Heron's algorithm for Hybrid Continued Fractions and other n-adic algorithms

Cryptography, pseudo-random generators and "unimaginable" numbers

The First Symposium of the International Pythagorean School

Università della Calabria

Dr. Antonino Leonardis

Università della Calabria,

Italy

Sep 26^{th} 2018

Table of contents

Moving on to...

Introduction

p-adic fields and n-adic rings

p-adic numbers, and more in general n-adic numbers for any given integer $n > 1$, can be represented as a power series in the letter p (or n) with exponents growing towards $+\infty$ and digits in a finite set of p (or n) elements, generally $0, 1, \ldots, p-1$.

Introduction

p-adic fields and n-adic rings

p-adic numbers, and more in general n-adic numbers for any given integer $n > 1$, can be represented as a power series in the letter p (or n) with exponents growing towards $+\infty$ and digits in a finite set of p (or n) elements, generally $0, 1, \ldots, p-1$.

For instance, the number $-1 \in \mathbb{Z}$ can be represented as:

$$\ldots 999999 = \sum_{i=0}^{\infty} 9 \cdot 10^i$$

Introduction

p-adic fields and n-adic rings

p-adic numbers, and more in general n-adic numbers for any given integer $n > 1$, can be represented as a power series in the letter p (or n) with exponents growing towards $+\infty$ and digits in a finite set of p (or n) elements, generally $0, 1, \ldots, p-1$.

For instance, the number $-1 \in \mathbb{Z}$ can be represented as:

$$\ldots 999999 = \sum_{i=0}^{\infty} 9 \cdot 10^i$$

because indeed:

$$\begin{aligned} \ldots 999999 + \\ 1 = \\ \ldots 000000 \end{aligned}$$

Introduction

p-adic fields and n-adic rings

In the first case one obtains a field $\mathbb{Z}_p$, which is the completion of rational numbers under the so-called p-adic absolute value. The latter is defined for a fraction $\pm p^t \frac{a}{b}$ where $p \not| a, b$ as:

$$\left| \pm p^t \frac{a}{b} \right|_p = p^{-t}$$

so that in fact positive powers of p converge to 0.

Introduction

p-adic fields and n-adic rings

In the first case one obtains a field $\mathbb{Z}_p$, which is the completion of rational numbers under the so-called p-adic absolute value. The latter is defined for a fraction $\pm p^t \frac{a}{b}$ where $p \not| a, b$ as:

$$\left| \pm p^t \frac{a}{b} \right|_p = p^{-t}$$

so that in fact positive powers of p converge to 0.

Example

- $|1000|_2 = |2^3 \cdot 5^3|_2 = 2^{-3} = \frac{1}{8}$
- $\left| -\frac{24}{25} \right|_5 = |-24 \cdot 5^{-2}|_5 = 5^2 = 25$

Introduction

p-adic fields and n-adic rings

n-adic rings

In the general case $\mathbb{Z}_n$ is a ring with the following properties:

Introduction

p-adic fields and n-adic rings

n-adic rings

In the general case $\mathbb{Z}_n$ is a ring with the following properties:

- $\mathbb{Z}_{p^k} \xrightarrow{\cong} \mathbb{Z}_p$ *for any $k > 1$ by writing all digits of the first ring in base p.*

Introduction

p-adic fields and n-adic rings

n-adic rings

In the general case $\mathbb{Z}_n$ is a ring with the following properties:

- $\mathbb{Z}_{p^k} \xrightarrow{\cong} \mathbb{Z}_p$ *for any $k > 1$ by writing all digits of the first ring in base p.*
- $\mathbb{Z}_{mn} \xrightarrow{\cong} \mathbb{Z}_m \times \mathbb{Z}_n$ *when m and n are coprime as approximants converge in both rings, giving this way the two projections, and the map is invertible by chinese remainder theorem.*

Introduction

p-adic fields and n-adic rings

n-adic rings

In the general case $\mathbb{Z}_n$ is a ring with the following properties:

- $\mathbb{Z}_{p^k} \xrightarrow{\cong} \mathbb{Z}_p$ *for any $k > 1$ by writing all digits of the first ring in base p.*
- $\mathbb{Z}_{mn} \xrightarrow{\cong} \mathbb{Z}_m \times \mathbb{Z}_n$ *when m and n are coprime as approximants converge in both rings, giving this way the two projections, and the map is invertible by chinese remainder theorem.*
- *Thus $\mathbb{Z}_n \cong \prod_{i=1}^{k} \mathbb{Z}_{p_i}$ considering all prime divisors p_i of n. As a side fact, when $k > 1$ the ring has always zero-divisors.*

Introduction

p-adic fields and n-adic rings

Example

Hexadecimal representations of 24-bits RGB colors is just a shortened version of the actual bit representation:

$$FF{\cdot}FF{\cdot}00_{16} = 1111'1111'1111'1111'0000'0000_2 \text{ (yellow)}$$
$$00{\cdot}FF{\cdot}7F_{16} = 0000'0000'1111'1111'0111'1111_2 \text{ (water blue)}$$
$$7F{\cdot}3F{\cdot}00_{16} = 0111'1111'0011'1111'0000'0000_2 \text{ (brown)}$$

Introduction

p-adic fields and n-adic rings

Example

Hexadecimal representations of 24-bits RGB colors is just a shortened version of the actual bit representation:

$$\mathit{FF}\cdot\mathit{FF}\cdot\mathit{00}_{16} = 1111'1111'1111'1111'0000'0000_2 \text{ (yellow)}$$
$$\mathit{00}\cdot\mathit{FF}\cdot\mathit{7F}_{16} = 0000'0000'1111'1111'0111'1111_2 \text{ (water blue)}$$
$$\mathit{7F}\cdot\mathit{3F}\cdot\mathit{00}_{16} = 0111'1111'0011'1111'0000'0000_2 \text{ (brown)}$$

Example

Let's see an example of a zero-divisor:

$$\ldots 8961090041066199773922562599182128906 25.\times$$
$$\ldots 8961090041066199773922562599182128906 24. =$$
$$\ldots 0000000000000000000000000000000000000000.$$

Introduction

Hybrid Continued Fractions

Given a positive integer $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, one can consider the following (generalized) continued fraction:

$$x = [a_0; a_1, a_2, \ldots]_n = a_0 + \cfrac{n}{a_1 + \cfrac{n}{a_2 + \cfrac{n}{\vdots}}}$$

where $a_i \in \mathbb{Z}$, $(a_i, n) = 1$ and $a_i > n$ for $i > 0$.

Introduction

Hybrid Continued Fractions

Given a positive integer $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, one can consider the following (generalized) continued fraction:

$$x = [a_0; a_1, a_2, \ldots]_n = a_0 + \cfrac{n}{a_1 + \cfrac{n}{a_2 + \cfrac{n}{\vdots}}}$$

where $a_i \in \mathbb{Z}$, $(a_i, n) = 1$ and $a_i > n$ for $i > 0$.

This so-called n-continued fraction, not only is convergent for the usual archimedean absolute value, but converges also for any p_i-adic value $(i = 1, \ldots, k)$. Moreover, we can see that a periodic one satisfies the same second degree equation over $\mathbb{Z}$ thus giving the "same" surd in all the related completions.

Introduction

Heron's Algorithm

Newton's method

*The **Newton's method** for finding the roots of a polynomial consists in starting with an approximation x_i of such a root, drawing the tangent at the point (x_i, y_i) to the graph and intersecting this tangent with the x-axis, obtaining x_{i+1}; the sequence obtained by this method converges to a root of the polynomial.*

Introduction

Heron's Algorithm

Newton's method

*The **Newton's method** for finding the roots of a polynomial consists in starting with an approximation x_i of such a root, drawing the tangent at the point (x_i, y_i) to the graph and intersecting this tangent with the x-axis, obtaining x_{i+1}; the sequence obtained by this method converges to a root of the polynomial.*

Heron's Algorithm

*When one considers the polynomial $x^2 - a$ and starts with $x_0 = \lfloor \sqrt{a} \rfloor$, Newton's method just sends x_i to the arithmetic mean between x_i and $\frac{a}{x_i}$ and is known as the **Heron's algorithm** for finding (the geometric mean) $\sqrt{a}$. The intervals between x_i and $\frac{a}{x_i}$ give a so-called **sequence of chinese boxes**.*

Moving on to...

Heron's algorithm for n-continued fractions

Classical theorem

The author proved the following:

Theorem (AL 2017)

Suppose $\sqrt{x}$ has (classical) continued fraction expansion $[x_0 = \lfloor \sqrt{x} \rfloor, x_1, x_2, \ldots]$ with period of length 1 or 2. Apply Heron's algorithm to $a_0 := x_0$ obtaining a sequence $\{a_0, a_1, \ldots\}$. Then a_i is the 2^i-th approximant via the continued fraction. Vice versa, if the continued fraction has period length greater than 2, applying in the same way Heron's algorithm one does not get the same sequence of approximants.

Heron's algorithm for n-continued fractions

Hybrid case

The theorem also holds for our n-continued fractions:

Theorem

Suppose we have a hybrid n-continued fraction expansion $\sqrt{x} = [x_0 = \lfloor \sqrt{x} \rfloor, x_1, x_2, \ldots]_n$ with period of length 1 or 2. Apply Heron's algorithm to $a_0 := n_0$ obtaining a sequence $\{a_0, a_1, \ldots\}$. Then a_i is the 2^i-th approximant via the continued fraction. Vice versa, if the continued fraction has period length greater than 2, applying in the same way Heron's algorithm one does not get the same sequence of approximants.

Heron's algorithm for n-continued fractions

Some examples

Example

#1 For the number $\sqrt{14} = [3;\overline{6}]_5$ *we have:*

$$\begin{aligned} a_0 &= 3 && = [3]_5; \\ a_1 &= \frac{3}{2} + \frac{7}{3} = \frac{23}{6} && = [3,6]_5; \\ a_2 &= \frac{23}{6\cdot 2} + \frac{7\cdot 6}{23} = \frac{1033}{276} && = [3,6,6,6]_5. \end{aligned}$$

Heron's algorithm for n-continued fractions

Some examples

Example

#2 For the number $\sqrt{21} = [4;\overline{8}]_5$ we have:

$$\begin{aligned} a_0 &= 4 && = [4]_5; \\ a_1 &= \frac{4}{2} + \frac{21}{8} = \frac{37}{8} && = [4,8]_5; \\ a_2 &= \frac{37}{8\cdot 2} + \frac{21\cdot 8}{37\cdot 2} = \frac{2713}{592} && = [4,8,8,8]_5. \end{aligned}$$

Heron's algorithm for n-continued fractions

Some examples

Example

#3 For the number $\sqrt{79} = [8; \overline{16}]_{15}$ we have:

$$\begin{aligned} a_0 &= 8 && = [8]_{15}; \\ a_1 &= \frac{143}{16} && = [8, 16]_{15}; \\ a_2 &= \frac{40673}{4576} && = [8, 16, 16, 16]_{15}. \end{aligned}$$

Heron's algorithm for n-continued fractions

Some examples

Example

#4 For the number $\sqrt{22} = [4; \overline{4, 8}]_3$ we have:

$$\begin{aligned} a_0 &= 4 && = [4]_3; \\ a_1 &= \frac{4}{2} + \frac{22}{8} = \frac{19}{4} && = [4, 4]_3; \\ a_2 &= \frac{19}{4 \cdot 2} + \frac{22 \cdot 4}{19 \cdot 2} = \frac{713}{152} && = [4, 4, 8, 4]_5. \end{aligned}$$

Heron's algorithm for n-continued fractions

n-adic algorithms

In the case of p-adic fields the equivalent of Newton's method is known as one of the most important theorems under the name of Hensel's lemma.

Heron's algorithm for n-continued fractions

n-adic algorithms

In the case of p-adic fields the equivalent of Newton's method is known as one of the most important theorems under the name of Hensel's lemma.

Using well known results about Hensel's lemma, one finds out that a precision of p^{-k} is always achieved within $\log_2 k$ steps applying Heron's algorithm.

Heron's algorithm for n-continued fractions

n-adic algorithms

In the case of p-adic fields the equivalent of Newton's method is known as one of the most important theorems under the name of Hensel's lemma.

Using well known results about Hensel's lemma, one finds out that a precision of p^{-k} is always achieved within $\log_2 k$ steps applying Heron's algorithm.

Thus it has applications to p-adic (and n-adic) computations, where it is indeed a very fast algorithm for computing the square root of a number.

Heron's algorithm for n-continued fractions

n-adic algorithms

In this setup, we can implement algorithm for calculation with the following:

Heron's algorithm for n-continued fractions

n-adic algorithms

In this setup, we can implement algorithm for calculation with the following:

Proposition

The fundamental operations (addition, opposite, multiplication, reciprocal) can be turned into a simple algorithm for calculations into the set $\mathbb{Z}_p^\times$ "p-adically approximated to the k-th digit" by the projection (or truncation) into $(\mathbb{Z}/p^k\mathbb{Z})^\times$, i.e. modulo any element with p-adic absolute value less than p^{-k}. A similar result holds for n-adic rings, given any integer $n > 1$. The algorithms can be (and have been by the author) implemented on a computer.

Heron's algorithm for n-continued fractions

n-adic algorithms

Moreover:

Heron's algorithm for n-continued fractions

n-adic algorithms

Moreover:

Proposition

Any advanced operation which requires approximations by Hensel's lemma (and satisfying its hypotheses) can be (and have been by the author) as well implemented as an algorithm.

Some common examples are:

- *quadratic surds;*
- *exponentials and logarithms (or other functions determined by a power series) within their convergence radius.*

Moving on to...

Randomizing p-adic methods

Randomizing p-adic methods

p-adic randomizers

Remark

The Montecarlo method for calculating a probability, which is used in physics abundantly, can be used in reverse to verify that an experiment is random enough.

Randomizing p-adic methods

p-adic randomizers

Remark

The Montecarlo method for calculating a probability, which is used in physics abundantly, can be used in reverse to verify that an experiment is random enough.

Example

We can try the following randomizing methods given a seed $s \in \mathbb{N}$ (and ignoring trivial endings):

- *considering $\exp(ps)$;*
- *considering $\sqrt{1+ps}$;*
- *iterating s times the function $x_i \to x_{i+1} = \sqrt{x_i}$.*

Randomizing p-adic methods

Square root p-adic randomizer

We implement the third method with 5-adics (starting from $11_5 = 6$), creating a list of random couples (x, y) with $0 <= x <= 15624 = 444444_5$ and $0 <= y <= 15624 = 444444_5$.

Randomizing p-adic methods

Square root p-adic randomizer

We implement the third method with 5-adics (starting from $11_5 = 6$), creating a list of random couples (x, y) with $0 <= x <= 15624 = 444444_5$ and $0 <= y <= 15624 = 444444_5$.

Grouping together 40 of those couples, we count how many satisfy $x^2 + y^2 <= 15625$, and multiply the ratio by 4: as the probability of such inequality is approximately $\pi/4$ (the area of the defined figure), we compare the statistic values with a random distribution around π.

Randomizing p-adic methods

Square root p-adic randomizer

We implement the third method with 5-adics (starting from $11_5 = 6$), creating a list of random couples (x, y) with $0 <= x <= 15624 = 444444_5$ and $0 <= y <= 15624 = 444444_5$.

Grouping together 40 of those couples, we count how many satisfy $x^2 + y^2 <= 15625$, and multiply the ratio by 4: as the probability of such inequality is approximately $\pi/4$ (the area of the defined figure), we compare the statistic values with a random distribution around π.

We iterate 100 times this procedure and obtain a statistic with average 3.115 and variance 0.1, confirming the pseudo-randomness of the algorithm by the 3rd law of pseudo-randomness (*cannot be distinguished from a random one by a chosen method*).

Moving on to...

Other applications

Elementary cryptography

We observe that:

Other applications

Elementary cryptography

We observe that:

Proposition

Let us consider the strings of k elements in the set $0, 1, \ldots, n-1$, i.e. elements of $S = \mathbb{Z}/n^k\mathbb{Z}$. Fixing an element $y \in (\mathbb{Z}/n^k\mathbb{Z})^\times$ (it suffices that the last digit is coprime to n), this determines a simple symmetric encrypting key $S \to S$ by normal n-adic multiplication:

$$x \to xy$$

where the decrypting key is simply y^{-1}.

Other applications

Elementary cryptography

We observe that:

Proposition

Let us consider the strings of k elements in the set $0, 1, \ldots, n-1$, i.e. elements of $S = \mathbb{Z}/n^k\mathbb{Z}$. Fixing an element $y \in (\mathbb{Z}/n^k\mathbb{Z})^\times$ (it suffices that the last digit is coprime to n), this determines a simple symmetric encrypting key $S \to S$ by normal n-adic multiplication:

$$x \to xy$$

where the decrypting key is simply y^{-1}.

It is likely that studying further these kind of algorithms one can find better encryption methods.

Other applications

Elementary cryptography

Example

Decimal numbers from 0000 *to* 9999 *can be encrypted using the key* 73*, which has as a reverse key the number* 137 *by the well known peculiar factorization* $73 \times 137 = 10001$*.*

Other applications

Elementary cryptography

Example

Decimal numbers from 0000 *to* 9999 *can be encrypted using the key* 73*, which has as a reverse key the number* 137 *by the well known peculiar factorization* $73 \times 137 = 10001$*.*

Example

Alphanumeric strings can be considered as 37*-adic numbers with digits* $0, \ldots, 9, A, \ldots, Y, Z, \_$ *(the last being a separator) and therefore encrypted using the properties of* $\mathbb{F}_{37} = \mathbb{Z}/37\mathbb{Z}$*.*

Other applications

Big basis systems

Example

Using bit-mapped bases, we may as well consider the possibility to apply our cryptography methods to such expressions.

Other applications

Big basis systems

Example

Using bit-mapped bases, we may as well consider the possibility to apply our cryptography methods to such expressions.

We know that using basis $2^{100\times 100}$ *(which corresponds to representing digits with a* 100×100 *black and white bitmap), or any other power of* 2*, a number is invertible if and only if the last digit is odd; the only possible issue in the division algorithm is effectively calculating the reciprocal of this last digit, but this can be done by considering for this digit the* 2*-adic expansion and applying* 2*-adic division.*

Other applications

Last digits of unimaginable numbers

For some so-called "unimaginable" numbers, like Graham's number, we may calculate the last digits using n-adic numbers.

Other applications

Last digits of unimaginable numbers

For some so-called "unimaginable" numbers, like Graham's number, we may calculate the last digits using n-adic numbers.

Example

In $\mathbb{Z}_{10}$ there are two non trivial idempotent elements (whose sum is 1 and product is 0) given by:

$$16^{5^\infty} := \lim_{k\to\infty} 16^{5^k} = \ldots 0774374008178710937 6;$$

$$5^{2^\infty} := \lim_{k\to\infty} 5^{2^k} = \ldots 9225625991821289062 5.$$

Their last k digits are in common with the unimaginable numbers 16^{5^k} and 5^{2^k}, given that k is big enough to justify the "unimaginable" attribute.

Other applications

Last digits of unimaginable numbers

We recall that the Graham number is defined as:

$$a \uparrow b = a * a * a \ldots * a \ [b \text{ times}] = a^b$$

$$a \uparrow\uparrow b = a \uparrow a \uparrow a \ldots \uparrow a \ [b \text{ times}]$$

$$a \uparrow^k b = a \uparrow^{k-1} a \uparrow^{k-1} a \uparrow^{k-1} a \ldots \ [b \text{ times}]$$

$$g_0 = 4$$

$$g_1 = 3 \uparrow\uparrow\uparrow\uparrow 3$$

$$g_k = 3 \uparrow^{g_{k-1}} 3$$

$$G = g_{64}$$

Other applications

Last digits of unimaginable numbers

We recall that the Graham number is defined as:

$$a \uparrow b = a * a * a \ldots * a \ [b \text{ times}] = a^b$$
$$a \uparrow\uparrow b = a \uparrow a \uparrow a \ldots \uparrow a \ [b \text{ times}]$$
$$a \uparrow^k b = a \uparrow^{k-1} a \uparrow^{k-1} a \uparrow^{k-1} a \ldots \ [b \text{ times}]$$
$$g_0 = 4$$
$$g_1 = 3 \uparrow\uparrow\uparrow\uparrow 3$$
$$g_k = 3 \uparrow^{g_{k-1}} 3$$
$$G = g_{64}$$

This literally unimaginable number was involved in the first proof for Graham's problem in Conway's theory, even though it has been now substituted by the smaller (but still insanely big) number $2 \uparrow\uparrow 2 \uparrow\uparrow 2 \uparrow\uparrow 9$.

Other applications

Last digits of unimaginable numbers

Example (Last digits of Graham's number)

We now consider the problem of computing the last digits of $G = g_{64}$.

Other applications

Last digits of unimaginable numbers

Example (Last digits of Graham's number)

We now consider the problem of computing the last digits of $G = g_{64}$. *It can be proved that the following algorithm:*

$$a_0 = 3;\ x_i = a_i \ (\mathit{mod}\ 10^i);\ a_{i+1} = 3^{x_i};\ x = \lim_{i \to +\infty} x_i$$

converges in $\mathbb{Z}_{10}$ *and that also* $g_\infty := \lim_{i \to \infty} g_i$ *exists and* $x = g_\infty$.

Other applications

Last digits of unimaginable numbers

Example (Last digits of Graham's number)

We now consider the problem of computing the last digits of $G = g_{64}$. *It can be proved that the following algorithm:*

$$a_0 = 3;\ x_i = a_i \ (\mathit{mod}\ 10^i);\ a_{i+1} = 3^{x_i};\ x = \lim_{i \to +\infty} x_i$$

converges in $\mathbb{Z}_{10}$ *and that also* $g_\infty := \lim_{i\to\infty} g_i$ *exists and* $x = g_\infty$. *This number can be seen to be the fixed point for the equation* $x = 3^x$.

Other applications

Last digits of unimaginable numbers

Example (Last digits of Graham's number)

We now consider the problem of computing the last digits of $G = g_{64}$. *It can be proved that the following algorithm:*

$$a_0 = 3;\ x_i = a_i \ (\mathit{mod}\ 10^i);\ a_{i+1} = 3^{x_i};\ x = \lim_{i \to +\infty} x_i$$

converges in $\mathbb{Z}_{10}$ *and that also* $g_\infty := \lim_{i\to\infty} g_i$ *exists and* $x = g_\infty$. *This number can be seen to be the fixed point for the equation* $x = 3^x$.

Observing that the 10*-adic difference* $G - g_\infty$ *ends with an "unimaginable" number of zeroes, their last digits are the same for all practical purposes.*

Other applications

Last digits of unimaginable numbers

Remark

More generally, an infinite tetration $k \uparrow\uparrow \infty := \lim_{j\to\infty} k \uparrow\uparrow j$ *always converges in any* n*-adic ring.*

Other applications

Last digits of unimaginable numbers

Remark

More generally, an infinite tetration $k \uparrow\uparrow \infty := \lim_{j\to\infty} k \uparrow\uparrow j$ *always converges in any* n*-adic ring.*

This number can be seen too as a fixed point:

Other applications

Last digits of unimaginable numbers

Remark

More generally, an infinite tetration $k \uparrow\uparrow \infty := \lim_{j\to\infty} k \uparrow\uparrow j$ *always converges in any* n*-adic ring.*

This number can be seen too as a fixed point:

$$x = k^x \to x = k \uparrow\uparrow \infty.$$

Other applications

Last digits of unimaginable numbers

Remark

More generally, an infinite tetration $k \uparrow\uparrow \infty := \lim_{j\to\infty} k \uparrow\uparrow j$ *always converges in any* n*-adic ring.*

This number can be seen too as a fixed point:

$$x = k^x \to x = k \uparrow\uparrow \infty.$$

This is of course a generalization for $g_\infty = 3 \uparrow\uparrow \infty$.

Moving on to...

Conclusions

Thanks everyone for participating to this Symposium

Papers

- Jerzy Browkin, *Continued fractions in local fields, I*, Demonstratio Mathematica **1** (1978), Vol. XI, pp. 67–82
- Jerzy Browkin, *Continued fractions in local fields, II*, Mathematics of Computation **235** (2000), Vol. 70, pp. 1281–1292
- A. L., *Cyclotomic Approximation Lattices*, International Journal of Number Theory, Volume No.11, Issue No. 2., March 2015 (DOI: 10.1142/S1793042115500293)
- A. L., *Simple applications of continued fractions and an elementary result about Heron's algorithm*, waiting for publication.
- Evan O'Dorney, *Continued fractions and linear fractional transformations*, Integers 15 (2015), Paper No. A1, 23 pp.

Thesis

- A. L., *Il teorema di Skolem Mahler Lech*, First degree thesis (2006, http://uz.sns.it/~antonino/SMLTheorem.pdf)
- A. L., *Continued Fractions in Local Fields and Nested Automorphisms*, PhD thesis (2014)

Books

- Oded Goldreich, *A Primer on Pseudorandom Generators*, University Lecture Series Vol. 55, AMS
- Oskar Perron, *Die Lehre von den Kettenbrüchen*
- Marco Ripà, *La strana coda della serie* $n \uparrow n \uparrow \ldots \uparrow n$