Numeration: Mathematics and Computer Science
March 23–27, 2009

Lectures

Some arithmetic properties of automatic sequences

JEAN-PAUL ALLOUCHE (LRI, CNRS, Université Paris-Sud)

We explore some links between automata theory and number theory. We first recall several equivalent definitions of automatic sequences. Then we study Dirichlet series with automatic coefficients, and we give applications to computing curious infinite products and to proving the existence of logarithmic frequencies for automatic sequences. We then study formal power series, with coefficients in a finite field, that are algebraic over the rational functions on this field (Christol's, Salon's, Sharif-Woodcock's and Harase's theorems). We show how this permits to prove in a very simple way a theorem of Deligne on diagonals of algebraic formal power series. We conclude with a quick survey of transcendence results for real numbers generated by automata.

[1] B. Adamczewski, Y. Bugeaud, *On the decimal expansion of algebraic numbers*, Fiz. Mat. Fak. Moksl. Semin. Darb. **8** (2005), 5–13.

[2] J.-P. Allouche, H. Cohen, *Dirichlet series and curious infinite products*, Bull. Lond. Math. Soc. **17** (1985), 531–538.

[3] J.-P. Allouche, M. Mendès France, J. Peyrière, *Automatic Dirichlet series*, J. Number Theory **81** (2000), 359–373.

[4] J.-P. Allouche, J. Shallit, *Automatic sequences. Theory, Applications, Generalizations*, Cambridge University Press, 2003.

Ergodic theory of numbers

KARMA DAJANI (Universiteit Utrecht)

In this course we give an introduction to the ergodic theory behind common number expansions, like expansions to integer and non-integer bases, and continued fraction expansion. Starting with basic ideas in ergodic theory, we apply these to the familiar expansions mentioned above in order to obtain new and old results in an elegant and straightforward manner.

[1] K. Dajani and C. Kraaikamp, *Ergodic theory of numbers*, Carus Mathematical Monographs, 29. Mathematical Association of America, Washington, DC, 2002.

[2] M. Iosifescu and C. Kraaikamp, *Metrical theory of continued fractions*, Mathematics and its Applications, 547. Kluwer Academic Publishers, Dordrecht, 2002.

Exact computations with an arithmetic known to be approximate

JEAN-MICHEL MULLER (LIP, CNRS, ENS Lyon)

Floating-point (FP) arithmetic was designed as a mere approximation to real arithmetic. And yet, since the behaviour of each operation is fully specified by the IEEE-754 standard for floating-point arithmetic, FP arithmetic can also be viewed as a mathematical structure on which it is possible to design algorithms and proofs. We give some examples that show the interest of that point of view.

[1] S. Boldo, J.-M. Muller, *Some Functions Computable with a Fused-mac*, in: Paolo Montuschi and Eric Schwarz, editors, Proceedings of the 17th Symposium on Computer Arithmetic, Cape Cod, 2005, 52–58.

[2] S. Boldo, *Pitfalls of a Full Floating-Point Proof: Example on the Formal Proof of the Veltkamp/Dekker Algorithms*, in: Proceedings of the third International Joint Conference on Automated Reasoning (IJCAR), Seattle, 2006, 52–66.

[3] S. Boldo, G. Melquiond, *Emulation of FMA and Correctly Rounded Sums: Proved Algorithms Using Rounding to Odd*, IEEE Transactions on Computers **57** (2008), 462–471.

[4] N. Brisebarre, J.-M. Muller, *Correctly rounded multiplication by arbitrary precision constants*, IEEE Transactions on Computers **57** (2008), 165–174.

[5] T. Ogita, S. Rump, S. Oishi, *Accurate Sum and Dot Product*, SIAM J. Scientific Computing **26** (2005), 1955–1988.

[6] S. Pion, G. Melquiond, *Formally certified floating-point filters for homogeneous geometric predicate*, Theoret. Informatics Appl. **41** (2007), 57–70.

Invited talks

Finiteness and periodicity of beta expansions – number theoretical and dynamical open problems

SHIGEKI AKIYAMA (Niigata University)

In this talk, I shall give a survey on beta expansion and related dual tiling, putting stress on open problems of my taste. I will start from the basic definition and ergodic properties and then talk on:

1. Dynamical norm conjecture and connectedness of tiles
2. Finiteness condition and shift radix system
3. Weak finiteness condition, height reducing problem and Pisot conjecture
4. Periodic orbits on the boundary

Cobham's theorem and its extensions

JASON BELL (Simon Fraser University)
(joint work with Boris Adamczewski)

Cobham's thoerem is a fundamental result in the theory of automatic sequences, which states that a sequence that is automatic with respect to two multiplicatively independent bases is in fact eventually periodic. We give some of the history behind this result including some extensions and conjectured extensions. We also show the relationship between automatic sequences and fractals (self-similar sets, with self-similarity suitably defined) and describe a recent analogue of Cobham's theorem for fractals. More specifically, we show that a compact subset of the real numbers that is self-similar with respect to two multiplicatively independent bases is a finite union of closed intervals.

Discrete Geometry and Numeration

VALÉRIE BERTHÉ (LIRMM, CNRS, Université Montpellier 2)

The aim of this lecture is to show how discrete geometry and numeration systems can interact through the study of the most basic objects in discrete geometry, namely arithmetic discrete planes. In word combinatorics, Sturmian words and regular continued fractions are known to provide a very fruitful interaction between arithmetics, discrete geometry and symbolic dynamics. Recall that Sturmian words can be defined as infinite words which code irrational discrete lines over a two-letter alphabet. Most combinatorial properties of Sturmian words can be described in terms of the continued fraction expansion of the slope of the discrete line that they code. We show how to extend this interaction to higher dimensions. We thus generalize the notions of free group morphisms (among them substitutions), of Sturmian words and to work with a multi-dimensional version of the Euclidean algorithm, that is, a multi-dimensional continued fraction algorithm. The role played respectively by words, substitutions, and classical continued fractions will be played by stepped surfaces, dual maps and Brun algorithm. Special focus will be given on a generation method for discrete planes based on a numeration system associated with Brun algorithm.

Some numeration questions encountered in cryptology

GUILLAUME HANROT (LORIA, INRIA Nancy Grand-Est)

In this talk, we shall try to review some links between numeration systems and cryptography. Numeration problems appear naturally to have fast operations: design of efficient addition chains for exponentiation – a widely used building block in cryptosystems, fancy representations of integers to get faster arithmetic. We shall also study some less obvious occurrences of "numeration techniques" in number theoretic algorithms related to cryptography, eg. point counting on elliptic curves.

Applications of Digital Expansions in the Efficient Implementation of Cryptosystems

CLEMENS HEUBERGER (Technische Universität Graz)

Elliptic curve cryptography is based on computing scalar multiples nP of a point P in the point group of an elliptic curve over a finite field, as it is believed to be hard to compute n from the knowledge of P and nP.

This operation can be performed by using a binary expansion of n and computing nP by a variant of Horner's scheme, the double-and-add algorithm. The number of doublings on the curve depends

on the length of the expansion, whereas the number of additions corresponds to the Hamming weight of the expansion, i.e., the number of non-zero digits.

Various improvements are available: for instance, signed binary expansions may be used as subtraction is as cheap as addition; sliding window methods (somewhat related to higher bases of the expansions), usage of complex bases corresponding to endomorphisms of the curve, "joint expansions" related to linear combinations of points ...

The talk will give a survey on related results.

Integer base expansions of prime numbers

CHRISTIAN MAUDUIT (IML, Université de la Méditerranée Aix–Marseille II)

We will present recent results and open problems concerning the q-adic representation of prime numbers. In particular we proved in a joint work with Joel Rivat (see `http://annals.math.princeton.edu/issues/2008/FinalFiles/MauduitRivatFinal.pdf`) that, under some trivial necessary conditions, the sum of digits function of prime numbers is well distributed in arithmetic progressions, solving a conjecture due to Alexander Gelfond (1967). The technics we use to estimate the associated exponential sums can also be applied to give precise estimates for the number of prime numbers with an average sum of digits (joint work with Michael Drmota and Joel Rivat, see `http://www.dmg.tuwien.ac.at/drmota/`).

Développement décimal des nombres algébriques

TANGUY RIVOAL (Insitut Fourier, CNRS, Université Grenoble)

My talk will focus on the following result, proved in 2004 by Bailey, Borwein, Crandall and Pomerance: Let $B(x, n)$ denotes the number of 1 in the binary expansion of a real number $x \in [0, 1)$ up to the nth digit; then for any algebraic number x of degree $d \geq 2$, there exists a constant $c(x, d) > 0$ such that $B(x, n) \geq c(x, d) n^{1/d}$.

Rosen continued fractions and Veech groups

THOMAS A. SCHMIDT (Oregon State University)

This is an expository talk, aimed at an audience that has possibly heard of neither "Rosen continued fractions" nor "Veech groups". An emphasis will be placed on explicit examples.

It is well known that simple continued fractions are closely related to the group $SL(2, \mathbb{Z})$. In his 1952 Ph.D. dissertation, D. Rosen introduced a type of continued fractions similarly related to each of an infinite family of matrix groups earlier studied by E. Hecke. The partial quotients of these Rosen continued fractions are algebraic integers, whose degree over the rationals goes to infinity with the index of the group involved. The Rosen fractions have recently attracted increasing research interest.

The dynamics of a billiard ball inside a Euclidean polygon can be studied in terms of the paths on a related flat surface. For example, the surface corresponding to billiards in a square turns out to be the square torus. In 1989, W. Veech showed that when the group of appropriate self-maps of this surface is in a sense large, then the dynamics has optimal (ergodic theoretic) properties. This notion of size is expressible in terms of a group of 2-by-2 matrices related to the derivatives of these maps. Veech's original examples with optimal dynamics have their corresponding groups being (directly related to) the Hecke groups. P. Arnoux and P. Hubert showed in 2000 that one can thus use Rosen(-like) continued fractions to study the dynamics.

Contributed talks

A Residue Approach of the Finite Fields Arithmetics

JEAN-CLAUDE BAJARD (LIRMM, Université Montpellier 2)

Finite fields arithmetic is one of the challenges in current computer arithmetic. It occurs, in particular, in cryptography where the needs increase with the evolution of the technologies and also of the attacks. Through our research, we have proposed different systems based on residues representations. Different kinds of finite fields are concerned with. For each of them, some specificities of the representations are exploited to ensure the efficiency, as well as for the performances, than for the robustness to side channel attacks. In this paper, we deal with three similar approaches: the first one is dedicated to prime field using residue number systems, a seconde one concerns extension finite fields of characteristic two, the last one discusses of medium characteristic finite fields. The main interest of these systems is their inherent modularity, well suited for circuit implementations.

Resemblance and difference between beta-integers and ordinary integers

LUBOMÍRA BALKOVÁ (Czech Technical University in Prague)
(joint work with J.-P. Gazeau, K. Klouda, and E. Pelantová)

Beta-integers, an analogy of integers when expanding real numbers in a non-integer base β, supersede in quasicrystalline studies "crystallographic" ordinary integers. When the number β is a Parry number, the corresponding beta-integers realize only a finite number of distances between consecutive elements. In this talk, we will determine to which extent beta-integers bear a resemblance to ordinary integers. We will explain for which subclass of Parry numbers they appear in an asymptotic way like ordinary integers. On the contrary, while classical crystals contain arbitrarily long periodic repetitions of a single motif, beta-integers do not. We will determine the maximal possible repetition of the same motif occurring in beta-integers.

Multidimensional generalized automatic sequences and shape-symmetric morphic words

EMILIE CHARLIER (Université de Liège)
(joint work with Tomi Kärki and Michel Rigo)

An infinite word is S-automatic if, for all $n \geq 0$, its $(n + 1)$st letter is the output of a deterministic automaton fed with the representation of n in the considered numeration system S. In this work, we consider an analogous definition in a multidimensional setting and study the relationship with the shape-symmetric infinite words as introduced by Arnaud Maes. Precisely, for $d \geq 2$, we show that a multidimensional infinite word $x : \mathbb{N}^d \to \Sigma$ over a finite alphabet Σ is S-automatic for some abstract numeration system S built on a regular language containing the empty word if and only if x is the image by a coding of a shape-symmetric infinite word.

Rauzy fractal in $\mathbb{R} \times \mathbb{C}$ and points with multiple expansions

FABIEN DURAND (LAMFA, Université de Picardie Jules Verne)

We study the boundary of the 3-dimensional Rauzy fractal $\mathcal{E} \subset \mathbb{R} \times \mathbb{C}$ generated by the polynomial $P(x) = x^4 - x^3 - x^2 - x - 1$. The finite automaton characterizing the boundary of $\mathcal{E}$ is given explicitly. As a consequence we prove that the set $\mathcal{E}$ has 18 neighborhoods where 6 of them intersect the central tile $\mathcal{E}$ in a point. Our construction shows that the boundary is generated by an iterated function system starting with 2 compact sets.

Subword complexity and finite characteristic numbers

ALINA FIRICEL (ICJ, Université Claude Bernard Lyon 1)

Decimal expansions of classical constants such as $\sqrt{2}$, π and $\zeta(3)$ have long been a source of difficult questions. In the case of finite characteristic numbers (Laurent series with coefficients in a finite field), where no carry-over difficulties appear, the situation seems to be simplified. On the other hand, the theory of Drinfeld modules provides analogs of real numbers such as pi, e or ζ values. Hence, it became reasonable to enquire how "complex" the Laurent representation of these "numbers" is.

A remarkable theorem by Christol states that the sequence of coefficients of such series cannot be generated by a finite automaton. But does this sequence contain any repetitions or any interesting patterns? The first part of this talk is focused on this type of questions. Subsequently, some closure properties of classes of formal power series associated with the hierarchy induced by the subword complexity shall be examined.

On Complex Pisot Numeration Systems

MAKI FURUKADO (Yokohama National University) and SHUNJI ITO (Kanazawa University)

Starting from the polynomial $x^3 + x^2 + x - 1$ and its companion matrix M, it is known that we obtain the disjoint compact sets called the Rauzy fractals γ_1, γ_2, γ_3 on the expanding plane P_e of M satisfying the equations: $M\gamma_1 = \gamma_3 - \pi_e \mathbf{e}_2 - \pi_e \mathbf{e}_3$, $M\gamma_2 = \gamma_1 \cup (\gamma_3 - \pi_e \mathbf{e}_2)$, $M\gamma_3 = \gamma_3 \cup \gamma_2$ where $\pi_e : \mathbb{R}^3 \to P_e$ is the projection.

In this talk, starting from the complex Pisot polynomial $f(x) = x^3 - ax^2 - bx \pm 1$, $a, b \in \mathbb{Z}$, that is, the roots λ_i, $i = 1, 2, 3$ of $f(x)$ satisfy $|\lambda_1| = |\lambda_2| > 1 > |\lambda_3|$ and its companion matrix, we discuss how we obtain the "Rauzy fractals" and its set equation.

Noncommutative continued fractions

JOHANNES HUISMAN (Université de Bretagne Occidentale)

A classical continued fraction can be seen as an infinite product in the infinite cartographic group generated by 3 elements, i.e., the group generated by r, s, t, subject to the relations $r^2 = s^2 = t^2 = 1$. It is then natural to define a generalized continued fraction as an infinite product in an infinite cartographic group generated by n elements, where n is some natural integer. In this talk, we study periodic generalized continued fractions.

Digital expansions and multiple tilings

CHARLENE KALLE (Universiteit Utrecht)

We consider a general class of transformations that can be used to obtain digital expansions. These transformations are piecewise linear expanding maps with constant slope β. If β is a Pisot unit and if all the digits are contained in $\mathbb{Q}(\beta)$, then we can associate a multiple tiling of a Euclidean space to the transformation. This does not have to be a tiling.

Möbius number systems

ALEXANDR KAZDA (Charles University in Prague)
(joint work with Petr Kůrka)

A Möbius iterative system is a family of orientation-preserving real Möbius transformations $(M_u : \overline{\mathbb{R}} \to \overline{\mathbb{R}})_{u \in A^*}$ indexed by words of a finite alphabet, such that $F_{uv} = F_u F_v$. The transformations act not only on the extended real line $\overline{\mathbb{R}} = \mathbb{R} \cup \{\infty\}$ but also on the upper half-plane $\mathbb{U} = \{z \in \mathbb{Z} : \Im(z) > 0\}$, where they preserve the hyperbolic metric. The convergence space $\mathbb{X}_F$ consists of all infinite words $u \in A^{\mathbb{N}}$ such that $\lim_{n \to \infty} F_{u_{[0,n)}}(i)$ exists and belongs to $\overline{\mathbb{R}}$ (here i is the imaginary unit). The symbolic map $\Phi : \mathbb{X}_F \to \overline{\mathbb{R}}$ is defined by $\Phi(u) = \lim_{n \to \infty} F_{u_{[0,n)}}(i)$. A Möbius number system is defined by a subshift $\Sigma \subseteq \mathbb{X}_F$, such that $\Phi : \Sigma \to \overline{\mathbb{R}}$ is continuous and surjective. We give several examples of Möbius number systems based on continued fractions.

On negative bases

ANNA CHIARA LAI (LIAFA, Université Paris 7 and Università di Roma "La Sapienza")
(joint work with Christiane Frougny)

We study expansions in non-integer negative base $-\beta$ introduced by Ito and Sadahiro. We show that most of the properties satisfied by the classical β-expansions transfer to the $-\beta$ case.

In particular we characterize the case where the $(-\beta)$-shift is a system of finite type. We prove that, if β is a Pisot number, then the $(-\beta)$-shift is a sofic system. In that case, addition (and more generally normalization on any alphabet) is realizable by a finite transducer.

On sets of integers recognized by countable automata

MARION LE GONIDEC (Université du Sud Toulon Var)
(joint work with Julien Cassaigne)

We introduce 2 families of sets of integers recognized by finite or countable automata and study the structural properties of these 2 families. Some presented results extend usual results on recognizable sets whereas some others underline differences between finite case and countable case.

Nombres de Salem et équirépartition

MICHEL MENDÈS FRANCE (Université Bordeaux 1)
(joint work with Christophe Doche and Jean-Jacques Ruch)

On sait que les puissances successives d'un nombre de Salem sont denses modulo 1, mais ne constituent pas une suite équirépartie modulo 1. Nous nous proposons d'étudier la famille de ses sous-suites équiréparties modulo 1.

Pseudo random sequences generated by dynamical systems

MAKOTO MORI (Nihon University)

Using dynamical system, we can generate pseudo random sequences. We can estimate its discrepancy by the spectra of the Perron-Frobenius operator. In one dimensional cases, the essential spectrum radius of the Perron-Frobenius operator equals $e^{-\xi}$, where ξ is the Lyapunov index. From this fact, we

can characterize the discrepancy of the pseudo random sequences. But for higher dimensional cases, even if we restrict the domain of the Perron-Frobenius operator on suitable spaces, the essential spectrum radius may become larger than $e^{-\xi}$. We will construct transformations for which the essential spectrum radius equals $e^{-\xi}$, and show that they generate low discrepancy sequences.

About the existence/uniqueness of the invariant IBCM measure in Pisot-basis

Eric Olivier (Université de Provence Aix–Marseille 1)

For $1 < \beta < 2$ the (normalized) Infinite Bernoulli Convolition Measure (IBCM) ν_β is the distribution of the random variable $\xi = (\xi_0\xi_1\cdots) \mapsto (\beta-1)\sum_{k=0}^\infty \xi_k/\beta^{k+1} \pmod 1$ for ξ in $\{0,1\}^\mathbb{N}$ weighted by the uniform Bernoulli measure. In the case of the so-called Erdős measure (i.e. ν_β for β the Golden Number) Sidorov and Vershik (1998) proved the existence and the uniqueness of a measure μ_β on the 1-torus, ergodic w.r.t. the endomorphism $x \mapsto \beta x \pmod 1$ and absolutely continuous w.r.t. ν_β; we shall investigate a generalization of this result for some Pisot numbers: we use the strong mixing property of the Parry-Bowen measure (of maximal entropy) on the sofic affine invariant subset of the 2-torus related to a limit Rademacher function and left invariant by the diagonal endomorphism $(x,y) \mapsto (2x, \beta y) \pmod 1$.

Combinatorial interpretation of Rosen continued fractions and generalizations

Benoît Rittaud (Institut Galilée, Université Paris 13)

Rosen continued fractions are continued fractions in which partial quotients belong to $\lambda\mathbb{Z}$, where λ is of the form $2\cos(\pi/k)$ ($k \geq 3$ integer). It was originally studied in a geometrical context. Here, we give a combinatorial interpretation in term of additive continued fraction theory and Stern-Brocot algorithm. This interpretation shows that Rosen continued fractions are, in a quite straightforward sense, the equivalent of the system of numeration in base $(k-1)$. We use this analogy to give some generalizations of Rosen continued fractions to other values of λ which correspond to numeration systems in non-integer bases.

The tilings of Kari and Culik

E. Arthur Robinson, Jr. (The George Washington University)

A new class of aperiodic sets of planar Wang tiles (call them KC tiles) were discovered in 1995 by Kari and Culik. Tilings by KC tiles (KC tilings) seem different than other known aperiodic examples, including those with a self-similar structure, like Penrose tiles and the tiles of Raphael Robinson, and also from tilings that are obtained from the projection method (also like Penrose tilings). KC tilings have Sturmian sequences as rows, and move from row to row by "multiplying" by a rational number. In this talk we give a geometric interpretation of these tilings, and their generalizations, which suggests that KC tilings may not be so different from other known examples as it first appears.

Non-Unimodularity

Bernd Sing (University of Bath)

In this talk we will give an overview explaining how and why (and that) things known for unimodular beta-integers/Pisot-numbers are also working in the non-unimodular case. In the non-unimodular case, one has to consider the numbers involved also as p-adic numbers. However, considering these p-adic cases also helps us to understand the unimodular case better.

The Number of Symbol Comparisons in Quicksort and Quickselect

BRIGITTE VALLÉE (GREYC, CNRS, Université de Caen)

We revisit the famous *QuickSort* algorithm and its derivative, *QuickSelect*. Although the analyses of these algorithms are well-established, we argue, following Sedgewick, that their simplifying assumptions are unsatisfactory, both from the information-theoretic viewpoint and from the perspective of algorithmic engineering. Our complexity model fully takes into account the elementary comparisons between symbols that compose records to be sorted, while our probabilistic models comprise a wide category of information sources that encompass memoryless (i.e., independent-symbol), Markov, as well as many unbounded-correlation sources. Under this perspective, commonly accepted assertions, such as "*the complexity of Quicksort is $O(n \log n)$*", are to be challenged.

Conjugates of Parry numbers near the unit circle

JEAN-LOUIS VERGER-GAUGRY (Insitut Fourier, CNRS, Université Grenoble 1)

Let (β_i) be a sequence of Parry numbers (ex:- beta-numbers). We present a new equidistribution theorem for the conjugates of Parry numbers near the unit circle in Solomyak's fractal set based on a suitable notion of convergence of (β_i), and on the theory of Erdős-Turán, improved by Amoroso and Mignotte. This theorem is addressed to the union of the Galois conjugates and the beta-conjugates of all the β_is.

This theorem asks questions about the factorization of the Parry polynomial (ex: -characteristic polynomial) of a Parry number β, the multiplicities of its beta-conjugates, the geometry of its beta-conjugates within the Galois closure of the number field generated by β. Some partial results to these questions are given.

The structure of groups supporting a numeration system

CHRISTIAAN VAN DE WOESTIJNE (Technische Universität Graz)

Let G be an abelian group, f an endomorphism of G and D a subset of G such that $\#D = [G : f(G)]$. I call (G, f, D) a number system if every element of G has a finite expansion of the form

$$g = \sum_{i=0}^{\ell} f^i(d_i) \qquad (d_i \in D).$$

We may ask which groups G support such a number system. I will give some examples, and prove some finiteness properties that G must have. Next, I will propose the conjecture that G must be a split group, and comment on the possibility to prove this claim.

Part of this work is joint with Ryotaro Okazaki.