Lambda_{k+1} \subset \Lambda_k$, $\#\left(\Lambda_k/\Lambda_{k+1}\right) = p$.
  - A basis for Λ_k is: $\begin{pmatrix} p^k \\ 0 \end{pmatrix}, \begin{pmatrix} x_k \\ 1 \end{pmatrix}$.

Other expressions

Approximation Lattices

- Suppose that a sequence of lattices of rank 2 $\mathbb{Z}^2 = \Lambda_0 \supset \Lambda_1 \supset \dots$ has the following properties:
  - $\#\left(\Lambda_k/\Lambda_{k+1}\right) = p$ (we say that it *has index* p).
  - $\Lambda_{k+2} \neq p\Lambda_k$ (we say that it is *irreducible*).
  - A basis $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \begin{pmatrix} \gamma \\ \delta \end{pmatrix}$ for Λ_1 (and then also every basis) is such that $(\beta, \delta) = 1$ (notice that $\alpha\delta - \beta\gamma = \pm p$, so $(\beta, \delta) = 1$ or p).
- Then $\exists! x \in \mathbb{Z}_p$ such that $\{\Lambda_k\}_{k\in\mathbb{N}}$ is its sequence of approximation lattices; more precisely, Λ_k has a basis of the form $\begin{pmatrix} p^k \\ 0 \end{pmatrix}, \begin{pmatrix} x_k \\ 1 \end{pmatrix}$ with $x_k \in \{0, \dots, p^k - 1\}$ and $x = \lim_{k\to\infty} x_k$.

Other expressions

Approximation Lattices

- We say that a sequence of AL is *periodic* if $\exists h \in \mathbb{N} \backslash \{0\}$, $k_0 \in \mathbb{N}$ and a linear mapping $\Xi : \mathbb{Q}^2 \to \mathbb{Q}^2$ such that $\Xi(\Lambda_k) = \Lambda_{k+h}$ whenever $k \geq k_0$.
- Periodicity of some continued fraction expansion of $x \in \mathbb{Z}_p$ implies periodicity of the sequence of AL.
- An element $x \in \mathbb{Z}_p$ has periodic sequence of AL if and only if it is rational or quadratic over $\mathbb{Q}$.

Other expressions

Cyclotomic Approximation Lattices

- Let us fix an embedding $\mathbb{Q}(\zeta_{p-1}) \subseteq \mathbb{Q}_p$ and set $p\mathbb{Z}_p \cap \mathbb{Z}[\zeta_{p-1}] = (p, \phi)$.
- We define the **sequence of cyclotomic approximation lattices** (CAL) of $x \in \mathbb{Z}_p$ as:

$$\Lambda_k = \left\{ (a,b) \in \mathbb{Z}[\zeta_{p-1}]^2 \,|\, v_p(a - bx) \geq k \right\}.$$

- The sequence of CAL has the following properties:
  - Λ_k is a lattice in $\mathbb{Z}[\zeta_{p-1}]^2$.
  - $\Lambda_0 = \mathbb{Z}[\zeta_{p-1}]^2$, $\Lambda_{k+1} \subset \Lambda_k$, $\#\left(\Lambda_k / \Lambda_{k+1}\right) = p$.
  - A set of generators for Λ_k is: $\begin{pmatrix} p^k \\ 0 \end{pmatrix}, \begin{pmatrix} \phi^k \\ 0 \end{pmatrix}, \begin{pmatrix} x_k \\ 1 \end{pmatrix}$.

Other expressions

Cyclotomic Approximation Lattices

- Suppose that a sequence of lattices $\mathbb{Z}[\zeta_{p-1}]^2 = \Lambda_0 \supset \Lambda_1 \supset \dots$ has the following properties:
  - $\#\left(\Lambda_k/\Lambda_{k+1}\right) = p$ (we say that it *has index* p).
  - $\forall k \in \mathbb{N}$ holds $\Lambda_k \cap \mathbb{Z}[\zeta_{p-1}] \times \{0\} = (p,\phi)^k \times \{0\}$.
- Then $\exists! x \in \mathbb{Z}_p$ such that $\{\Lambda_k\}_{k\in\mathbb{N}}$ is its sequence of approximation lattices; more precisely, Λ_k has a set of generators of the form $\begin{pmatrix} p^k \\ 0 \end{pmatrix}, \begin{pmatrix} \phi^k \\ 0 \end{pmatrix}, \begin{pmatrix} x_k \\ 1 \end{pmatrix}$ with $x_k \in \{0,\dots,p^k-1\}$ and $x = \lim_{k\to\infty} x_k$.

Other expressions

Cyclotomic Approximation Lattices

- We say that a sequence of CAL is *periodic* (of period h) if $\exists h \in \mathbb{N}\setminus\{0\}$, $k_0 \in \mathbb{N}$ and a linear mapping $\Xi : \mathbb{Q}(\zeta_{p-1})^2 \to \mathbb{Q}(\zeta_{p-1})^2$ such that $\Xi(\Lambda_k) = \Lambda_{k+h}$ whenever $k \geq k_0$.
- An element $x \in \mathbb{Z}_p$ has periodic sequence of CAL if and only if it is rational or quadratic (with a specific condition on discriminant) over $\mathbb{Q}(\zeta_{p-1})$.

Continued Fractions in $\mathbb{Q}_p$

Definition

- Let us consider the following standard set of representatives modulo p: $A = \{0\} \bigcup \{\zeta_{p-1}^j\}_{j=1,\dots,p-1}$
- To every sequence $[a_0, a_1, \dots]_p \in A^{\mathbb{N}}$ with $a_0 \neq 0$ we may associate a unique element $x \in \mathbb{Z}_p^\times$ and vice versa in the following way:

$$x = a_0 - \frac{p^k}{[a_k, a_{k+1}, a_{k+2}, \dots]_p}$$

  where k is the smallest integer > 0 (possibly $+\infty$) such that $a_k \neq 0$.
- The expression $x = [a_0, a_1, \dots]_p$ will be referred to as the **standard continued expression of** x.

Continued Fractions in $\mathbb{Q}_p$

Definition

- This definition is very similar to **Schneider's** one, and both are particular cases of Nested Automorphisms.
- Notice that $a_0 = \lfloor x \rfloor$, justifying the name of integral part in analogy with the real continued fractions.
- If A is another set of residue classes containing zero, we may write x as continued fraction in the same way, but in this case we won't call it the standard expression, and we'll write it as $x = [a_0, a_1, \ldots]_{p,A}$.

Continued Fractions in $\mathbb{Q}_p$

Definition

- We furthermore set:

$$[0, a_1, a_2, \dots]_{p,A} = \frac{[a_1, a_2, \dots]_{p,A}}{p}$$

so that we always have $\forall a_0 \neq 0 : x = a_0 - \frac{p}{[a_1, a_2, \dots]_{p,A}}$.

- Moreover, we may also use Schneider's notation:

$$\begin{aligned} &[a_0, a_1, a_2, a_3, a_4, \dots] = \\ &= [b_1, \dots, b_2, \dots, b_3, \dots] = \\ &= \begin{bmatrix} b_1, & b_2, & b_3, & \dots \\ k_1, & k_2, & k_3, & \dots \end{bmatrix} \end{aligned}$$

where in the second row there are exactly $k_i - 1$ zeroes after each $b_i \neq 0$.

Continued Fractions in $\mathbb{Q}_p$

Matrices

- Let R be the ring of algebraic integers.
- Fixed $k \in \mathbb{Z}$ $(k \neq 0)$ we define a k-**matrix** as a 2×2 matrix with coefficients in R where the second column is divisible by k; the **base matrix** of a k-matrix is the matrix obtained from it dividing the second column by k.
- We also define the k-**transpose** of a k-matrix M as the k-matrix with base matrix given by the transpose of the base matrix of M, and analogously the **Hermitian** k-**transpose**.
- A k-matrix is said k-**symmetric (or** k-**Hermitian)** if it coincides with its (Hermitian) k-transpose, i.e. if its base matrix is symmetric (or Hermitian).
- Notice that the product of two or more k-matrices is still a k-matrix.

Continued Fractions in $\mathbb{Q}_p$

Matrices

- We may associate to each element $a \in A$ a $(-p)$-symmetric $(-p)$-matrix of determinant p in the following way:
  - $0 \longrightarrow \widehat{0} = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$.
  - $a \longrightarrow \widehat{a} = \begin{pmatrix} a & -p \\ 1 & 0 \end{pmatrix}$.
- Considering matrices as automorphisms of $\mathbb{P}^1(\mathbb{Q}_p)$ and $\mathbb{Q}_p$ embedded in the projective line, we may write:

$$[a_0, a_1, \ldots]_{p,A} = \widehat{a}_0[a_1, \ldots]_{p,A}.$$

- It's easy to see that a finite product of them is a $(-p)$-matrix M that we may write as:

$$M = \begin{pmatrix} \lambda & -p\mu \\ \nu & -p\xi \end{pmatrix} = \widehat{a}_1\widehat{a}_2 \ldots \widehat{a}_h.$$

Continued Fractions in $\mathbb{Q}_p$

Matrices

- $\det(M) = p^h$, λ is invertible modulo p, $p^{-k}\nu$ (if exactly the first k matrices of the product are $\widehat{0}$) is invertible modulo p, $p^{-k}\mu$ (if exactly the last k matrices of the product are $\widehat{0}$) is invertible modulo p (also in the ring $\mathbb{Z}[A]$).
- The matrix elements have the following quotients:

$$\begin{aligned}
\lambda/\nu &= [a_1, \dots, a_{h-1}, a_h]_{p,A} \\
\mu/\xi &= [a_1, \dots, a_{h-1}]_{p,A} \text{ if } a_h \neq 0 \\
\lambda/\mu &= [a_h, \dots, a_2, a_1]_{p,A} \\
\nu/\xi &= [a_h, \dots, a_2]_{p,A} \text{ if } a_1 \neq 0.
\end{aligned}$$

  Also, numerator and denominator of these fractions are coprime in the ring $\mathbb{Z}[A]$.

Continued Fractions in $\mathbb{Q}_p$

Matrices

- The $(-p)$-transpose of M is exactly the matrix obtained reversing the order of the factors in the product.
- If A is closed by complex conjugation, the Hermitian $(-p)$-transpose of M is exactly the matrix obtained reversing the order of the factors in the product and taking their complex conjugates.

Continued Fractions in $\mathbb{Q}_p$

Recurrence

- Let $x = \begin{bmatrix} b_0, & b_1, & b_2, & \dots \\ k_0, & k_1, & k_2, & \dots \end{bmatrix}$.
- We may approximate $x \cong \frac{x_i}{y_i}$ using the following recurrence sequences:

$$
\begin{aligned}
x_0 &= 1 \\
x_1 &= b_0 \\
x_{i+1} &= b_i x_i - p^{k_{i-1}} x_{i-1} \\
y_0 &= 0 \\
y_1 &= 1 \\
y_{i+1} &= b_i y_i - p^{k_{i-1}} y_{i-1}
\end{aligned}
$$

Continued Fractions in $\mathbb{Q}_p$

Recurrence

- Suppose $\xi_0 = x = \sqrt{c}$ for some $c \in \mathbb{Z}[\zeta_{p-1}] \cap (\mathbb{Z}_p^\times)^2$. We describe the sequence of partial remainders in the following form:
$$\xi_n = b_n - \frac{p^{k_n}}{\xi_{n+1}} = \frac{P_n + \sqrt{c}}{Q_n}.$$
- P_n, Q_n satisfy the recurrence:
$$P_{n+1} = b_n Q_n - P_n$$
$$Q_{n+1} = \frac{P_{n+1}^2 - c}{p^{k_n} Q_n}$$
- $P_n, Q_n \in \mathbb{Z}[\zeta_{p-1}]_f$
- $Q_n | P_n^2 - c$

Continued Fractions in $\mathbb{Q}_p$

Finiteness

- Let $A \subseteq \mathbb{Z}$ and such that $\forall n \in A : |n| < p$; let $x = [a_0, a_1, \ldots]_{p,A} \in \mathbb{Z}_p^\times$ and suppose that the expression of x is not periodic with period $\overline{(p-1), (1-p)}$. Then $[a_0, a_1, \ldots]_{p,A}$ is finite iff $x \in \mathbb{Q}$.
- Corollary: the standard expression of $x \in \mathbb{Z}_2^\times$ or $x \in \mathbb{Z}_3^\times$ is finite iff $x \in \mathbb{Q}$.
- In the case $\phi(x) = x$, if A is as before, the elements of $\mathbb{Z}$ always have finite Nested Automorphisms expression or a periodic one with period $\overline{(p-1)}$ or $\overline{(1-p)}$.
- An analogue theorem for Ruban CFs holds.

Continued Fractions in $\mathbb{Q}_p$

Finiteness

- Let $\alpha, n \in \mathbb{Z}$ s.t. $(n, \alpha) = 1$. If $\frac{\alpha}{n} = [a_0, \dots, a_h]_{p,A}$, then $\exists! m \in \mathbb{Z}$ s.t. $(m, \alpha) = 1$ and $\frac{\alpha}{m} = [a_h, \dots, a_0]_{p,A}$.
- Corollary: the set of finite continued fractions representing the reciprocals of nonzero rational integers is closed for the mapping $[a_0, \dots, a_h]_{p,A} \to [a_h, \dots, a_0]_{p,A}$.
- A finite standard continued fraction represents an element of $\mathbb{Q}$ if and only if the digits involved in the expression are just $0, 1, -1$.
- Corollary: a rational integer (invertible modulo p) has a finite standard continued fraction iff it's of the form $\pm 1 - np^k$ where $k \in \mathbb{N} \setminus \{0\}$, $n \in \mathbb{Z} \setminus \{0\}$ and $1/n$ has a finite standard continued fraction.

Continued Fractions in $\mathbb{Q}_p$

Periodicity

- A periodic continued fraction is associated to an element of $\mathbb{Q}(A)$ or to an element algebraic of degree 2 over this field.
- Let $x = [\overline{a_0, \ldots, a_h}] \in \mathbb{Z}_p^\times$, and let:

$$\widehat{a}_0 \cdots \widehat{a}_h = \begin{pmatrix} \lambda & -p\mu \\ \nu & -p\xi \end{pmatrix}$$

  then in this case x satisfies the equation:

$$x = \frac{\lambda x - p\mu}{\nu x - p\xi} \Rightarrow \nu x^2 - (\lambda + p\xi)x + \mu p = 0.$$

- An element $x \in \mathbb{Z}_p^\times \backslash \mathbb{Q}[\zeta_{p-1}]$ can have purely periodic standard continued fraction only when it is of the form $x = \frac{P+\sqrt{c}}{Q}$ with $P, Q, c \in \mathbb{Z}[\zeta_{p-1}]$ and c is congruent to a $\frac{\varphi(q)}{2}$-th root of unity modulo p.

Continued Fractions in $\mathbb{Q}_p$

Periodicity

- Let $x = [\overline{a_0, \dots, a_h}]$ be a purely periodic continued fraction, let $\widetilde{x}$ be the other root of the associated quadratic equation. We suppose $a_0 \neq 0$. Then we have:

$$\widetilde{x} = \frac{p}{[\overline{a_h, \dots, a_0}]} = a_0 - [\overline{a_0, a_h, a_{h-1}, \dots, a_1}]$$

- Using this fact we can find solutions to the equation $a^2 - db^2 = \omega p^{k+1}$.
- For $p > 2$ a rational number $r \in \mathbb{Q} \cap \mathbb{Z}_p^\times$ cannot have an infinite purely periodic standard expression.

Continued Fractions in $\mathbb{Q}_p$

Periodicity

- Suppose that $p > 3$ factors in $\mathbb{Z}[A]$ as $p = \alpha\alpha^*$ (also as an ideal); then a finite sequence $a_1, \ldots, a_h$ is the period of the continued fraction of some $x \in \mathbb{Z}[A]$ if the trace of the matrix $M = \widehat{a}_1 \cdots \widehat{a}_h$ equals $2\Re(\alpha^h \zeta)$ for some $(p-1)$th root of 1 ζ.
- **Peculiar Periods:**
  - Palindrome Periods
  - Hermitian Periods
  - Antihermitian Periods
  - Wavelike Periods
  - Regular Periods

Continued Fractions in $\mathbb{Q}_p$

Open questions

- Periodicity and regularity of periods for square roots of rational integers.
- Periodicity of the factors of $p = \alpha\alpha^*$.
- Finding continued fractions like $1 = [1]_5$, $-4 = [1,1]_5$, $-279 = [1,1,1,1,1,1,1]_5$.

Continued Fractions in $\mathbb{Q}_p$

Examples: finite CFs

- Let λ_n be the sequence $1, 0, \ldots, 0$ containing exactly $n-1$ zeroes separated by commas.
- Let $p > 2$. Let $x_n = \frac{1-p^n}{1-p}$. We have: $x_1 = [1]_p$, $x_2 = [1, -1]_p$, $x_{n+2} = [1, -1, -\lambda_n, x_n]_p$.
- Let $p > 2$. Let $\alpha_{hk} = \frac{1-p^h}{1-p^k}$ $(h, k \in \mathbb{N}\backslash\{0\})$, and let $d = |h-k|$. We have: $\alpha_{hk} = [1]_p$ if $h = k$, $\alpha_{hk} = [\lambda_k, -\alpha_{kd}]_p$ if $h > k$, $\alpha_{hk} = [\lambda_h, \alpha_{kd}]_p$ if $h < k$.
- Let $x_n = 2^n - 1$. We have: $x_1 = [1]_2$, $x_{n+1} = [1, \lambda_n, x_n]_2$.
- Let $y_n = \frac{1}{2^n-1}$, $n > 1$. We have: $y_{n+1} = [1, \lambda_n, \lambda_n, 1]_2$.

Continued Fractions in $\mathbb{Q}_p$

Examples: periodic CFs

- $i \in \mathbb{Z}_5$ will be the square root of -1 s.t. $2 - i \in 5\mathbb{Z}_5$.
- $\omega \in \mathbb{Z}_7$ will be the cubic root of -1 s.t. $3 - \omega \in 7\mathbb{Z}_7$.
- Rational integers whose standard continued fraction is periodic (with regular period) but not finite:
  - $2 = [i, \overline{1, -i, -1, -1, i, 1}]_5$
  - $10 \pm 1 = [\pm 1, i, -1, \overline{0, -1, 1, -1}]_5$ (analogously for 50 ± 1, 250 ± 1, etc.)
  - $2 = [\omega^2, \overline{\omega^2, -\omega}]_7$
  - $3 = [\omega, \overline{\omega^2, -\omega}]_7$
- Let A be any set of residues. Let $p > 2$ and let us suppose $(p-1), (1-p) \in A$. Then $-1 = \left[\overline{(p-1), (1-p)}\right]_{p,A}$.

Continued Fractions in $\mathbb{Q}_p$

Examples: periodic CFs

- Square roots of rational integers whose standard continued fraction for $p = 2$ is periodic with hermitian (that is, palindrome) period:
  - $\sqrt{-7} = [1, 1, 1, \overline{1, 0, 1}]_2$
  - $\sqrt{17} = [1, 0, 0, 1, 1, \overline{1, 1, 0, 1, 0, 1, 1}]_2$
- Square roots of rational integers whose standard continued fraction is periodic with regular period:
  - $\sqrt{7} = [1, \overline{-1, -1, 1, 1, 1, -1}]_3$
  - $\sqrt{13} = [1, 1, 1, \overline{1, 1, -1, 0, 1, -1, -1, -1, -1, 1, 0, -1, 1, 1}]_3$
  - $\sqrt{19} = [1, \overline{0, -1, 0, -1, -1, -1, 1, -1, 1, 1, 1, 0, 1, 0, 1, 1, 1, -1, 1, -1, -1, -1}]_3$
  - $\sqrt{-4} = [1, \overline{i, -1, -i}]_5$
  - $\sqrt{-3} = [-\omega^2, \overline{1}]_7$

Continued Fractions in $\mathbb{Q}_p$

Examples: periodic CFs - non periodic CFs

- Purely periodic continued fractions:
  - $\frac{i+\sqrt{-21}}{2} = [\overline{i}]_5$
  - $\frac{1+\sqrt{1+20i}}{2} = [\overline{1, i}]_5$
  - $\frac{\omega+\sqrt{-28+\omega^2}}{2} = [\overline{\omega}]_7$
- Non-periodic continued fractions:
  - $\sqrt{1-i} = [i, -1, -1, 0, -1, -i, i, 1, -1, i, 1, 1, i, -1, 0, 1, i, 0, i, -i, -i, i, 0, \dots]_5$

Continued Fractions in DVFs

Definition

- Let $\mathbb{K}$ be a DVF (Discrete Valuation Field), i.e. the quotient field of a discrete valuation ring.
- Let π be a chosen element of valuation 1
- Let A be a suitable set of representatives modulo π (in the case of function fields we choose the whole base field).
- Given $x \in \mathbb{K}$, there exist unique $k \in \mathbb{Z}$, $x_j \in A$ $(x_k \neq 0)$ such that: $x = \sum_{j=k}^{\infty} x_j \pi^j$
- We define the **integral part** of x as: $\lfloor x \rfloor = \sum_{j=k}^{0} x_j \pi^j$
- We write the **continued fraction**: $x = \lfloor x \rfloor + \frac{1}{y} \to x = [\lfloor x \rfloor, y]$

Continued Fractions in DVFs

Function Fields

- Let $\mathbb{K} = k((x))$, $y = x^{-1}$ so that $k[y] \subseteq k((x))$ is the polynomial ring of integral parts. We suppose that char k is not 2. The results given here hold for any k, not necessarily finite.
- Let $A, B \in k[y]$. Then $\frac{A}{B} = Q + \frac{R}{B} = [Q, B/R]$ for some $Q, R \in k[y]$. By $v(R/B) > 0$ follows $\deg(R) < \deg(B)$, so this is the polynomial euclidean algorithm.
- To every polynomial $a \in k[y]$ one associates a matrix $\widehat{a} \in k[y]^{2\times 2}$ of determinant -1 so that, considering such matrices as automorphisms of $\mathbb{P}^1(\mathbb{K}) \supset \mathbb{K}$, one has $\widehat{a_0}[a_1, a_2, \ldots] = [a_0, a_1, a_2, \ldots]$.

Continued Fractions in DVFs

Function Fields

- A pseudoperiodic continued fraction always represents an element quadratic over $k(y)$.
- Suppose k is finite. Then $x \in \mathbb{K}$ has periodic continued fraction if and only if it is quadratic over $k(y)$.
- Let $D \in k[y]$. Then $\sqrt{D}$ either has a periodic continued fraction of the form $[a_0, \overline{a_1, a_2, \dots, a_2, a_1, 2a_0}]$ or is non-periodic. Again, we get a link with the **functional Pell's equation** $A^2 - B^2 D = 1$.
- **Ruban's** CFs are obtained exactly in this way.

Continued Fractions in DVFs

Function Fields

- With notations as before, the following statements are equivalent:
  1. $\sqrt{D}$ has periodic continued fraction
  2. $\exists A, B \in k[y]$ s.t. $A^2 - B^2 D \in k$
  3. $\infty^+ - \infty^-$ (the difference of the two points at infinity) is a torsion divisor on the related hyperelliptic curve $y^2 = D(x)$
  4. Setting $C = A'/B$, there is an integral of the form:

$$\int \frac{C dy}{\sqrt{D}} = \log(A + B\sqrt{D}) + \text{const.}$$

Summary of accomplished results

- Real continued fractions: classical results to be generalized and a simple application.
- Structure of $\mathbb{Z}_p^\times$, definition of integral part as a cyclotomic representative.
- Algebraic integers in quadratic extensions of cyclotomic fields: some lemmas, characterization theorem, simple applications (examples).
- Expression of p-adic integers: nested automorphisms (special case: power series expansion) and related algorithms.

Summary of accomplished results

- Other expressions: definition of continued exponentials; [cyclotomic] approximation lattices, relation with continued fractions and analogue of Lagrange's theorem.
- Continued fractions in $\mathbb{Q}_p$ and Schneider's definition as special cases of nested automorphisms.
- Continued fractions in $\mathbb{Q}_p$: definition of k-matrices, recurrences definitions and results, finiteness results, periodicity results, open questions and examples.
- Review of continued fractions in discrete valuation fields (special case: Ruban's definition) and in function fields.

Thanks - the exposition is over