DIOPHANTINE PROBLEMS: DETERMINISM, RANDOMNESS AND APPLICATIONS

Dijana Kreso, Joël Rivat & Robert F. Tichy (eds.)

Panoramas et Synthèses

Numéro 62 2024

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Comité de rédaction

Samuel BOISSIÈRE
Fabienne CASTELL
Indira CHATTERJI
Élise GOUJARD
Anne-Sophie de SUZZONI
Diego IZQUIERDO
Claire LACOUR
Quentin MÉRIGOT
Sergio SIMONELLA
Todor TSANKOV
Anne MOREAU (dir.)

Diffusion

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 9
France
`christian.smf@cirm-math.fr`

AMS
P.O. Box 6248
Providence RI 02940
USA
`www.ams.org`

Tarifs

Vente au numéro : 54 € ($ 81)

Des conditions spéciales sont accordées aux membres de la SMF.

Secrétariat

Panoramas et Synthèses
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France
Tél : (33) 01 44 27 67 99 • Fax : (33) 01 40 46 90 96
`panoramas@smf.emath.fr` • `http://smf.emath.fr/`

© *Société Mathématique de France 2024*

Tous droits réservés (article L 122–4 du Code de la propriété intellectuelle). Toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'éditeur est illicite. Cette représentation ou reproduction par quelque procédé que ce soit constituerait une contrefaçon sanctionnée par les articles L 335–2 et suivants du CPI.

ISSN 1272-3835

ISBN 978-2-37905-205-7

Directeur de la publication : Isabelle Gallagher

PANORAMAS ET SYNTHÈSES 62

DIOPHANTINE PROBLEMS: DETERMINISM, RANDOMNESS AND APPLICATIONS

Dijana Kreso, Joël Rivat & Robert F. Tichy (eds.)

Société mathématique de France

Dijana Kreso
Graz University of Technology
Institute of Analysis and Number Theory
Kopernikusgasse 24/II
8010 Graz, Austria
E-mail : kreso@math.tugraz.at

Joël Rivat
Institut de Mathématiques de Marseille CNRS UMR 7373
Institut Universitaire de France
Université d'Aix-Marseille
163 avenue de Luminy, 13288 Marseille, Cedex 9, France
E-mail : joel.rivat@univ-amu.fr

Robert F. Tichy
Graz University of Technology
Institute of Analysis and Number Theory
Steyrergasse 30/II
8010 Graz, Austria
E-mail : tichy@tugraz.at

***Classification mathématique par sujets.* (2020) —** 42A55, 11K38, 60G09, 11K31, 11K60, 60F05, 60F15, 11K06, 11D61, 11C08, 39B12, 11D45, 11B37, 43A07, 37F10, 37A44, 11B85, 37B10, 11L20, 11A63, 28A80, 11K45, 65D30, 97M30, 91G20, 91-10.

***Keywords and phrases.* —** Discrepancy functions, trigonometric sums, limit theorems, lacunary sequences, metric number theory, normal numbers, diophantine equations, subsequence principle, exchangeable sequences, Pillai's problems, Ritt's decomposition theory, polynomial equations, polynomial power sums, semigroups, amenability, measure of maximal entropy, functional equations, arithmetic dynamics, ergodic theory, sums over primes, automatic sequences, arithmetic dynamical systems, self-affine sets, tilings, digit systems, quasi-Monte Carlo method, pseudorandom sequences, low-discrepancy sequences, randomized quasi-Monte Carlo method, financial mathematics, Hardy-Krause variation, option pricing.

***Mots-clés et phrases.* —** Fonctions de discrépance, sommes trigonométriques, théorèmes de limite, séquences lacunaires, théorie métrique des nombres, nombres normaux, équations diophantiennes, principe des sous-suites, séquences échangeables, problèmes de Pillai, théorie de décomposition de Ritt, équations polynomiales, sommes de puissances polynomiales, semi-groupes, aménabilité, mesure d'entropie maximale, équations fonctionnelles, dynamique arithmétique, théorie ergodique, sommes sur les nombres premiers, séquences automatiques, systèmes dynamiques arithmétiques, ensemble auto-affine, pavage, système de numération, méthode quasi-Monte Carlo, séquences pseudo-aléatoires, séquences à faible discrépance, méthode quasi-Monte Carlo aléatoire, mathématiques financières, variation Hardy-Krause, évaluation des options.

DIOPHANTINE PROBLEMS: DETERMINISM, RANDOMNESS AND APPLICATIONS

Dijana Kreso, Joël Rivat & Robert F. Tichy (eds.)

***Abstract.* —** This volume comprises a collection of eight papers in number theory, which are devoted to research topics explored during *Jean Morlet* Chair Program 2020/2021, titled *Diophantine problems: Determinism, Randomness, and Applications.* The volume includes survey articles as well as some original papers in diophantine number theory and applications. The most extensive contribution deals with equidistribution and discrepancy theory from a probalistic point of view. In this article, Aistleitner, Berkes, and Tichy investigate lacunary trigonometric sums and lacunary sums of dilated functions. Using a combination of tools (probabilistic method, methods from Diophantine analysis, etc.) they widely generalize some classical results of Salem, Zygmund, Erdős, Gál and others in Fourier analysis and metric number theory. Two papers, one by Kreso and Tichy and the other by Heintze, focus on polynomial variants of Pillai's Diophantine equations, which have been extensively studied since the 1930s. Both papers present new results and utilize classical findings on vanishing sums in function fields to establish analogues of Pillai's asymptotic results in the context of polynomials and polynomial power sums. The paper of Kreso and Tichy further employs Ritt's theory of polynomial decomposition, which finds broad applications in number theory, complex analysis, etc. Pakovich's contribution revolves around the theory of Ritt and its generalizations, focusing on certain problems and conjectures concerning semigroups of rational functions under the operation of functional composition. The paper by Drmota, Lemańczyk, Müllner and Rivat provides a survey of recent advancements on the Sarnak conjecture within the context of product spaces, prime number theorems, polynomial subsequences, and morphic sequences. It also introduces novel results concerning products of automatic sequences. Rossi, Steiner, and Thuswaldner's paper opens up new directions in the study of arithmetic dynamical systems and their interaction with the analysis of fractal structures. The survey paper by Ökten offers an introduction into quasi-random numbers, pseudorandomness and number-theoretic algorithms for generating pseudorandom sequences, as well as their applications in numerical integration, such as the quasi-Monte Carlo method in mathematical finance. This article has been successfully used by students in summer schools as a first step to get familiar with quasi-Monte Carlo methods, their number theoretic origin and some applications. Finally, a related paper by Nachbagauer and Thonhauser examines an option pricing problem in mathematical finance from the perspective of quasi-Monte Carlo integration.

The third editor would like to express his deep gratitude to the Aix-Marseille University, to CIRM and to SMF for their support and hospitality.

Résumé. **(Problèmes diophantiens: déterminisme, aléa et applications) —** Ce volume comprend une collection de huit articles en théorie des nombres, consacrés à des sujets de recherche explorés lors du programme de la Chaire *Jean Morlet* 2020/2021, intitulé *Problèmes diophantiens : déterminisme, aléatoire et applications*. Le volume comprend des articles de synthèse ainsi que des articles originaux en théorie des nombres diophantiens et applications. La contribution la plus approfondie porte sur l'équidistribution et la théorie de la discrépance d'un point de vue probabiliste. Dans cet article, Aistleitner, Berkes et Tichy étudient les sommes trigonométriques lacunaires et les sommes lacunaires de fonctions dilatées. En utilisant une combinaison d'outils (méthode probabiliste, méthodes de géométrie diophantienne, etc.), ils généralisent largement certains résultats classiques de Salem, Zygmund, Erdős, Gal et d'autres en analyse de Fourier et en théorie des nombres métriques. Deux articles, l'un de Kreso et Tichy et l'autre de Heintze, se concentrent sur des variantes polynomiales des équations diophantiennes de Pillai, qui ont été largement étudiées depuis les années 1930. Les deux articles présentent de nouveaux résultats et utilisent des résultats classiques sur les sommes nulles dans les corps de fonctions pour établir des analogues des résultats asymptotiques de Pillai dans le contexte des polynômes et des sommes de puissances polynomiales. L'article de Kreso et Tichy utilise en outre la théorie de décomposition polynomiale de Ritt, qui trouve de larges applications en théorie des nombres, en analyse complexe, etc. La contribution de Pakovich porte sur la théorie de Ritt et ses généralisations, en se concentrant sur certains problèmes et conjectures concernant les semi-groupes de fonctions rationnelles sous l'opération de composition fonctionnelle. L'article de Drmota, Lemańczyk, Müllner et Rivat propose un survol des avancées récentes concernant la conjecture de Sarnak dans le contexte des espaces produits, des théorèmes sur les nombres premiers, des sous-suites polynomiales et des séquences morphiques. Il présente également de nouveaux résultats concernant les produits de séquences automatiques. L'article de Rossi, Steiner et Thuswaldner ouvre de nouvelles perspectives dans l'étude des systèmes dynamiques arithmétiques et de leur interaction avec l'analyse des structures fractales. L'article de synthèse de Ökten offre une introduction aux nombres quasi-aléatoires, à la notion de pseudo-aléa et aux algorithmes basés sur la théorie des nombres pour générer des suites pseudo-aléatoires, ainsi qu'à leurs applications dans l'intégration numérique, telle que la méthode quasi-Monte Carlo en mathématiques financières. Cet article a été utilisé avec succès par les étudiants lors des écoles d'été comme une première étape pour se familiariser avec les méthodes quasi-Monte Carlo, leur origine en théorie des nombres et certaines applications. Enfin, un article connexe de Nachbagauer et Thonhauser examine un problème d'évaluation des options en mathématiques financières du point de vue de l'intégration quasi-Monte Carlo.

Le troisième éditeur souhaite exprimer sa profonde gratitude à l'Université Aix-Marseille, au CIRM et à la SMF pour leur soutien et leur hospitalité.

TABLE DES MATIÈRES

Christoph Aistleitner & István Berkes & Robert Tichy — *Lacunary sequences in analysis, probability and number theory* 1

1. Introduction 2
2. Uniform distribution and discrepancy 4
3. Arithmetic effects: Diophantine equations and sums of common divisors 7
4. The central limit theorem for lacunary sequences 12
5. The law of the iterated logarithm for lacunary sequences 16
6. Normality and pseudorandomness 20
7. Random sequences 24
8. The subsequence principle 28
9. New results: Exact criteria for the central limit theorem for subsequences 36

References 49

Dijana Kreso & Robert F. Tichy — *On variants of Pillai's problems with polynomials* 61

1. Introduction 62
2. Proofs of Theorem 1 and Theorem 3 65
3. Proof of Theorem 4 and some open problems 77

References 81

Sebastian Heintze — *Asymptotics for Pillai's problem with polynomials* 83

1. Introduction 83
2. Notation and results 84
3. Preliminaries 85
4. Proof 86

References 88

Fedor Pakovich — *Semigroups of rational functions: some problems and conjectures* 89

1. Introduction 89
2. Semigroups $C(P)$ 91
3. Semigroups $C_\infty(P)$ and $E(P)$ 94

4. Reversible semigroups 96
5. Amenable semigroups 100
References 101

M. Drmota & M. Lemańczyk & C. Müllner & J. Rivat — *Some Recent Developments on the Sarnak Conjecture* 105

1. Introduction 105
2. Product Dynamical Systems 109
3. Prime Number Theorems 111
4. Polynomial Subsequences 116
5. Morphic Sequences 118
6. Appendix – Proof of Theorem 2.3 120
References 125

Lucía Rossi & Wolfgang Steiner & Jörg M. Thuswaldner — *Rational self-affine tiles associated to standard and nonstandard digit systems* 129

1. Introduction 130
2. Setting and definitions 132
3. Results on rational self-affine tiles 139
4. Characters and multiple tiling 147
References 159

Giray Ökten — *Number sequences for simulation* 161

1. Introduction 161
2. Pseudorandom sequences 163
3. Low-discrepancy sequences and quasi-Monte Carlo methods 168
4. Randomized quasi-Monte Carlo methods 179
5. Conclusion 188
References 188

Florian Nachbagauer & Stefan Thonhauser — *Regularity of a* best-of option*'s payoff* 191

1. Introduction 191
2. Hardy and Krause variation 194
3. Financial market model 202
4. Finite variation of the maximum 207
5. Numerical example 213
6. Conclusion and alternative 215
References 215

RÉSUMÉS DES ARTICLES

Séquences de lacunes en analyse, probabilités et théorie des nombres
Christoph Aistleitner & István Berkes & Robert Tichy 1

Dans cette étude, nous présentons la théorie des sommes trigonométriques lacunaires et des sommes lacunaires de fonctions dilatées, depuis les origines du sujet jusqu'aux développements récents. Nous décrivons les liens avec des sujets mathématiques tels que l'équidistribution et la discrépance, la théorie métrique des nombres, la normalité, le caractère pseudo-aléatoire, les équations diophantiennes et le principe de sous-séquence. Dans la dernière section de l'article, nous prouvons de nouveaux résultats qui fournissent des conditions nécessaires et suffisantes pour le théorème de la limite centrale pour les sous-séquences, dans l'esprit du théorème de résonance de Nikishin pour les systèmes de convergence. Plus précisément, nous caractérisons les suites de variables aléatoires qui permettent d'extraire une sous-suite satisfaisant une forme forte du théorème de la limite centrale.

Sur les variantes des problèmes de Pillai avec des polynômes
Dijana Kreso & Robert F. Tichy 61

Nous allons résoudre plusieurs variantes polynomiales de certains problèmes diophantiens de Pillai bien connus. En particulier, nous nous concentrons sur l'équation

$$a_1 p(x)^{n_1} + b_1 q(x)^{m_1} = a_2 p(x)^{n_2} + b_2 q(x)^{m_2} = f(x)$$

dans les polynômes complexes f, p, q avec f non nul et p et q non constants. Les nombres complexes a_i, b_i sont non nuls et les n_i, m_i désignent des entiers positifs. Le cas particulier $a_1 = a_2 = 1$ et $b_1 = b_2 = -1$ correspond à une équation diophantienne de Pillai bien étudiée $a^{n_1} - b^{m_1} = a^{n_2} - b^{m_2}$ dans des entiers positifs n_i, m_i, a, b avec $a > 1$ et $b > 1$.

Nous montrerons de plus que pour des polynômes complexes non constants premiers entre eux p et q, le nombre de solutions $(n, m) \in^2$ de $0 \leq \deg\left(p(x)^n - q(x)^m\right) \leq d$ est asymptotiquement égal à $d^2/(\deg p \deg q)$ lorsque $d \to \infty$, et nous considérerons également une généralisation de ce problème où les puissances des polynômes sont remplacées par les sommes des puissances des polynômes.

Asymptotique pour les problèmes de Pillai avec les polynômes

Sebastian Heintze 83

Soit $a_1(x)p_1(x)^n + \cdots + a_k(x)p_k(x)^n$ ainsi que $b_1(x)q_1(x)^m + \cdots + b_{\ell(x)}q_\ell(x)^m$ deux sommes de puissances polynomiales où les polynômes complexes $p_i(x)$ et $q_j(x)$ sont tous non constants. Dans cet article, nous donnerons une formule asymptotique pour le nombre de couples $(n, m) \in \mathbb{N}^2$ tels que le degré de la somme de ces deux sommes de puissances est compris entre 0 et d lorsque d tend vers l'infini.

Semigroupes de fonctions rationnelles : certains problèmes et conjectures

Fedor Pakovich 89

Nous formulons des problèmes et des conjectures concernant les semi-groupes de fonctions rationnelles sous composition. Les problèmes considérés surgissent dans différents contextes, mais la plupart d'entre eux sont liés par une certaine relation avec le concept d'aménabilité.

Quelques développements récents sur la conjecture de Sarnak

M. Drmota & M. Lemańczyk & C. Müllner & J. Rivat 105

Dans cet article, nous examinons certains développements récents de la conjecture de Sarnak dans le contexte des espaces de produits, des théorèmes des nombres premiers, des sous-suites polynomiales et des suites morphiques. Nous présentons également un nouveau résultat sur les produits de suites automatiques.

Tuiles rationnelles auto-affines associées à des systèmes de chiffres standards et non standards

Lucía Rossi & Wolfgang Steiner & Jörg M. Thuswaldner 129

Nous considérons des systèmes de chiffres $(\mathcal{A}, \mathcal{D})$, où $A \in \mathbb{Q}^{n\times n}$ est une matrice d'expansion et l'ensemble de chiffres $\mathcal{D}$ est un sous-ensemble approprié de $\mathbb{Q}^n$. À un tel système, nous associons un ensemble auto-affine $\mathcal{F} = \mathcal{F}(\mathcal{A}, \mathcal{D})$ qui vit dans un certain espace de représentation $\mathbb{K}_\mathcal{A}$. Si A est une matrice entière, alors $\mathbb{K}_\mathcal{A} = \mathbb{R}^n$, tandis que dans le cas rationnel général $\mathbb{K}_\mathcal{A}$ contient un facteur solénoïdal supplémentaire. Nous donnons un critère pour que $\mathcal{F}$ ait une mesure de Haar positive, c'est-à-dire pour être une *mosaïque rationnelle auto-affine*. Nous étudions les propriétés topologiques de $\mathcal{F}$ et prouvons certains théorèmes de mosaïque. Notre cadre est très général dans le sens où nous permettons à $(\mathcal{A}, \mathcal{D})$ d'être un *système de chiffres non standard*. Un système de chiffres standard $(\mathcal{A}, \mathcal{D})$ est un système dans lequel nous exigeons que $\mathcal{D}$ soit un système complet de représentants de classes de résidus par rapport à un certain anneau de classes de résidus choisi naturellement. Nos outils comprennent la forme normale de Frobenius et la théorie des caractères des groupes localement compacts abéliens.

Séquences de nombres pour la simulation
GIRAY ÖKTEN 161

Nous présentons un survol introductif de certains concepts clés des méthodes de Monte Carlo, de quasi-Monte Carlo et de quasi-Monte Carlo randomisées. Les sujets comprennent l'aléatoire, les suites pseudo-aléatoires et à faible discrépance, les suites à faible discrépance randomisées et les applications à l'intégration numérique. Notre survol n'est pas exhaustif et le traitement des sujets est aussi peu technique que possible, en mettant l'accent sur les idées et la motivation derrière eux.

Régularité du gain d'une best-of option
FLORIAN NACHBAGAUER & STEFAN THONHAUSER 191

Cette contribution considère un problème de tarification des options du point de vue de l'intégration quasi-Monte Carlo. En particulier, nous sommes en mesure de montrer qu'une certaine fonction de paiement non lisse conduit à un intégrande à variation bornée, même dans le cas de Hardy et Krause. La clé de ce résultat est l'application d'une transformation spéciale au cube unité et une utilisation astucieuse des résultats d'Art B. Owen (de son article *Multidimensional variation for quasi-Monte Carlo* publié en 2005).

ABSTRACTS

Lacunary sequences in analysis, probability and number theory
CHRISTOPH AISTLEITNER & ISTVÁN BERKES & ROBERT TICHY 1

In this paper we present the theory of lacunary trigonometric sums and lacunary sums of dilated functions, from the origins of the subject up to recent developments. We describe the connections with mathematical topics such as equidistribution and discrepancy, metric number theory, normality, pseudorandomness, Diophantine equations, and the subsequence principle. In the final section of the paper we prove new results which provide necessary and sufficient conditions for the central limit theorem for subsequences, in the spirit of Nikishin's resonance theorem for convergence systems. More precisely, we characterize those sequences of random variables which allow to extract a subsequence satisfying a strong form of the central limit theorem.

On variants of Pillai's problems with polynomials
DIJANA KRESO & ROBERT F. TICHY 61

We will solve several polynomial variants of some well-known Pillai's Diophantine problems. In particular, in our focus is the equation

$$a_1 p(x)^{n_1} + b_1 q(x)^{m_1} = a_2 p(x)^{n_2} + b_2 q(x)^{m_2} = f(x)$$

in complex polynomials f, p, q with f nonzero and p and q nonconstant. The complex numbers a_i, b_i are nonzero and the n_i, m_i denote positive integers. The special case $a_1 = a_2 = 1$ and $b_1 = b_2 = -1$ corresponds to a well-studied Pillai's Diophantine equation $a^{n_1} - b^{m_1} = a^{n_2} - b^{m_2}$ in positive integers n_i, m_i, a, b with $a > 1$ and $b > 1$.

We will further show that for nonconstant coprime complex polynomials p and q, the number of solutions $(n, m) \in^2$ of $0 \leq \deg\left(p(x)^n - q(x)^m\right) \leq d$ is asymptotically equal to $d^2/(\deg p \deg q)$ as $d \to \infty$, as well as consider a generalization of this problem where the powers of polynomials are replaced by the sums of powers of polynomials.

Asymptotics for Pillai's problem with polynomials
SEBASTIAN HEINTZE 83

Let $a_1(x)p_1(x)^n + \cdots + a_k(x)p_k(x)^n$ as well as $b_1(x)q_1(x)^m + \cdots + b_l(x)q_l(x)^m$ be two polynomial power sums where the complex polynomials $p_i(x)$ and $q_j(x)$ are all non-constant. Then in the present paper we will give an asymptotic for the number of pairs $(n, m) \in \mathbb{N}^2$ such that the degree of the sum of these two power sums is between 0 and d when d goes to infinity.

Semigroups of rational functions: some problems and conjectures
FEDOR PAKOVICH 89

We formulate some problems and conjectures about semigroups of rational functions under composition. The considered problems arise in different contexts, but most of them are united by a certain relationship to the concept of amenability.

Some Recent Developments on the Sarnak Conjecture
M. DRMOTA & M. LEMAŃCZYK & C. MÜLLNER & J. RIVAT 105

In this article we survey some recent developments on the Sarnak conjecture in the context of product spaces, of prime number theorems, of polynomial subsequences, and of morphic sequences. We also present a new result on products of automatic sequences.

Rational self-affine tiles associated to standard and nonstandard digit systems
LUCÍA ROSSI & WOLFGANG STEINER & JÖRG M. THUSWALDNER 129

We consider digit systems $(A, \mathcal{D})$, where $A \in \mathbb{Q}^{n\times n}$ is an expanding matrix and the *digit set* $\mathcal{D}$ is a suitable subset of $\mathbb{Q}^n$. To such a system, we associate a self-affine set $\mathcal{F} = \mathcal{F}(A, \mathcal{D})$ that lives in a certain representation space $\mathbb{K}$. If A is an integer matrix, then $\mathbb{K} = \mathbb{R}^n$, while in the general rational case $\mathbb{K}$ contains an additional solenoidal factor. We give a criterion for $\mathcal{F}$ to have positive Haar measure, i.e., for being a *rational self-affine tile*. We study topological properties of $\mathcal{F}$ and prove some tiling theorems. Our setting is very general in the sense that we allow $(A, \mathcal{D})$ to be a *nonstandard* digit system. A *standard* digit system $(A, \mathcal{D})$ is one in which we require $\mathcal{D}$ to be a complete system of residue class representatives w.r.t. a certain naturally chosen residue class ring. Our tools comprise the Frobenius normal form and character theory of locally compact abelian groups.

Number sequences for simulation
GIRAY ÖKTEN 161

We present an introductory survey of some key concepts from Monte Carlo, quasi-Monte Carlo, and randomized quasi-Monte Carlo methods. The topics include randomness, pseudorandom and low-discrepancy sequences, randomized low-discrepancy sequences, and applications to numerical integration. Our survey is by no means exhaustive, and the treatment of topics is as little technical as possible, emphasizing the ideas and motivation behind them.

Regularity of a best-of option*'s payoff*
FLORIAN NACHBAGAUER & STEFAN THONHAUSER 191

This contribution considers a problem of option pricing from the perspective of quasi-Monte Carlo integration. In particular, we are able to show that a certain non-smooth payoff function leads to an integrand of bounded variation, even in the sense of Hardy and Krause. The key to this result is the application of a special transformation to the unit cube and a neat use of results from Owen [*Multidimensional variation for quasi-Monte Carlo*, 2005].