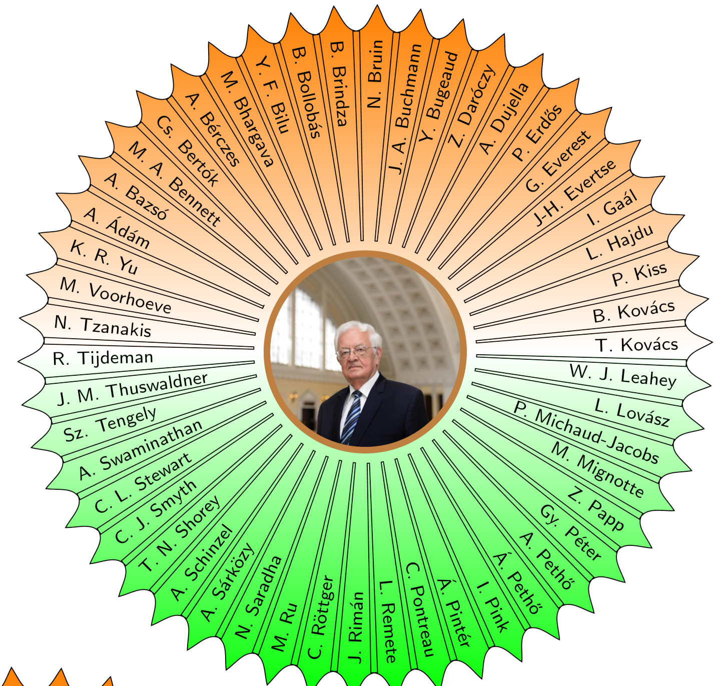
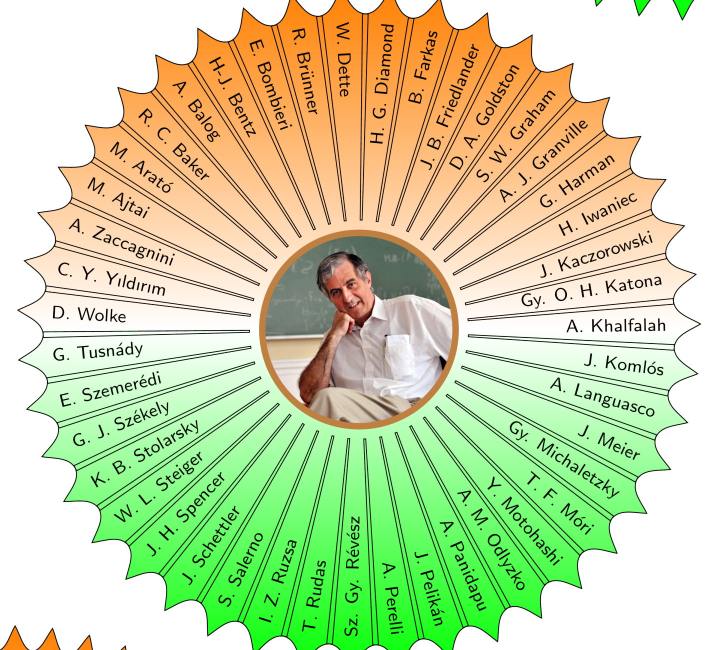
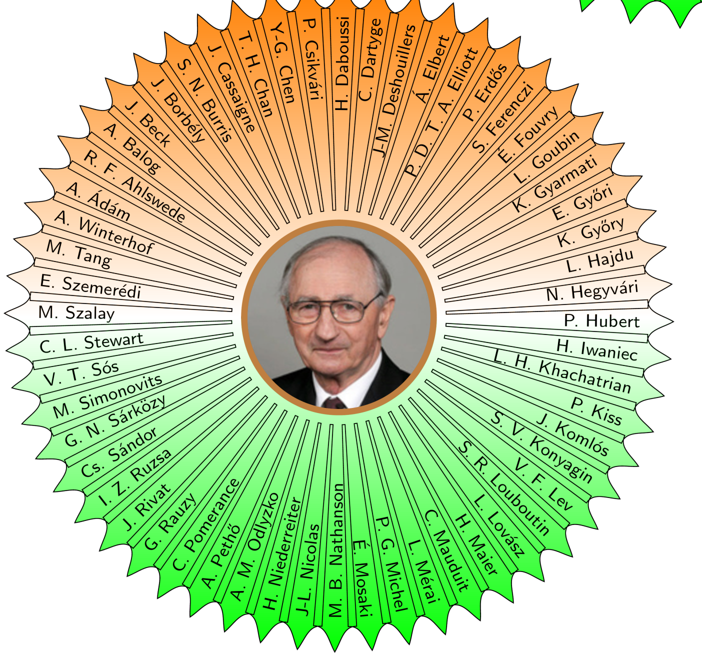
Number Theory Conference
4-8 July 2022
In honour of Professors
Kálmán Győry, János Pintz
and András Sárközy







Sponsors

National Research, Development and Innovation Office (NKFIH)	NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION OFFICE
University of Debrecen	15 38
Student Council of the University of Debrecen	15 38
Foundation Compositio Mathematica	
Number Theory Foundation	Number Theory NTF ζ(ρ) = 0 Foundation

List of plenary speakers

- Mike Bennett, University of British Columbia (Canada)
- Yann Bugeaud, University of Strasbourg (France)
- Cecile Dartyge, Université de Lorraine (France)
- Jan-Hendrik Evertse, Leiden University (The Netherlands)
- Daniel Goldston, San José State University (USA)
- Henryk Iwaniec, Rutgers University (USA)
- Jerzy Kaczorowski, Poznan University (Poland)
- Attila Pethő, University of Debrecen (Hungary)
- Ákos Pintér, University of Debrecen (Hungary)
- Carl Pomerance, Dartmouth College (USA)
- Szilárd Révész, Alfréd Rényi Institute of Mathematics (Hungary)
- Joël Rivat, Aix-Marseille University (France)
- Igor Shparlinski, University of New South Wales (Australia)
- Cameron L. Stewart, University of Waterloo (Canada)
- Robert Tichy, Graz University of Technology (Austria)
- Robert Tijdeman, Leiden University (The Netherlands)
- Arne Winterhof, Johann Radon Institute (Austria)
- Cem Yalçın Yıldırım, Bogaziçi University (Turkey)

Organization

Scientific Committee

- Attila Bérczes
- István Gaál
- Katalin Gyarmati
- Lajos Hajdu
- Ákos Pintér

Secretaries

- András Bazsó
- Nóra Varga

Organizing Committee

- Tímea Arnóczki
- Csanád Bertók
- Eszter Gyimesi
- Orsolya Herendi
- Adrián Nagy
- Gábor Nyul
- Ágoston Papp
- István Pink
- András Pongrácz
- Gabriella Rácz
- László Remete
- Péter Sebestyén
- Szabolcs Tengely

List of abstracts

Nikola Adžaga

nikola.adzaga@grad.unizg.hr, (University of Zagreb (Croatia))
Joint work with: Vishal Arul, Lea Beneish, Mingjie Chen, Shiva Chidambaram, Timo Keller, Oana Padurariu and Boya Wen

Rational points on quotients of modular curves by Atkin-Lehner involutions

In this talk we present how to provably determine all rational points on curves $X_0^+(p)$ of genus g up to 6 (for prime p). Denote by r the rank of the Jacobian of the curve over the rationals. As these curves usually satisfy $r = g$, we use Quadratic Chabauty. We also determine all rational points on hyperelliptic curves $X_0^*(N)$ where we used other methods as well: quotients, Mordell-Weil Sieve and variations of Chabauty's method. Since the points on these curves parametrize elliptic curves with additional structure, we also classify rational points on all $X_0^+(p)$ and on hyperelliptic $X_0^*(N)$ for N squarefree.

Shigeki Akiyama

akiyama@math.tsukuba.ac.jp, (University of Tsukuba (Japan))
Joint work with: Teturo Kamae and Hajime Kaneko

Multiplicative Lagrange spectrum and symbolic dynamics

For a fixed irrational $\alpha \in \mathbb{R}$, approximation of 0 by the sequence $n\alpha \mod 1$ for $n = 1, 2, \dots$ is a classical subject in number theory. Topological structure of the set

$$\left\{ \limsup_n \frac{1}{n\|n\alpha\|} \;\middle|\; \alpha \in \mathbb{R} \setminus \mathbb{Q} \right\}$$

is very curious and known as Markoff-Lagrange spectra. We study a multiplicative analogy of this spectra. Let us fix a linear recurrence of exponential growth. We consider the set

$$\left\{ \limsup_n \|\Re(x_n)\| \right\}$$

where x_n runs over all complex sequences satisfying this recurrence. Under some condition, we derive results analogous to Markoff-Lagrange spectra. As a special case, our results give information on the topology of the set

$$\left\{ \limsup_{n} \|\Re(\xi\alpha^n)\| \;\middle|\; \xi \in \mathbb{C} \right\}$$

when α is a complex Pisot number. The basic idea is to construct an intertwing formula to lift the problem to a symbolic dynamical setting.

Vishnupriya Anupindi

vishnupriya.anupindi@ricam.oeaw.ac.at, (Johann Radon Institute for Computational and Applied Mathematics (Austria))
Joint work with: László Mérai

Pseudorandom sequences from hyperelliptic curves of genus 2

Pseudorandom sequences, i.e. sequences which are generated with deterministic algorithms but look random, have many applications, for example in cryptography, in wireless communication or in numerical methods. In this work, we are interested in studying the properties of pseudorandomness of sequences derived from hyperelliptic curves of genus 2.

In particular, we will look at two different ways of generating sequences, that is, the linear congruential generator and the Frobenius endomorphism generator. We show that these sequences possess good pseudorandom properties in terms of linear complexity. In this talk, we will introduce the N-th linear complexity of a sequence, the group structure on hyperelliptic curves of genus 2 and look at the main results.

References

[1] Anupindi, V. and Mérai, L. *Linear complexity of some sequences derived from hyperelliptic curves of genus 2*, Cryptogr. Commun. **14** (2022), 117–134.

[2] Anupindi, V. *Linear complexity of sequences on Koblitz curves of genus 2*, Uniform Distribution Theory, Bd. to appear.

Tímea Arnóczki

arnoczki.timea@science.unideb.hu, (University of Debrecen (Hungary))
Joint work with: Gábor Nyul

Jacobi–Whitney numbers

W. N. Everitt, L. L. Littlejohn and R. Wellman introduced a new class of Stirling-like numbers, the Legendre–Stirling numbers of the first and second kind. A few years later, these numbers were generalized to the Jacobi–Stirling numbers by the same authors together with K. H. Kwon and G. J. Yoon. All these definitions are based on a deep analytical problem.

In the talk, we give combinatorial interpretations of Jacobi–Stirling numbers of the first and second kind in a unified spirit, that also fit with the combinatorial definition of ordinary Stirling numbers. Moreover, we define a new type of combinatorial numbers, the Jacobi–Whitney numbers of the first and second kind in a combinatorial way, which give back Jacobi–Stirling numbers as a special case. We present several properties of Jacobi–Whitney numbers, for example recurrence relations, polynomial identity, orthogonality, unimodality.

Finally, we mention the difficulties of defining Jacobi–Whitney–Lah numbers.

Gergő Batta

battagergo424@gmail.com, (University of Debrecen (Hungary))

On 3rd Power Rational Diophantine Triples and Quadruples

Let $k \geq 2$ be a fixed integer. A set of non-zero rationals $\{a_1, a_2, ..., a_n\}$ is said to be a kth power rational Diophantine n-tuple if for every $1 \leq i < j \leq n$ there exist rationals r_{ij} such that $a_i a_j + 1 = r_{ij}^k$. It is fairly simple to find examples for small values of k and n, the sets $\{1, 3, 8, 120\}$, $\{2, 171, 25326\}$, $\{1352, 8539880, 9768730\}$ all being examples. The natural problem arising from the definition is the following: how large, say for a given k, the tuple can be?

The case of $k = 2$ is classical, its history dating back to Diophantus himself and follows the work of Fermat and Euler, eventually becoming a more and more actively researched area in relation with Diophantine equations and Diophantine geometry. As of today, the "best" published results establish that there exists infinitely many sextuples and, provided that we are restricted to rational integers, that no quintuple exists. Surprisingly, or not, the higher values of k did not receive much attention except for the case of rational integers: here, Bugeaud and Dujella set explicit bounds on n.

In present talk, we prove the existence of infinite families of 3rd power rational

Diophantine triples and quadruples. We first introduce the concept of elliptic curves induced by 3rd power rational Diophantine pairs, then use 3-descent to find points on this curve that extend the pair to a triple. For special families of pairs, we go one step further and find pairs of points that both serve as extension to a triple and together to a quadruple. The approach is an analogue of the $k = 2$ case, where elliptic curves induced by triples and 2-descent are leveraged.

The talk serves as a follow up to another contributed talk entitled ”On Higher Power Rational Diophantine Tuples”.

Francesco Battistoni
francesco.battistoni@unimi.it, (University of Milan (Italy))
Joint work with: Giuseppe Molteni

Optimization of polynomials for the study of small regulators

Number fields with small regulators can be detected thanks to a method developed by Astudillo, Diaz y Diaz and Friedman. The efficiency of the procedure can be strengthened by improving the upper bound of a logarithmic term in a specific inequality, and this corresponds to finding the true maximum of a certain polynomial over an hypercube.

We show how we found and proved the true maximum in the case of totally real fields (thus solving a conjecture by Pohst [2]) and how we consistently lowered the upper bound in the case of fields with one complex embedding: as a consequence, we are able to detect the field of degree 8 and signature (6,1) with minimum regulator (as conjectured in [1]).

References

[1] F. Battistoni. A conjectural improvement for inequalities related to regulators of number fields. *Bollettino dell’Unione Matematica Italiana*, 14: 609–627, 2021.

[2] F. Battistoni and G. Molteni. Generalization of a Pohst’s inequality. *J. Number Theory*, 228: 73–86, 2021.

Attila Bérczes

berczesa@science.unideb.hu, (University of Debrecen (Hungary))

Effective results for Diophantine equations over finitely generated domains

Let $A := \mathbb{Z}[z_1, \dots, z_r] \supset \mathbb{Z}$ be a finitely generated integral domain over $\mathbb{Z}$ and denote by K the quotient field of A. Finiteness results for several kinds of Diophantine equations over A date back to the middle of the last century. S. Lang generalized several earlier results on Diophantine equations over the integers to results over A, including results concerning unit equations, Thue-equations and integral points on curves. However, all his results were ineffective. The first effective results for Diophantine equations over finitely generated domains were published in the 1980's, when Győry developed his new effective specialization method. This enabled him to prove effective results over finitely generated domains of a special type. In 2011 Evertse and Győry refined the method of Győry such that they were able to prove effective results for unit equations $ax + by = 1$ in $x, y \in A^*$ over arbitrary finitely generated domains A of characteristic 0. Using this new general method Bérczes, Evertse and Győry obtained effective results for Thue equations, hyper- and superelliptic equations and for the Schinzel-Tijdeman equation over arbitrary finitely generated domains. Later Bérczes proved effective results for equations $F(x, y) = 0$ in $x, y \in A^*$ for arbitrary finitely generated domains A, and for $F(x, y) = 0$ in $x, y \in \overline{\Gamma}$, where $F(X, Y)$ is a bivariate polynomial over A and $\overline{\Gamma}$ is the division group of a finitely generated subgroup Γ of K^*. Koymans generalized the effective result of Tijdeman on the Catalan equation for finitely geberated domains, while Evertse and Győry proved effective results for decomposable form equations in this generality.

In my talk I will present a short survey of the method of Evertse and Győry and of the above mentioned results obtained by this method.

Michael A. Bennett

bennett@math.ubc.ca, (University of British Columbia (Canada))
Joint work with: Samir Siksek and Philippe Michaud-Jacobs

Differences between squares and perfect powers

I survey recent work on the classical Lebesgue-Nagell equation $x^2 + D = y^n$, when the prime divisors of D are restricted to a fixed finite set S. This is joint work with Samir Siksek and, in part, with Philippe Michaud-Jacobs. Our results rely upon a combination of various results based upon the modularity of Galois representations, with bounds for linear forms in logarithms.

András Biró

biro.andras@renyi.hu, (Alfréd Rényi Institute of Mathematics (Hungary))

Class number one problem for a family of real quadratic fields

We effectively solve the class number one problem for a certain family $\mathbf{Q}\left(\sqrt{D}\right)$ $(D \in \mathcal{F})$ of real quadratic fields, where $\mathcal{F}$ is an infinite subset of the set of odd positive fundamental discriminants. The set $\mathcal{F}$ contains the Yokoi discriminants n^2+4, so our result is a generalization of the solution of Yokoi's Conjecture. But this family may contain fields with comparatively larger fundamental units than the fields in the Yokoi family (it may be as large as $\log^2 D$ instead of $\log D$). The proof is also a generalization of the proof of Yokoi's Conjecture.

Frederik Broucke

fabrouck.broucke@ugent.be, (Ghent University (Belgium))
Joint work with: Gregory Debruyne and Jasson Vindas

Malliavin's problems for Beurling generalized primes

A system of Beurling generalized primes $\mathcal{P}$ is a non-decreasing sequence of reals $p_1 \le p_2 \le \cdots$ with the requirement that $p_1 > 1$ and that $p_j \to \infty$. The associated system of generalized integers $\mathcal{N} = (n_0 = 1, n_1, n_2, \cdots)$ is the multiplicative semigroup generated by 1 and $\mathcal{P}$. With these systems one associates counting functions

$$\pi_{\mathcal{P}}(x) = \sum_{p_j \le x} 1, \quad N_{\mathcal{P}}(x) = \sum_{n_k \le x} 1.$$

One of the central goals of the theory is to investigate the relationship between these counting functions, especially when one is close to its classical counterpart. More specifically, we consider asymptotics of the form

$$\pi(x) = \int_2^x \frac{dt}{\log t} + O(R_1(x)), \quad \text{or} \quad N(x) = \rho x + O(R_2(x)),$$

where ρ is a positive constant and R_1 and R_2 are certain remainders. P. Malliavin [4] considered remainders of the form

$$R_1(x) = x\exp(-c_1 \log^{\alpha} x), \quad R_2(x) = x\exp(-c_2 \log^{\beta} x),$$

for some $c_1, c_2 > 0$ and with $\alpha, \beta \in (0, 1]$. It turns out that a remainder of the form R_1 for π implies a remainder of the form R_2 for N, and vice-versa. Malliavin's problems concern finding the optimal form of the remainders in these relations.

In this talk, I will present some recent progress in this problem. In particular, we recently definitively settled the direction $\pi \to N$. This talk is based on collaborative work with G. Debruyne and J. Vindas, which appeared in the articles [1, 2, 3].

References

[1] F. Broucke, *Note on a conjecture of Bateman and Diamond concerning the abstract PNT with Malliavin-type remainder*, Monatsh. Math. **196** (2021), no. 3, 456-470.

[2] F. Broucke, G. Debruyne, J. Vindas, *Beurling integers with RH and large oscillation*, Adv. Math. **370** (2020), article number 107240.

[3] F. Broucke, G. Debruyne, J. Vindas, *The optimal Malliavin-type remainder for Beurling generalized integers*, to appear in J. Inst. Math. Jussieu.

[4] P. Malliavin, *Sur le reste de la loi asymptotique de répartition des nombres premiers généralisés de Beurling*, Acta Math. **106** (1961), 281–298.

Yann Bugeaud

bugeaud@math.unistra.fr, (University of Strasbourg (France))

B'

Let $n \geq 1$ be an integer and $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers. Let $b_1, \ldots, b_n$ be integers with $b_n \neq 0$, and set $B = \max\{3, |b_1|, \ldots, |b_n|\}$. For $j = 1, \ldots, n$, let A_j be such that $\log A_j \geq \max\{h(\alpha_j), 2\}$, where h denotes the (logarithmic) Weil height. Assume that the quantity $\Lambda = b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n$ is nonzero. A typical lower bound of $\log |\Lambda|$ given by Baker's theory of linear forms in logarithms takes the shape

$$-c(n, D) \log A_1 \ldots \log A_n \log B,$$

where $c(n, D)$ is positive, effectively computable and depends only on n and on the degree D of the field generated by $\alpha_1, \ldots, \alpha_n$. However, in certain special cases and in particular when $|b_n| = 1$, this bound can be improved to

$$-c(n, D)\ \log A_1 \ldots \log A_n \log \frac{B}{\log A_n}.$$

The term $B' := B/\log A_n$ in place of B originates in works of Feldman and is a key tool for improving, in an effective way, the upper bound for the irrationality exponent of a real algebraic number of degree at least 3 given by Liouville's theorem. We survey various applications of Feldman's B' to exponents of approximation evaluated at algebraic numbers, to the S-part of integer sequences, and to Diophantine equations.

Cecile Dartyge

Cecile.Dartyge@univ-lorraine.fr, (Université de Lorraine (France))
Joint work with: James Maynard

On the largest prime factor of quartic polynomial values : the dihedral and cyclic cases

Let P be a monic, quartic and irreducible polynomial with integer coefficients and with a cyclic or dihedral Galois group.

We prove that there exists $c_P > 0$ such that $P(n)$ has a prime factor $> n^{1+c_P}$ for a positive proportion of integers n.

Gregory Debruyne

gregory.debruyne@ugent.be, (Ghent University (Belgium))
Joint work with: Jasson Vindas

Optimality in Tauberian theorems

One version of the Ingham-Karamata theorem states that for each *slowly oscillating* function τ whose Laplace transform admits an analytic continuation beyond the line $\Re s\ s = 0$ must obey the asymptotic law $\tau(x) = o(1)$. This theorem is a cornerstone in Tauberian theory and has plenty of applications in number theory; one of the quickest proofs of the Prime Number Theory passes through this theorem.

In this talk, we shall investigate if one can obtain stronger asymptotics on τ if one assumes the analytic extension of the Laplace transform goes up to a certain half-plane $\Re s\ s = -C$. The answer is negative if one assumes merely analytic continuation on these half-planes; we shall provide a non-constructive proof of this fact that is based on the open mapping theorem.

Andrej Dujella

duje@math.hr, (University of Zagreb (Croatia))
Joint work with: Gökhan Soydan

On elliptic curves induced by rational Diophantine quadruples

We consider elliptic curves induced by rational Diophantine quadruples, i.e. sets of four nonzero rationals such that the product of any two of them plus 1 is a perfect square. We show that for each of the groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ for $k = 2, 4, 6, 8$, there are infinitely many rational Diophantine quadruples $\{a, b, c, d\}$ with the property that the elliptic curve birationally equivalent to the curve $y^2 = (ax+1)(bx+1)(cx+1)(dx+1)$ has this torsion group. We also construct elliptic curves with moderately large ranks in each of these four cases.

Christian Elsholtz

elsholtz@math.tugraz.at, (Graz University of Technology (Austria))
Joint work with: Rainer Dietmann, Alexander Kalmynin, Sergei Konyagin and James Maynard

Longer gaps between values of binary quadratic forms

We prove new lower bounds on large gaps between integers which are sums of two squares, or are represented by *any* binary quadratic form of discriminant D, improving results of Richards. Let $s_1, s_2, \ldots$ be the sequence of positive integers, arranged in increasing order, that are representable by *any* binary quadratic form of fixed discriminant D, then

$$\limsup_{n\to\infty} \frac{s_{n+1} - s_n}{\log s_n} \gg \frac{|D|}{\varphi(|D|) \log |D|},$$

improving a lower bound of $\frac{1}{|D|}$ of Richards. In the special case of sums of two squares, we improve Richards's bound of 1/4 to $\frac{390}{449} = 0.868\ldots$.

We also generalize Richards's result in another direction: If d is composite we show that there exist constants C_d such that for all integer values of x none of the values $p_d(x) = C_d + x^d$ is a sum of two squares. Let d be a prime. For all $k \in \mathbf{N}$ there exists a smallest positive integer y_k such that none of the integers $y_k + j^d, 1 \leq j \leq k$, is a sum of two squares. Moreover,

$$\limsup_{k\to\infty} \frac{k}{\log y_k} \gg \frac{1}{\sqrt{\log d}}.$$

The pdf of the paper is on the speaker's webpage.

Jan-Hendrik Evertse

evertse@math.leidenuniv.nl, (Leiden University (The Netherlands))
Joint work with: Manjul Bhargava, Kálmán Győry, László Remete and Ashvin A. Swaminathan

Equivalence relations of polynomials

We recall a long-forgotten notion of equivalence for polynomials in $\mathbb{Z}[X]$ introduced by Hermite in the 1850s. We compare this with better known equivalence relations for such polynomials, i.e., $\mathrm{GL}_2(\mathbb{Z})$-equivalence and order equivalence (in the talk we define the order associated to a polynomial in $\mathbb{Z}[X]$; then two polynomials in $\mathbb{Z}[X]$ are order equivalent if they have the same associated order). As it will turn out, $\mathrm{GL}_2(\mathbb{Z})$-equivalence implies Hermite equivalence, which in turn implies order equivalence. From work of Delone and Faddeev (1940) it follows that for cubic polynomials in $\mathbb{Z}[X]$ these equivalence relations coincide, but for higher degree polynomials this is no longer the case. We will discuss this in more detail.

Victor Fadinger

victor.fadinger@uni-graz.at, (University of Graz (Austria))
Joint work with: Sophie Frisch and Daniel Windisch

Integer-valued polynomials on discrete valuation rings of global fields with prescribed lengths of factorizations

Let V be a discrete valuation domain with residue field of characteristic $p \geq 3$ whose quotient field K is a global field. We show that for all integers $1 \leq k$ and $2 \leq n_1 \leq \ldots \leq n_k$ there exists an integer-valued polynomial on V, that is, an element of $\mathrm{Int}(V) = \{f \in K[X] \mid f(V) \subseteq V\}$, which has precisely k essentially different factorizations into irreducible elements of $\mathrm{Int}(V)$ whose lenghts are exactly $n_1, \ldots, n_k$. This solves an open problem proposed by Cahen, Fontana, Frisch and Glaz in this case.

Sébastien Ferenczi

ssferenczi@gmail.com, (Aix-Marseille University (France))
Joint work with: Pascal Hubert

A dynamical application of Ostrowki's algorithm

We look at *d-point extensions* of a rotation of angle α with r marked points, generalizing the famous examples of Veech 1969 and Sataev 1975. The Ostrowski expansions of the marked points by α allows us to study the dynamical property of *rigidity* for these examples, and its relation to the word-combinatorial property of *linear recurrence* for the natural coding of the rotation with marked points. This allows us to build the first examples of non linearly recurrent and non rigid interval exchange transformations.

Ferdinánd Filip

filipf@ujs.sk, (J. Selye University (Slovakia))
Joint work with: János T. Tóth

On the powers of asymptotic density

A natural method for measuring sets of natural numbers is the asymptotic density, which is a special case of weighted densities. These densities are based on the Riesz summation method. More generally, any regular non-negative Toeplitz matrix determines a density. Let $\mathbf{C}$ denote the matrix that generates the asymptotic density.

In our talk, we study the relation of the densities defined by the matrices $\mathbf{C}^k$, $(k = 2, 3, \dots)$ to the asymptotic and logarithmic densities.

Alan Filipin

alan.filipin@grad.unizg.hr, (University of Zagreb (Croatia))
Joint work with: Ana Jurasić

Polynomial $D(-3)$-quadruples

In this talk we prove that there does not exist a set of four non-zero polynomials from $\mathbb{Z}[X]$, not all constant, such that the product of any two of its distinct elements decreased by 3 is a square of a polynomial from $\mathbb{Z}[X]$. For integer $n \neq 0$, a set of m positive integers is called $D(n)$-m-tuple if products of any two of its distinct elements increased by n is a perfect square. There are many results concerning the upper bounds for such sets. It is easy to prove that if $n \equiv 2 \pmod 4$, then there does not exist a $D(n)$-quadruple. On the other hand, Dujella proved that if $n \not\equiv 2 \pmod 4$ and $n \notin S = \{-4, -3, -1, 3, 5, 8, 12, 20\}$, then there exist at least one $D(n)$-quadruple. Moreover, he conjectured that there does not exist a $D(n)$-quadruple, if $n \in S$. That conjecture is still open, but was recently confirmed for $n = -1$ and $n = -4$. Here we consider the polynomial version of this problem, and proving that there does not exist a polynomial $D(-3)$-quadruple in $\mathbb{Z}[X]$, together with previous results of more authors, we finish the proof that there does not exist such polynomial $D(n)$-quadruple for $n \in S$.

Pavel Francírek

francirek@math.muni.cz, (Masaryk University (Czech Republic))
Joint work with: Radan Kučera

Annihilators of the ideal class group of an imaginary abelian field

The aim of this talk is to study annihilators of the minus part of the ideal class group of an imaginary abelian field M. The usual source of these annihilators is the Stickelberger ideal (defined by Sinnott) whose elements come from the factorization of Gauss sums. Under certain assumptions on M, we managed to enlarge this ideal by adding annihilators obtained by factoring a suitable generalized root of modified Gauss sums. It can be shown that this enlarged Stickelberger ideal is strictly larger than the Stickelberger ideal if there is an odd prime $\ell \mid [M : \mathbb{Q}]$, unramified in $M/\mathbb{Q}$, and two primes q and q' ramifying in $M/\mathbb{Q}$, having their decomposition groups $D_q \subseteq D_{q'}$ cyclic of ℓ-power order.

István Gaál

gaal.istvan@unideb.hu, (University of Debrecen (Hungary))

Monogenity and power integral bases

Monogenity and power integral bases is a classical topic of algebraic number theory, which is intensively studied even nowadays, cf. [1]. In our survey we describe the most important classical and recent results and the most important methods that can be applied to prove monogenity or non-monogenity of number fields and certain classes of number fields.

References

[1] I. Gaál, Diophantine equations and power integral bases. Theory and algorithms. 2nd edition, Birkhäuser, Boston, 2019.

Mikhail R. Gabdullin

gabdullin@mi-ras.ru, (Steklov Mathematical Institute (Russia))
Joint work with: Kevin Ford

Sets whose differences avoid squares modulo m

Let $A \subset \mathbb{Z}_m$ be such that $A - A$ does not contain nonzero quadratic residues modulo m.

It is highly believed that for square-free m the bound $|A| \ll_\varepsilon m^\varepsilon$ holds for any $\varepsilon > 0$, but this hypothesis seems to be far beyond the reach of current methods. M. Matolcsi and I. Ruzsa proved that $|A| \leq m^{1/2}$ if m is square-free and has prime divisors of the form $4k+1$ only, and I showed that $|A| \ll m^{1/2+o(1)}$ for almost all positive integers m.

In our joint work with K. Ford we overcome this square-root barrier and prove that if $\varepsilon(m) \to 0$ arbitrarily slowly, then for almost all m we have $|A| \leq m^{1/2-\varepsilon(m)}$.

Krystian Gajdzica

Krystian.Gajdzica@im.uj.edu.pl, (Jagiellonian University (Poland))

The log-concavity of the restricted partition function $p_{\mathcal{A}}(n,k)$ and beyond

Let k be a positive integer, and let $\mathcal{A}$ be a weakly increasing sequence of positive integers. The restricted partition function $p_{\mathcal{A}}(n,k)$ enumerates all partitions of n whose parts belong to the multiset $\{a_1, a_2, \ldots, a_k\}$. We discuss under what conditions on k and $\mathcal{A}$, the function $p_{\mathcal{A}}(n,k)$ is log-concave — it satisfies

$$p_{\mathcal{A}}^2(n,k) > p_{\mathcal{A}}(n+1,k)p_{\mathcal{A}}(n-1,k)$$

for all sufficiently large values of n. Moreover, we also investigate other inequalities of this type for the function $p_{\mathcal{A}}(n,k)$. Among other things, we show some results related to: the strong log-concavity, the log-balancedness, the higher order Turán inequalities and the r-log-concavity.

Filip Gawron

filipux.gawron@student.uj.edu.pl, (Jagiellonian University (Poland))
Joint work with: Tomasz Kobos

On the length of the period of the continued fraction of $n\sqrt{d}$

It is known that if α is a quadratic irrational number then the continued fraction expansion of α is eventually periodic. Let us denote by $D(\alpha)$ the length of the periodic part of the continued fraction expansion. In the paper from 1972, Chowla and Chowla [1] asked the following question:

Question 1. For a given integer $k \geq 1$, are there infinitely many integers $d \geq 1$ such that $D(\sqrt{d}) = k$?

The answers turns out to be positive, which was shown by Friesen in [2]. Changing the point of view, we can fix a positive integer d, which is not a perfect square, and study the set of values of the sequence $(D(n\sqrt{d}))_{n=1}^{\infty}$. This raises a natural question:

Question 2. For a given integers $k \geq 1$ and $d \geq 1$, are there infinitely many integers $n \geq 1$ such that $D(n\sqrt{d}) = k$?
Contrary to the previous question, the answer turns out easily to be negative. For example, if $D(\sqrt{d})$ is even, then $D(n\sqrt{d})$ is also even for every $n \geq 1$. Therefore, in order to make this question more specific and interesting, we define

$$A_d = \{k \in \mathbb{N} : \text{ there exist infinitely many } n \text{ for which } D(n\sqrt{d}) = k\}.$$

In other words, A_d is the set of limit points of the sequence $(D(n\sqrt{d}))_{n=1}^{\infty}$. In my talk, I will describe the connections between continued fractions, Pell's equation, and the Euclidean algorithm. Then I will use these connections to show the idea of proof that for fixed positive integer d, which is not a perfect square, the set A_d contains infinitely many even numbers. Finally, I will mention some conjectures related to the set A_d.

References

[1] P. Chowla. S. Chowla, *Problems on Periodic Simple Continued Fractions*, Proceedings of the National Academy of Sciences, **69** (1972), 3745-3745.

[2] C. Friesen, *On continued fractions of given period*, Proc. Amer. Math. Soc. **103** (1988), 8-14.

Daniel Goldston

daniel.goldston@sjsu.edu, (San José State University (USA))
Joint work with: Ade Irma Suriajaya

Pair Correlation of Zeta-Zeros and Two Problems on Primes

We assume the Riemann Hypothesis. Denoting a complex zero of the Riemann zeta-function by $\rho = 1/2 + i\gamma$, Montgomery introduced the function

$$F(x,T) := \sum_{0<\gamma,\gamma' \leq T} x^{i(\gamma-\gamma')} \frac{4}{4+(\gamma-\gamma')^2},$$

which is useful in studying the pair correlation of zeros. He conjectured that F satisfies an asymptotic formula in the range $T \leq x \leq T^M$ for any fixed constant M. This conjecture improves on a number of classical results on primes obtained assuming the Riemann Hypothesis. We show by extending the range of Montgomery's conjecture that we can improve the error term in a formula of Fujii for the average number of Goldbach representations and also the error in the prime number theorem.

References

[1] D. A. Goldston and A. I. Suriajaya, *On an average Goldbach representation formula of Fujii*, https://arxiv.org/abs/2110.14250

[2] D. A. Goldston and A. I. Suriajaya, *The prime number theorem and pair correlation of zeros of the Riemann zeta-function*, https://arxiv.org/abs/2205.06503

Domingo Gómez-Pérez

domingo.gomez@unican.es, (University of Cantabria (Spain))
Joint work with: Ana I. Gómez

Revisiting the linear complexity of a random bit lattice

The study of measures of pseudorandomness has received much attention in the over the last two decades. The work of Sárközy, Maudit, Golomb and many others have been fundamental to understand the behavior of random sequences and construct pseudorandom sequences for communications and cryptography. Multidimensional lattice (or multidimensional arrays) are mathematical objects studied for encryption and watermarking bitmap. Hubert, Mauduit and Sárközy [3] generalized several measures of pseudorandomness from binary sequences to their multidimensional equivalent. One missing measure was linear complexity, which is an important and frequently used measure of unpredictability for sequences. This measure was introduced in [1] for two dimensional lattices and further developed in [2], where the authors conjectured that the normalized linear complexity is close to 1/2.

In this talk, we plan to show several new results towards the solution of the conjecture, a new relationship between pseudorandom measure of order ℓ and the linear complexity. Finally, we will discuss high order correlation attacks on several families of multidimensional arrays.

References

[1] Katalin Gyarmati, Christian Mauduit, and András Sárközy. On the linear complexity of binary lattices. *The Ramanujan Journal*, 32(2):185–201, 2013.

[2] Katalin Gyarmati, Christian Mauduit, and András Sárközy. On linear complexity of binary lattices, II. *The Ramanujan Journal*, 34(2):237–263, 2014.

[3] Pascal Hubert, Christian Mauduit, and András Sárközy. On pseudorandom binary lattices. *Acta Arithmetica*, 125:51–62, 2006.

Krisztián Gueth

gueth.krisztian@sek.elte.hu, (Eötvös Loránd University (Hungary))

On a Diophantine equation involving k-Fibonacci numbers

In this lecture, we deal with the so-called k-Fibonacci sequence. Let $G_0 = 0$, $G_1 = 1$, and $G_n = kG_{n-1}+G_{n-2}$ for any $n \geq 2$, where k is a fixed positive integer. We determine the solutions to the diophantine equation

$$G_1^p + 2G_2^p + \cdots + \ell G_\ell^p = G_n^q$$

in positive integers ℓ, n if k, p and q are small. More precisely we suppose that $p, q, k \leq 10$. These bounds are subjective, the method, al least in theory would work with arbitrary p, q, and k.

Tomislav Gužvić

tguzvic@math.hr, (University of Zagreb (Croatia))

Torsion groups of elliptic curves with rational j-invariant

Let $[K : \mathbb{Q}] = p$ be a prime number and let E/K be an elliptic curve with $j(E) \in \mathbb{Q}$. We determine the all possibilities for $E(K)_{tors}$. We obtain these results by studying Galois representations of E and of its quadratic twists.

Katalin Gyarmati

katalin.gyarmati@ttk.elte.hu, (Eötvös Loránd University (Hungary))

Pseudorandomness of Legendre sequences based on random polynomials

It is crucial in pseudorandomness cryptographic applications that the smaller key used as a seed can be generated at random. Thus, if you use the Legendre sequence based on a polynomial (proposed by Hoffstein and Lieman) that is

$$\left\{ \left(\frac{f(1)}{p} \right), \left(\frac{f(2)}{p} \right), \left(\frac{f(3)}{p} \right), \ldots, \left(\frac{f(p)}{p} \right) \right\},$$

it is important to choose the polynomial coefficients at random. Goubin, Mauduit, and Sárközy presented some non-restrictive conditions on the polynomial f, but these conditions may not be satisfied if we choose a truly random polynomial. However, how can it be ensured that the sequence's pseudorandom measures are always low for polynomials that are almost "random"? These seemingly random polynomials will be constructed with as few modifications as necessary from a true random polynomial. The difficulties raised above will be discussed in my talk.

Eszter Gyimesi
gyimesie@science.unideb.hu, (University of Debrecen (Hungary))
Joint work with: Gábor Nyul

Associated r-Dowling numbers and some relatives

In our talk, we introduce and study a new generalization of Bell numbers by combining r-Bell numbers, associated Bell numbers and Dowling numbers. For defining these s-associated r-Dowling numbers, we partition elements into blocks so that r distinguished elements have to be in distinct blocks, the cardinality of certain blocks is bounded from below by s, and some elements are coloured according to a colouring rule. Along with them, we define some relatives, the s-associated r-Dowling factorials and the s-associated r-Dowling–Lah numbers, when the underlying set is decomposed into cycles or ordered blocks.

The results on these numbers are highly based on the exponential generating function of their sequences derived from the so-called r-compositional formula also presented in this talk. The talk is based on a joint paper [1] with Gábor Nyul.

References

[1] E. Gyimesi and G. Nyul, *Associated r-Dowling numbers and some relatives*, Comptes Rendus Mathématique **359** (2021), 47–55.

Lajos Hajdu

hajdul@science.unideb.hu, (University of Debrecen (Hungary))
Joint work with: Kálmán Győry and András Sárközy

Indecomposability of sequences defined by narrow sets of primes

A set $\mathcal{A}$ of positive integers is called additively or multiplicatively irreducible if it cannot be written as $\mathcal{A} = \mathcal{B}+\mathcal{C}$ or $\mathcal{A} = \mathcal{B}\cdot\mathcal{C}$, respectively, with $\mathcal{B}, \mathcal{C} \subset \mathbb{N}$, $|\mathcal{B}|, |\mathcal{C}| \geq 2$. In the talk we summarize recent results about the additive and multiplicative irreducibility, in the asymptotic sense, of sets $\mathcal{A}$ composed of a narrow set of primes. While these questions are strongly related to classical problems in additive and multiplicative number theory, in the proofs we need to combine deep tools from the theory of exponential Diophantine equations with various methods from prime number theory and combinatorics.

Gergely Harcos

gharcos@renyi.hu, (Alfréd Rényi Institute of Mathematics (Hungary))
Joint work with: Péter L. Erdős, Shubha R. Kharel, Péter Maga, Tamás R. Mezei and Zoltán Toroczkai

The sequence of prime gaps is graphic II.

This is the second part of two talks (the first part will be delivered by Péter Maga). Let us call a simple graph on $n > 1$ vertices a prime gap graph if its vertex degrees are 1 and the first $n-1$ prime gaps (we need the 1 so that the sum of these numbers is even). We can show that such a graph exists for every large n, and under RH for every $n > 1$. Moreover, a sequence of such graphs can be generated by a so-called degree preserving growth process: in any prime gap graph on n vertices, we can find $(p_{n+1}-p_n)/2$ independent edges, delete them, and connect the ends to a new, $(n+1)$-th vertex. This creates a prime gap graph on $n+1$ vertices, and the process never ends.

Norbert Hegyvári

hegyvari@renyi.hu, (Eötvös Loránd University (Hungary) and Alfréd Rényi Institute of Mathematics (Hungary))

Problems in Combinatorial Number Theory related to Computer Science

In the last decades there are several interplay between theoretical computer sciences and additive combinatorics. In this short talk we present some new applications of additive combinatorics in theory of Boolean functions. Some related problems are also discussed.

Orsolya Herendi

herendi.orsolya@science.unideb.hu, (University of Debrecen (Hungary))
Joint work with: Lajos Hajdu

Extrema of polynomials with real roots and Diophantine equations

There are many results in the literature concerning polynomial values and (shifted) power values of polynomials with consecutive integer roots, or more generally, with roots forming an arithmetic progression. It is an interesting question that how far one can 'disturb' the structure of the roots such that the finiteness results still remain valid. Also there are many results into this direction, with adding or removing one or more terms (roots).

In this talk we study a case where (part of) the symmetric root structure is preserved, however, we allow (possibly large) increasing gaps between the roots. We prove that the finiteness of the solutions can also be guaranteed under these generalized circumstances. In our proofs we combine Baker's method and the Bilu-Tichy theorem with a new result providing an increasing property of the extremal values of polynomials with distinct real roots satisfying certain symmetry and increasing gap properties.

Tamás Herendi

herendi.tamas@inf.unideb.hu, (University of Debrecen (Hungary))

Construction of Uniformly Distributed Linear Recurring Sequences Over Dedekind Domains

Uniformly distributed pseudorandom number sequences play an essential role in several applications. One frequently used construction is the linear congruential method. In the present paper, we give a sufficient condition for the generator, such that the corresponding sequence has a uniform distribution in an infinite set of residue rings. In particular, let D be a Dedekind domain, $q \in D[x]$ be a monic irreducible polynomial, $p(x) = (x-1)^2 q(x)$, and let $\mathcal{P} \in D$ be a prime ideal with a prime norm. If u is a sequence satisfying a linear recurrence relation and its minimal characteristic polynomial is p, then u is uniformly distributed mod $\mathcal{P}^s$, for any $s \in \mathbb{N}$.

Tobias Hilgart
tobias.hilgart@plus.ac.at, (University of Salzburg (Austria))

On families of cubic split Thue equations parametrised by linear recurrence sequences

Let $(A_n)_{n\in\mathbb{N}}, (B_n)_{n\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}}$ be two linear-recurrent sequences that meet a dominant root condition and a few additional, technical requirements. We show that the split family of Thue equations

$$\left|X(X - A_nY)(X - B_nY) - Y^3\right| = 1$$

has but the trivial solutions, where $(|x|, |y|) \in \{(1, 0), (0, 1), (|A_n|, 1), (|B_n|, 1)\}$, if the parameter n is larger than some effectively computable constant.

This work follows the one of Thomas [1] and Heuberger [2], who proved similar results if one parametrises the Thue equations by integer polynomials instead of linear-recurrent integer sequences, after experimental observations in [3] and [4] showed that such a derivation could lead to similar results.

References

[1] *E. Thomas*, *Complete solutions to a family of cubic Diophantine equations*, J. Number Theory 34, No. 2, 235–250 (1990)

[2] *C. Heuberger*, *On a conjecture of E. Thomas concerning parametrized Thue equations*, Acta Arith. 98, No. 4, 375–394 (2001)

[3] *T. Hilgart* and *I. Vukusic* and *V. Ziegler*, *On a family of cubic Thue Equations involving Fibonacci and Lucas numbers*, INTEGERS, Electronic Journal of Combinatorial Number Theory 22 (2022)

[4] *I. Vukusic*, On a cubic family of Thue equations involving Fibonacci numbers and powers of two, Quaestiones Mathematicae (2021)

Henryk Iwaniec

iwaniec@comcast.net, (Rutgers University (United States of America))

The large sieve aberrations

In this talk I will give a survey of classical results and modern developments in the large sieve methods. Special considerations will be given to the large sieve with respect to families of Dirichlet's characters. I will discuss peculiar features of the large sieve inequalities for the Fourier coefficients of automorphic forms in the spectral aspect.

Jerzy Kaczorowski

kjerzy@amu.edu.pl, (Adam Mickiewicz University (Poland))
Joint work with: Alberto Perelli

Classification of L-functions of degree 2 and conductor 1

After a short review of the known fact of the structure of the Selberg class, we give a complete description of the functions F of degree 2 and conductor 1 in the general framework of the extended Selberg class $S^\sharp$. This is performed using a new numerical invariant χ_F, which is easily computed from the data of the functional equation. We show that the value of χ_F gives a precise description of the nature of F, thus providing a sharp form of the classical converse theorems of Hecke and Maass. In particular, our result confirms, in the special case under consideration, the conjecture that the functions in the Selberg class S are automorphic L-functions.

Laima Kaziulyte

laima.kaziulyte@gmail.com, (University of Reading (United Kingdom))

Omega result for the remainder term in Beurling's prime number theorem for well-behaved integers

In this paper we obtain a new Ω-result for the remainder term $\psi(x) - x$ of a Beurling prime system for which the integers are very well-behaved in the sense that $N(x) = ax + O(x^\beta)$ for some $a > 0$ and $\beta < \frac{1}{2}$.

As part of this, we prove how bounds on $\psi(x) - x$ lead to zero-free regions for the Beurling zeta function, generalizing a result of Pintz to the Beurling setting. This may be of independent interest.

Dong Han Kim

drkimdh@gmail.com, (Dongguk University (South Korea))
Joint work with: Byungchul Cha

Intrinsic Diophantine approximation of spheres and the complex plane

Let $\mathbf{S}^2_{\mathrm{I}}$ and $\mathbf{S}^2_{\mathrm{II}}$ be the unit sphere and the sphere of radius $\sqrt{2}$ in $\mathbb{R}^3$, both centered at the origin. Let $A = \{(x_0, x_1, x_2, x_3) \in \mathbb{R}^4 \mid x_0 + x_1 + x_2 + x_3 = 1\}$ and $\mathbf{S}^2_{\mathrm{III}}$ be the sphere of the intersection of the unit 3-sphere in $\mathbb{R}^4$ and A. We consider Diophantine approximation on $\mathbf{S}^2_{\mathrm{I}}$, $\mathbf{S}^2_{\mathrm{II}}$ and $\mathbf{S}^2_{\mathrm{III}}$. For $\mathbf{x} \in \mathbf{S}^2_{\mathrm{I}}, \mathbf{S}^2_{\mathrm{II}}, \mathbf{S}^2_{\mathrm{III}}$. we define Lagrange number as

$$L_{\mathbf{S}}(\mathbf{x}) = \limsup_{\mathbf{p}/q \in \mathbb{Q}^3} q \left\| \mathbf{x} - \frac{\mathbf{p}}{q} \right\|,$$

where the limit superior runs over $\mathbf{p}/q \in \mathbb{Q}^3$ or $\mathbf{p}/q \in \mathbb{Q}^4 \cap A^3$ for an integral vector $\mathbf{p}$ and a positive integer q without common factors. On the other hand, for $\xi \in \mathbb{C}$, we define Lagrange number with respect to an imaginary quadratic number field $\mathbb{Q}(\sqrt{d})$ as

$$L_{\mathbb{Q}(\sqrt{d})}(\xi) = \limsup_{z/w \in \mathbb{Q}(\sqrt{d})} |w|^2 \left| \xi - \frac{z}{w} \right|.$$

The Diophantine approximation on the spheres $\mathbf{S}^2_{\mathrm{I}}$, $\mathbf{S}^2_{\mathrm{II}}$ and $\mathbf{S}^2_{\mathrm{III}}$ with rational points of $\mathbb{R}^3$ and A^3 are equivalent to the Diophantine approximation on the complex plane with Gaussian rationals $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$ and Eisenstein rationals $\mathbb{Q}(\sqrt{-3})$ respectively, in the sense that there are continuous maps from the spheres $\mathbf{S}^2_{\mathrm{I}}$, $\mathbf{S}^2_{\mathrm{II}}$ and $\mathbf{S}^2_{\mathrm{III}}$ to $\mathbb{C} \cup \{\infty\}$ which preserve the Lagrange number with respect to $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-3})$ respectively up to constants.

Sándor Kiss

ksandor@math.bme.hu, (Budapest University of Technology and Economics (Hungary))
Joint work with: Csaba Sándor

Dense sumsets of Sidon sets

Let $k \geq 2$ be an integer. A set A of positive integers is called asymptotic basis of order k if every large enough positive integer can be written as the sum of k terms from A. A set of positive integers A is said to be a Sidon set if all the two terms sums formed by the elements of A are different. Many years ago Pál Erdős, András Sárközy and

Vera T. Sós asked whether there exists a Sidon set which is asymptotic basis of order 3. In this talk I prove the existence of a Sidon set A with positive lower density of the three fold sumset $A + A + A$ by using probabilistic methods.

Attila Kovács and Norbert Tihanyi
attila.kovacs@inf.elte.hu,ntihanyi@inf.elte.hu, (Eötvös Loránd University (Hungary))
Joint work with: Bertalan Borsos

Tight upper and lower bounds for the reciprocal sum of generalized Proth primes

Calculating the reciprocal sum of sparse integer sequences can be challenging from both mathematical and computational aspects. Just to name a few examples: amicable numbers, Carmichael numbers, twin primes. These are examples where even the first decimal digit is unknown. In order to be able to compute accurate bounds the exact structure of the sequences needs to be unfolded. A *Proth* number is a natural number of the form $k \cdot 2^s + 1$ where $k, s \in \mathbb{N}$, k is odd and $k < 2^s$. In 1979 [1] Erdős and Odlyzko investigated the natural density of the prime numbers having the form $k \cdot 2^s + 1$ without the $k < 2^s$ restriction. It was shown that odd integers k such that $k \cdot 2^s + 1$ is prime for some positive integer s have a positive lower density. Assuming the Generalized Riemann Hypothesis one can prove that there exists at least one prime in the arithmetic progression $k \cdot 2^s + 1$ with $k < 2^{s+\epsilon}$. Without the additional ϵ the prime counting problem becomes extremely hard. Solving the problem of Siegel zeroes could help, however, this seems even harder. Let us denote the set of Proth primes by $\mathcal{R}$ and the sum of the reciprocals of Proth primes by $\omega_{\mathcal{R}} = \sum_{p \in \mathcal{R}} \frac{1}{p} = \frac{1}{3} + \frac{1}{5} + \frac{1}{13} + \frac{1}{17} + \cdots$. It was shown by the authors [2] that $0.7473924793 < \omega_{\mathcal{R}} < 0.7473924795$. In this talk we consider the generalized Proth numbers for any given $p \in \mathcal{P}$ by $\mathcal{T}_p = \{k \cdot p^n + 1 : k < p^n\, , (k, p) = 1, n \in \mathbb{N}\}$. Let us denote the sum of the reciprocals of $\mathcal{T}_p$ by

$$\omega_p = \sum_{i=1}^{\infty} \frac{1}{T_i^p} = \frac{1}{p+1} + \cdots .$$

Among other results we proved the following theorem:

Theorem 1. *ω_p can be calculated by*

$$\omega_p = \sum_{i=1}^{\infty} p^{-i-1}\Big(\Psi(p^{i+1}+p^{-i-1}) - \Psi(p^{i-1}+p^{-i-1})\Big) + \\ \big(\Psi(p+1+1/p)-\Psi(1+1/p)\big)p^{-1} + (1+p^2)^{-1}\,.$$

We are interested in searching for primes in each set of $\mathcal{T}_p$. The result of Goldfeld implies that there are infinitely many $p \in \mathcal{P}$ exists where at least one prime can be found in the appropriate set $\mathcal{T}_p$. We show that ω_p can efficiently be used to give a general formulae for the reciprocal sum of the primes in $\mathcal{T}_p$.

References

[1] P. Erdős, A.M. Odlyzko, *On the density of odd integers of the form $(p-1)2^{-n}$ and related questions*, Journal of Number Theory, Volume 11, Issue 2, 1979

[2] Bertalan Borsos, Attila Kovács, Norbert Tihanyi Tight upper and lower bounds for the reciprocal sum of Proth primes. Ramanujan Journal (2022). `https://doi.org/10.1007/s11139-021-00536-2`

Radan Kučera

kucera@math.muni.cz, (Masaryk University (Czech Republic))
Joint work with: Olivier Bernard

A short basis of the Stickelberger ideal of a cyclotomic field

We exhibit an explicit *short* basis of the Stickelberger ideal of cyclotomic fields of any conductor m, i.e., a basis containing only short elements. By definition, an element of $\mathbb{Z}[G_m]$, where G_m denotes the Galois group of the field, is called short whenever it writes as $\sum_{\sigma\in G_m} \varepsilon_\sigma \sigma$ with all $\varepsilon_\sigma \in \{0,1\}$.

As a direct practical consequence, we deduce from this short basis an *explicit* upper bound on the relative class number of the considered cyclotomic field, that is valid for *any* conductor. This basis also has several concrete applications, in particular for the cryptanalysis of the Shortest Vector Problem on Ideal lattices, one of the mathematical problems considered as a possible base for a post-quantum cryptosystem.

References

[1] O. Bernard, R. Kučera: A short basis of the Stickelberger ideal of a cyclotomic field, arXiv:2109.13329 [math.NT], 2021.

Renan Laureti

renan.laureti@univ-lorraine.fr, (Université de Lorraine (France))

Parry numbers and Pisot numbers

We are familiar with integer expansions, that is, for an integer b greater than 1, every real number in $[0, 1)$ can be written as $x = \sum_{n\geq 1} x_n b^{-n} = 0.x_1x_2...$ for a unique set of digits x_i that are integers lying in $[0, b)$, with the relation $0.999999\cdots = 1.000000\cdots$. The most natural generalisation, perhaps, of the integer expansions are called β-expansions and consist in writing x in the same way, but using instead of the integer b a real number β greater than 1, with the digits still being integers lying in $[0, \beta)$, but then x might have more than one expansion. This can be corrected by using the dynamical point of view with the transformation $T : x \mapsto \beta x$, but then a new problem arise regarding the cylinders, which are the intervals defined by finite words in a given base (for example the cylinders of order 1 in base 2 are $[0, 1/2)$, given by the word 0, and $[1/2, 1)$, given by the word 1). Indeed, in an integer base b, every cylinder of order n has length b^{-n}, while in a non integer base β, some cylinders, generated by the fractional part of β, have lengths that are not equal to β^{-n} at order n. In general, there are infinitely many types of cylinders for a beta expansion. The real numbers β such that there are only finitely many types of $\beta - cylinders$ are called *Parry numbers* [1]. Every Pisot number, as well as some Salem numbers, are known to be Parry numbers. Conversely, Schmidt (1980) showed that Parry numbers verifying a certain condition must be either Pisot numbers or Salem Numbers. In this talk, I will show examples of how the Pisot and Parry condition are connected in small degrees as well as examples of non Parry numbers.

References

[1] `https://www.irif.fr/~steiner/num09/akiyama.pdf`

Tamás Lengyel

lengyel@oxy.edu, (Occidental College (USA))

On the 2-adic valuation of differences of harmonic numbers

We explicitly determine the exact 2-adic valuation of differences of harmonic sums. We also provide lower bounds on the 2-adic valuations of elementary symmetric functions of $1, 1/2, \ldots, 1/n$. We present applications to obtain lower bounds on the 2-adic valuations of products of binomial coefficients and differences of harmonic numbers, and lacunary sums involving binomial coefficients.

Jared Duker Lichtman

jared.d.lichtman@gmail.com, (University of Oxford (United States of America))

A proof of the Erdős primitive set conjecture

A set of integers greater than 1 is primitive if no member in the set divides another. Erdős proved in 1935 that the series $f(A) = \sum_{a\in A} 1/(a \log a)$ is uniformly bounded over all choices of primitive sets A. In 1988 he asked if this bound is attained for the set of prime numbers. In this talk we describe recent work which answers Erdős' conjecture in the affirmative. We will also discuss applications to old questions of Erdős, Sárközy, and Szemerédi from the 1960s.

Kálmán Liptai

liptai.kalman@uni-eszterhazy.hu, (Eszterházy Károly Catholic University (Hungary))

Distribution generated by a random inhomogenous Fibonacci sequence

We consider an inhomogenous version $G_n = G_{n-1} + G_{n-2} + w_{n-2}, (n \geq 2)$ of the Fibonacci sequence with initial values $G_0 = 0, G_1 = 1$ and we suppose that the term w_n takes value a with probability p, and takes b with probability q (generated by a coin tossing). We describe the process and the distribution of G_n values.

Florian Luca

florian.luca@wits.ac.za, (Wits University (South Africa))

Joint work with: Yuri Bilu, Joris Nieuwveld, Joël Ouaknine, David Purser and James Worrell

Recent progress on the Skolem problem

The celebrated Skolem-Mahler-Lech Theorem states that the set of zeros of a linear recurrence sequence is the union of a finite set and finitely many arithmetic progressions. The corresponding computational question, the Skolem Problem, asks to determine whether a given linear recurrence sequence has a zero term. Although the Skolem-Mahler-Lech Theorem is almost 90 years old, decidability of the Skolem Problem remains open. The main contribution of this talk is to present an algorithm to solve the Skolem Problem for simple linear recurrence sequences (those with simple characteristic roots). Whenever the algorithm terminates, it produces a stand-alone certificate that its output is correct – a set of zeros together with a collection of witnesses that no further zeros exist. We give a proof that the algorithm always terminates assuming two classical number-theoretic conjectures: the Skolem Conjecture (also known as the Exponential Local-Global Principle) and the p-adic Schanuel Conjecture. Preliminary experiments with an implementation of this algorithm within the tool SKOLEM point to the practical applicability of this method.

Péter Maga

maga.peter@renyi.hu, (Alfréd Rényi Institute of Mathematics (Hungary))
Joint work with: Péter L. Erdős, Gergely Harcos, Shubha R. Kharel, Tamás R. Mezei and Zoltán Toroczkai

The sequence of prime gaps is graphic I.

This is the first part of two talks (the second part will be delivered by Gergely Harcos). Let us call a simple graph on $n > 1$ vertices a prime gap graph if its vertex degrees are 1 and the first $n-1$ prime gaps (we need the 1 so that the sum of these numbers is even). We can show that such a graph exists for every large n, and under RH for every $n > 1$. Moreover, a sequence of such graphs can be generated by a so-called degree preserving growth process: in any prime gap graph on n vertices, we can find $(p_{n+1}-p_n)/2$ independent edges, delete them, and connect the ends to a new, $(n+1)$-th vertex. This creates a prime gap graph on $n+1$ vertices, and the process never ends.

Máté Matolcsi

matemato@gmail.com, (Budapest University of Technology and Economics (Hungary))
Joint work with: Imre Z. Ruzsa

Difference sets avoiding cubic residues in cyclic groups

By constructing suitable nonnegative exponential sums, we give upper bounds on the cardinality of any set B_q in cyclic groups $\mathbb{Z}_q$ such that the difference set $B_q - B_q$ avoids cubic residues modulo q.

László Mérai

laszlo.merai@oeaw.ac.at, (Austrian Academy of Sciences (Austria))

Divisors of sums of polynomials

In a series of papers, Sárközy and Stewart studied the prime divisors of sum-sets $\mathcal{A}+\mathcal{B}$. Among others, they showed that if $\mathcal{A}, \mathcal{B} \subset \{1, \ldots, N\}$ are not too small, then there are $a \in \mathcal{A}$ and $b \in \mathcal{B}$ such that $a + b$ has large prime divisors.

In this talk we explore this problem for polynomials over finite fields. In particular, we show that if $\mathcal{A}, \mathcal{B} \subset \mathbb{F}_q[x]$ are sets of polynomials of degree n, then $a + b$ has large degree irreducible divisors for some $a \in \mathcal{A}, b \in \mathcal{B}$. In particular, if $\mathcal{A}, \mathcal{B}$ have positive relative densities, then $a + b$ has an irreducible divisor of degree $n + O(1)$ for some $a \in \mathcal{A}, b \in \mathcal{B}$.

Piotr Miska

piotr.miska@uj.edu.pl, (Jagiellonian University (Poland))
Joint work with: János T. Tóth

(R)-dense and (N)-dense subsets of positive integers and generalized quotient sets

A subset A of the set of positive integers is (R)-dense if its quotient set $R(A) = \{a/b : a, b \in A\}$ is dense in the positive real half-line (with respect to natural topology on real numbers). It is a classical result that the set of prime numbers is (R)-dense. The proof of this fact is based on the property of counting function of prime numbers. Actually, this proof shows something more. Namely, for each infinite subset B of the set of positive integers, the set $R(\mathbb{P}, B) = \{p/b : p \in \mathbb{P}, b \in B\}$ is dense in the set of positive real numbers. This motivates to introduce the notion of (N)-denseness. We say that a set A of positive integers is (N)-dense if the set $R(A, B)$ is dense in the set of positive real numbers for every set B of positive integers. During the talk we will consider characterizations of (N)-dense sets and connections between (N)-denseness of a given set.

In 2019 Leonetti and Sanna introduced the notion of direction sets

$$D^k(A) = \{(a_1/||a||^2, ..., a_k/||a||^2) : a = (a_1, ..., a_k) \in A^k\}$$

that allows us to generalize the property of (R)-denseness. Indeed, A is (R)-dense if and only if $D^2(A)$ is dense in the set of points of unit circle with all the coordinates positive. We will see that denseness of $D^k(A)$ in the set of points of unit sphere with all the coordinates positive is equivalent to denseness of the generalized quotient set

$$R^k(A) = \{(a_1/a_k, ..., a_{k-1}/a_k) : a_1, ..., a_k \in A\}$$

in the set of points of $\mathbb{R}^{k-1}$ with all the coordinates positive. We will also show some connections between (N)-denseness of a given set A and denseness of sets $R^k(A)$ with the counting function of A and its dispersion.

Ladislav Mišík

ladislav.misik@osu.cz, (J. Selye University (Slovakia))

Maximal subsequences with prescribed sets of accumulation points

Let (x_n) be a uniformly distributed sequence mod 1. It is easy to verify that every set of indices for which the corresponding subsequence of (x_n) has a finite set of accumulation points, has asymptotic density zero. In 2009 Bugeaud, generalizing the previous result by Dubickas showed that this convergence to zero can be arbitrarily slow in the class of all sequences of the form $\{n\alpha\}$, where α is an irrational number and $\{x\}$ is the fractional part of a number x. This result was later generalized in two directions. At first it was extended to the class of all uniformly distributed sequences, at second, finite sets were generalized to arbitrary closed sets. In this contribution we generalize the last result extending it to the class of all sequences with increasing asymptotic distribution function which includes the class of all uniformly distributed sequences.

Takafumi Miyazaki

tmiyazaki@gunma-u.ac.jp, (Gunma University (Japan))
Joint work with: István Pink

Number of solutions to a special type of unit equations in two unknowns II

We give a brief introduction about the recent progress on the best possible general estimate of the number of solutions to the equation $a^x + b^y = c^z$ for fixed relatively prime positive integers a, b and c with $\min\{a, b, c\} > 1$. It is conjectured that there is at most one solution to the equation except for specific cases. Our work [3] is the continuation of [2] and the results prove the conjecture in several cases. As applications we obtain some 3-variable versions of Bennett's works in [1] on the equation $a^x - b^y = c$ for fixed positive integers a, b and c with $\min\{a, b\} > 1$, as well as an analytic proof of the celebrated theorem of Scott [4] solving the conjecture for $c = 2$.

References

[1] M.A. Bennett, *On some exponential equations of S. S. Pillai*, Canad. J. Math. **53** (2001), 897–922.

[2] T. Miyazaki and I. Pink, *Number of solutions to a special type of unit equations in two variables*, preprint 2020, arXiv:2006.15952.

[3] T. Miyazaki and I. Pink, *Number of solutions to a special type of unit equations in two variables II*, preprint 2022, arXiv:2205.11217.

[4] R. Scott, *On the equations $p^x - b^y = c$ and $a^x + b^y = c^z$*, J. Number Theory **44** (1993), 153–165.

Gábor Nyul

gnyul@science.unideb.hu, (University of Debrecen (Hungary))

Enumerative combinatorial numbers and polynomials in graph theory

We present two different ways how it is possible to connect enumerative combinatorial numbers and polynomials to graph theory.

On the one hand, we can generalize them into the context of graph theory. For example, we introduce and study the Fubini number of a graph which counts the ordered independent partitions of its set of vertices, and the related Fubini polynomial.

On the other hand, we may try to find graph theoretic interpretation of well-known combinatorial numbers and polynomials. For example, we show such results about r-Stirling numbers of the second kind, r-Lah numbers, their summed variants and the related polynomials by counting matchings in certain bipartite graphs.

The talk is mainly based on the two papers below.

References

[1] Zs. Kereskényi-Balogh and G. Nyul, *Fubini numbers and polynomials of graphs*, Mediterranean Journal of Mathematics **18** (2021), Article 230.

[2] G. Nyul and G. Rácz, *Matchings in complete bipartite graphs and the r-Lah numbers*, Czechoslovak Mathematical Journal **71** (2021), 947–959.

Mayank Pandey

mp9979@math.princeton.edu, (Princeton University (USA))
Joint work with: Maksym Radziwiłł

On the L^1 norm of the exponential sum with the Liouville function

Take $\lambda(n)$ the Liouville function, the completely multiplicative function with $\lambda(p) = -1$. We show that

$$\int_0^1 \left| \sum_{n \leq X} \lambda(n) e(n\alpha) \right| d\alpha \gg X^{\delta},$$

for some $\delta > 0$. This improves on a previous lower bound of $\gg \exp(c \log X / \log\log X)$ by methods of Balog and Perelli. Along the way we prove a bound on the L^2 norm of the exponential sum restricted to major arcs of height a small power of X, which might be of independent interest.

Łukasz Pańkowski

lpan@amu.edu.pl, (Adam Mickiewicz University (Poland))
Joint work with: Akshaa Vatwani and Kamalakshya Mahatab

Joint extreme values of L-functions

We consider L-functions $L_1, \ldots, L_k$ from the Selberg class which have polynomial Euler product and satisfy Selberg's orthonormality condition. We show that on every vertical line $s = \sigma + it$ with $\sigma \in (1/2, 1)$, these L-functions simultaneously take large values of size $\exp\left(c \frac{(\log t)^{1-\sigma}}{\log\log t} \right)$ inside a small neighborhood. Our method extends to $\sigma = 1$ unconditionally, and to $\sigma = 1/2$ on the generalized Riemann hypothesis. We also obtain similar joint omega results for arguments of the given L-functions.

Ágoston Papp

papp.agoston@science.unideb.hu, (University of Debrecen (Hungary))
Joint work with: Lajos Hajdu

Uniform bounds for the number of powers in arithmetic progressions

We give sharp, in some sense uniform bounds for the number of ℓ-th powers and arbitrary powers among the first N terms of an arithmetic progression, for N large enough.

Paul Péringuey

paul.peringuey@univ-lorraine.fr, (Université de Lorraine (France))

A generalization of Artin's primitive root conjecture among almost primes

Artin's conjecture states that the set of primes for which an integer a different from -1 or a perfect square is a primitive root admits an asymptotic density among all primes. In 1967 C. Hooley [1] proved this conjecture under the Generalized Riemann Hypothesis.
The notion of primitive root can be extended modulo any integer by considering the elements of the multiplicative group generating subgroups of maximal size. One can then look for which elements of a set of integers a given integer is a generalized primitive root, as did S. Li and C. Pomerance for all the integers [2]. I will discuss the set of almost primes for which an integer a is a generalized primitive root, and prove, under GRH, results similar to Artin's conjecture for primitive roots.

References

[1] *C. Hooley*, On Artin's conjecture, J. Reine Angew. Math. 225, 209–220 (1967; Zbl 0221.10048)

[2] *S. Li* and *C. Pomerance*, On generalizing Artin's conjecture on primitive roots to composite moduli, J. Reine Angew. Math. 556, 205–224 (2003; Zbl 1022.11049)

Attila Pethő

petho.attila@unideb.hu, (University of Debrecen (Hungary))

Generalized radix representations and power integral bases

In the last century mainly through the work of Grünwald, Knuth, Penney, Gilbert, Kátai and his students Júlia Szabó, B. Kovács, Körmendi, Környei and A. Kovács evolved the notation of number systems or equivalently the radix representations in algebraic number fields. Using Győry's famous result on the finiteness of the number of non-equivalent bases of power integral bases in algebraic number fields, B. Kovács proved in 1981 that there are only finitely many essentially different radix representations in algebraic number fields. He was the first PhD student of Győry, who inaugurated in 1973. Several generalization appeared, concrete examples were computed and connections to discrete dynamical systems were discovered in the meantime. I will report on that efforts, which culminated in the work of Evertse, Győry, Thuswaldner and myself in 2019, where we dealt with radix representations in general orders.

István Pink

pinki@science.unideb.hu, (University of Debrecen (Hungary))
Joint work with: Takafumi Miyazaki

Number of solutions to a special type of unit equations in two unknowns

For any fixed coprime positive integers a, b and c with $\min\{a, b, c\} > 1$, we prove that the equation $a^x + b^y = c^z$ has at most two solutions in positive integers x, y and z, except for one specific case which exactly gives three solutions. Our result is essentially sharp in the sense that there are infinitely many examples allowing the equation to have two solutions in positive integers. From the viewpoint of a well-known generalization of Fermat's equation, it is also regarded as a 3-variable generalization of the celebrated theorem of Bennett [M.A.Bennett, On some exponential equations of S.S.Pillai, Canad. J. Math. 53(2001), no.2, 897–922] which asserts that Pillai's type equation $a^x - b^y = c$ has at most two solutions in positive integers x and y for any fixed positive integers a, b and c with $\min\{a, b\} > 1$. In this talk we give a brief summary of corresponding earlier results and present the main improvements leading to this definitive result.

Ákos Pintér

apinter@science.unideb.hu, (University of Debrecen (Hungary))

Győry $80 + \varepsilon$

In this talk some beautiful and memorable moments of the private life and professional career of an outstanding mathematician Kálmán Győry are presented.

Michael Pohst

pohst@math.tu-berlin.de, (TU Berlin (Germany))

On solving Mordell's equation

In 1997 K. Wildanger [5] presented a new approach for calculating all integral solutions of Mordell's equation $y^2 = x^3 + k$. He used methods from the geometry of numbers and obtained solutions for integers k with $|k| < 10^7$. Later we improved a few of his bounds which allowed solutions for $|k|$ up to 10^9. For larger $|k|$ we recently applied methods from H. Hasse [4] for the calculation of the number $N(d_F)$ of non-isomorphic cubic number fields F of given discriminant d_F via class field theory in [2]. This extended the range for $|k|$ up to about 10^{15}. For still larger $|k|$ the computation of class fields became too slow. We therefore chose different theoretical methods from Hasse's paper which needed to be made computationally feasible [3]. With those we could calculate $N(d_F)$ for d_F up to 10^{25} and beyond.

In the paper [1] the authors used a classical approach via forms for calculating all solutions for all k up to 10^7. This paper also contains a nice description of the results on Mordel's equation untl 2015.

References

[1] M. A. Bennett and A. Ghadermarzi, *Mordell's equation: a classical approach*, LMS J. Comput. Math. **18** (2015), 633–646.

[2] I. Gaál, M.C. Pohst, and M.E. Pohst, *On computing integral points of a Mordell curve – the method of Wildanger revisited*, Exp. Math. **30** (2021), 127–134.

[3] I. Gaál and M.E. Pohst, *On calculating the number $N(D)$ of global cubic fields F of given discriminant D* , J. Number Theory **236** (2022), 479–491.

[4] H. Hasse, *Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage*, Math. Z. **31** (1930), 565–582.

[5] K. Wildanger, *Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern mit einer Anwendung auf die Bestimmung aller ganzen Punkte einer Mordellschen Kurve*, Thesis, TU Berlin, 1997.

Carl Pomerance

carlp@math.dartmouth.edu, (Dartmouth College (United States of America))

Permutations and arithmetic

Consider the coprime graph on the integers, where two numbers are connected with an edge if they are coprime. In particular, when is there a matching in the bipartite coprime graph between two intervals of n consecutive integers? If the two intervals are both 1 to n, we're asking for a coprime permutation, and the natural question is how many of them are there? One can also ask about permutations of 1 to n with other arithmetic conditions imposed. There have been at least 4 papers posted to arXiv on these topics since last Fall, by Bohman and Peng, Sah and Sawhney, and myself. This talk will discuss some of these recent results and problems.

Stefan Porubský

sporubsky@hotmail.com, (The Czech Academy of Science (Czech Republic))
Joint work with: Ladislav Mišík and Oto Strauch

Uniform distribution of the weighted sum-of-digits functions

The talk is based on a joint paper [1] with L.Mišík (Ostrava) and O.Strauch (Bratislava).

Let $d \geq 1, q \geq 2$ be integers and

$$\Gamma = \begin{pmatrix} \gamma^{(1)} \\ \gamma^{(2)} \\ \vdots \\ \gamma^{(d)} \end{pmatrix} = \begin{pmatrix} \gamma_0^{(1)} & \gamma_1^{(1)} & \gamma_2^{(1)} & \cdots \\ \gamma_0^{(2)} & \gamma_1^{(2)} & \gamma_2^{(2)} & \cdots \\ \vdots & \vdots & \vdots & \ddots \\ \gamma_0^{(d)} & \gamma_1^{(d)} & \gamma_2^{(d)} & \cdots \end{pmatrix}$$

be a $d \times \infty$-matrix with real entries with $\vec{\gamma}_j = (\gamma_j^{(1)}, \gamma_j^{(2)}, \ldots, \gamma_j^{(d)})$ transposed in the jth column. If $n = \sum_{j=0}^{\infty} n_j^{(i)} q^j$ is the q-ary representation of $n \in \mathbb{N}_0$, define the

d-dimensional weighted sum-of-digits function by

$$s_{q,\Gamma}(n)=\big(s_{q,\gamma^{(1)}}(n),s_{q,\gamma^{(2)}}(n),\dots,s_{q,\gamma^{(d)}}(n)\big),$$

where $s_{q,\gamma^{(i)}}(n)=\langle\gamma^{(i)},n^{(i)}\rangle$, $i=1,2,\dots,d$.

In [2, Theorem 1] F. Pillichshammer proved the following theorem:

The sequence $s_{q,\Gamma}(n)$ is u.d. mod 1 if and only if for every integral vector $\vec{h}\in\mathbb{Z}^d\setminus\{\vec{0}\}$ one of the following conditions is fulfilled: either $\sum\limits_{k=0,\langle\vec{h},\vec{\gamma}_k\rangle q\notin\mathbb{Z}}^{\infty}\|\langle\vec{h},\vec{\gamma}_k\rangle\|^2=\infty$, or, there exists a non-negative integer k with $\langle\vec{h},\vec{\gamma}_k\rangle\notin\mathbb{Z}$ and $\langle\vec{h},\vec{\gamma}_k\rangle q\in\mathbb{Z}$.

We replace Pillichshammer's conditions with a single one involving a trigonometric product:

Let Γ be the $d\times\infty$-matrix of real weights defined above. Then the sequence $s_{q,\Gamma}(n)$, $n=0,1,2,\dots$, is u.d. mod 1 if and only if for every integral vector $\vec{h}\in\mathbb{Z}^d\setminus\{\vec{0}\}$ we have

$$\lim_{N\to\infty}\prod_{j=0,\langle\vec{h},\vec{\gamma}_j\rangle\notin\mathbb{Z}}^{N-1}\frac{\sin\pi\|q\langle\vec{h},\vec{\gamma}_j\rangle\|}{q\sin\pi\|\langle\vec{h},\vec{\gamma}_j\rangle\|}=0.$$

As applications of our condition we prove some upper estimates of the extreme discrepancies of such sequences, that the existence of distribution function $g(x)=x$ implies the uniform distribution modulo one of the weighted q-adic sum-of-digits function $s_{q,\gamma}(n)$, $n=0,1,2,\dots$, or the uniform distribution modulo one of related sequences $h_1s_{q,\gamma}(n)+h_2s_{q,\gamma}(n+1)$, where h_1 and h_2 are integers such that $h_1+h_2\neq0$, ...

References

[1] Mišík, L., Porubský, Š., Strauch, O.: Uniform distribution of the weighted sum-of-digits functions. Unif. Distrib. Theory 16 (2021), No. 1, 93-126.

[2] Pillichshammer, F.: Uniform distribution of sequences connected with the weighted sum-of-digits function, Unif. Distrib. Theory 2 (2007), no. 1, 1-10.

Gabriella Rácz

racz.gabriella@science.unideb.hu, (University of Debrecen (Hungary))

The r-Fubini–Lah numbers and polynomials

In our talk, we define new combinatorial numbers, the r-Fubini–Lah numbers. They count those partitions of a finite set, where both the blocks and the partition itself are ordered, and r distinguished elements belong to distinct ordered blocks. In connection with these numbers, we introduce the r-Fubini–Lah polynomials, as well.

We give a detailed overview of the properties of the r-Fubini–Lah numbers and polynomials. We prove two recurrences and a Dobiński type formula for them, we derive the exponential generating function of their sequences, and we show their connection with r-Fubini numbers and polynomials.

The results of this talk have been published in [1].

References

[1] G. Rácz, *The r-Fubini–Lah numbers and polynomials*, Australasian Journal of Combinatorics **78** (2020), 145–153.

Maciej Radziejewski

maciejr@amu.edu.pl, (Adam Mickiewicz University (Poland))
Joint work with: Jerzy Kaczorowski and Alberto Perelli

Forbidden conductors of L-functions and continued fractions of particular form

We show a connection between values of the conductor q of L-functions of degree 2 in the extended Selberg class and properties of certain continued fractions, parametrised by q, on which we define a positive-valued weight. We call a finite sequence of integers $\mathbf{m} = (m_0, \ldots, m_k)$ a loop if

$$c(q, \mathbf{m}) = m_k + \cfrac{1}{qm_{k-1} + \cfrac{q}{qm_{k-2} + \cfrac{q}{\ddots + \cfrac{q}{qm_0}}}}$$

equals 0. It turns out that loops have a group structure and weight, when restricted to loops, is a group homomorphism. If it is non-trivial, then q is not a conductor of any L function of degree 2. We show several results on classes of forbidden qs, and also qs that do occur as conductors of L function of degree 2.

Csaba Rakaczki
matrcs@uni-miskolc.hu, (University of Miskolc (Hungary))

Indecomposability of linear combinations of Bernoulli polynomials

Bernoulli polynomials are defined by the following generating function

$$\frac{te^{tx}}{e^t - 1} = \sum_{n=0}^{\infty} B_n(x)\frac{t^n}{n!}.$$

Bernoulli polynomials appear in several classical results of number theory and have important applications in classical analysis. For example, there is a close relationship between power sums and Bernoulli polynomials. Let k and n be positive integers, then

$$1^k + 2^k + \cdots + n^k = \frac{B_{k+1}(n+1) - B_{k+1}(0)}{k+1}.$$

A polynomial $h(x) \in \mathbb{C}[x]$ is said to be indecomposable over $\mathbb{C}$ if $h = f(g(x))$, $f(x), g(x) \in \mathbb{C}[x]$ implies that $\deg(f(x)) = 1$ or $\deg(g(x)) = 1$.
In our lecture we will talk about the following result:

Theorem 1. *Let $3 \leq n$ be an odd integer, a_n be an integer which is not divisible by 4, $a_{n-2}, a_{n-4}, \ldots, a_3, a_1$ be arbitrary integers. Then the polynomial*

$$P_n(x) = a_n B_n(x) + a_{n-2}B_{n-2}(x) + \cdots + a_3 B_3(x) + a_1 B_1(x)$$

is indecomposable over the field of complex numbers.

Szilárd Révész
revesz@renyi.hu, (Alfréd Rényi Institute of Mathematics (Hungary))

Achievements of János Pintz in the theory of primes

János Pintz' 70th anniversary is one of the dedications of this conference. The lecture attempts to give a necessarily concise overview of János' wide-ranging, fundamental achievements in the distribution of primes, discussing only a few of the lecturer's choice in some more detail. Given that the lecturer is an analyst at the first place, we will also comment some of the methods and constructions from an analysis point of view.

Szilárd Révész

revesz@renyi.hu, (Alfréd Rényi Institute of Mathematics (Hungary))

On the connection of the error term in the Prime Number Theorem and the location of zeroes of the Beurling zeta function

We investigate the classical question of Littlewood, originally posed for natural primes and the Riemann zeta function, and asking for explicit determination of the oscillation of the error in the PNT ”caused by a given zero”. In the context of the more general Beurling systems of primes and integers, we build up the necessary ingredients to determine the best possible upper and lower estimates for the error, given a zero of the Beurling zeta function. The surprising exact constant will be explained and sharpness will be proved using a recent refinement by Broucke and Vindas of the 2005 breakthrough method of Diamond, Montgomery and Vorhauer, devised for randomly ”constructing” Beurling primes with approximately having some pre-set distribution properties.

Joël Rivat

joel.rivat@univ-amu.fr, (Aix-Marseille University (France))

Pseudo-random properties of sums and products

Along 25 years of collaboration with András Sárközy, often together with Christian Mauduit, we will discuss the pseudo-random properties of sumsets, products and shifted products, prime numbers and other remarkable deterministic sequences.

Imre Z. Ruzsa

ruzsa@renyi.hu, (Alfréd Rényi Institute of Mathematics (Hungary))

Sumsets with multiplicative structure

Let Q be an infinite subset of primes, and let R be the set of positive integers not divisible by any element of Q. Can R be a sumset in a nontrivial way? We construct examples, answering a question of Győry, Hajdu and Sárközy. The sum of two squares is an almost-example; we meditate on the possibility to modify it into a real example.

Diana Savin
diana.savin@unitbv.ro, (Transilvania University of Brasov (Romania))
Joint work with: Vincenzo Acciaro, Mohammed Taous and Abdelkader Zekhnini

On quaternion algebras over certain extensions of quadratic number fields

We obtain a complete characterization of division quaternion algebras $H_K(p, q)$ over the composite K of n quadratic number fields, where p and q are positive prime integers. Let F be a quadratic number field. Also, we we obtain a complete characterization of division quaternion algebras $H_L(p, q)$, where L is an extension of F of degree l such that L is a dihedral extension of $\mathbb{Q}$, or else L is an abelian l-extension of F, unramified over F whenever l divides the class number of F.

References

[1] V. Acciaro, D. Savin, M. Taous and A. Zekhnini, *On quaternion algebras that split over specific quadratic number fields*, Italian J. Pure Appl. Math. N. 47, p. 91-107 (2022).

[2] V. Acciaro, D. Savin, M. Taous and A. Zekhnini, *On quaternion algebras over the composite of quadratic number fields* Glasnik Matematicki 56(1), p. 63-78 (2021).

[3] V. Acciaro, D. Savin, M. Taous and A. Zekhnini, *On quaternion algebras over some extensions of quadratic number fields*, Boletin de la Sociedad Matematica Mexicana, vol. 27, Issue 3, November 2021, p.1-7.

[4] M. Alsina, P. Bayer, *Quaternion Orders, Quadratic Forms and Shimura Curves*, CRM Monograph Series, 22. American Mathematical Society, Providence (2004).

[5] D. Savin, *About division quaternion algebras and division symbol algebras*, Carpathian Journal of Mathematics, vol. 32, No. 2 (2016), pp. 233-240.

[6] D. Savin, *About split quaternion algebras over quadratic fields and symbol algebras of degree n*, Bull. Math. Soc. Sci. Math. Roumanie, Tome 60 (108) No. 3 p. 307-312, (2017).

Csaba Sándor

csandor@math.bme.hu, (Budapest University of Technology and Economics (Hungary))

Additive representation functions and discrete convolutions

For a set A of non-negative integers, let $R_A(n)$ denote the number of solutions to the equation $n = a + a'$ with $a,\ a' \in A$. Denote by $\chi_A(n)$ the characteristic function of A. Let $b_n > 0$ be a sequence satisfying $\limsup_{n\to\infty} b_n < 1$. In this talk, we formulate some Erdős–Fuchs-type theorems about the error terms appearing in approximation formulæ for $R_A(n) = \sum_{k=0}^{n} \chi_A(k)\chi_A(n-k)$ and $\sum_{n=0}^{N} R_A(n)$ having principal terms $\sum_{k=0}^{n} b_k b_{n-k}$ and $\sum_{n=0}^{N}\sum_{k=0}^{n} b_k b_{n-k}$, respectively.

Andrew Scoones

andrew.scoones@york.ac.uk, (University of York (United Kingdom))

On the *abc* conjecture in algebraic number fields

While the *abc* conjecture remains open, much work has been done on weaker versions, and on generalising the conjecture to number fields. Stewart and Yu were able to give an exponential bound for $\max\{a,\ b,\ c\}$ in terms of the radical over the integers [3],[4], while Győry was able to give an exponential bound for the projective height $H\,(a,\ b,\ c)$ in terms of the radical for algebraic integers [1]. We generalise Stewart and Yu's method to give an improvement on Győry's bound for algebraic integers, before briefly discussing applications to the effective Skolem-Mahler-Lech problem and the XYZ conjecture [2]. We note that independently Győry attained similar results which we will also discuss.

References

[1] K. Győry. On the *abc* conjecture in algebraic number fields. *Acta Arithmetica*, 133:281–295, 2008.

[2] A. Scoones. On the *abc* conjecture in algebraic number fields. *arXiv preprint*, arXiv:2111.07791, 2021

[3] C. L. Stewart and K. Yu. On the abc conjecture. *Mathematische Annalen*, 291:225–230, 1991.

[4] C. L. Stewart and K. Yu. On the abc conjecture, II. *Duke Mathematical Journal*, 108(1):169–181, 2001.

Péter Sebestyén

sebestyen.peter@science.unideb.hu, (University of Debrecen (Hungary))
Joint work with: Lajos Hajdu

Terms of recurrence sequences in the solution sets of generalized Pell equations

In this presentation we completely describe those recurrence sequences which have infinitely many terms in the solution sets of generalized Pell equations. Further, we give an upper bound for the number of such terms when there are only finitely many of them.

Igor Shpralinski

igor.shparlinski@unsw.edu.au, (University of New South Wales (Australia))

Bilinear forms with Kloosterman and Salie Sums and Moments of L-functions

We present some recent results on bilinear forms with complete and incomplete Kloosterman and Salie sums. These results are of independent interest and also play a major role in bounding error terms in asymptotic formulas for moments of various L-functions. We then describe several results about non-correlation of Kloosterman and Salie sums between themselves and also with some classical number-theoretic functions such as the Mobius function, the divisor function and the sum of binary digits, etc. Some open problems will be outlined as well.

Bartosz Sobolewski

bartosz.sobolewski@uj.edu.pl, (Jagiellonian University (Poland))

Monochromatic arithmetic progressions in binary words associated with pattern sequences

Let $e_v(n)$ denote the number of occurrences of a pattern v in the binary expansion of $n \in \mathbb{N}$. In the talk we consider monochromatic arithmetic progressions in the class of words $(e_v(n) \bmod 2)_{n \geq 0}$ over $\{0, 1\}$, which includes the Thue–Morse word $\mathbf{t}$ (for $v = 1$) and a variant of the Rudin–Shapiro word $\mathbf{r}$ (for $v = 11$). So far, the problem of exhibiting long progressions and finding an upper bound on their length has mostly been studied for $\mathbf{t}$ and certain generalizations [1, 2, 3]. The main goal of the talk is to show analogous results for $\mathbf{r}$ and some weaker results for a general pattern v. In particular, we prove that a monochromatic arithmetic progression of difference $d \geq 3$ starting at 0 in $\mathbf{r}$ has length at most $(d+3)/2$, with equality infinitely often. We also compute the maximal length of monochromatic progressions of differences $2^k - 1$ and $2^k + 1$.

References

[1] I. Aedo, U. Grimm, Y. Nagai, P. Staynova, *On long arithmetic progressions in binary Morse-like words*, preprint, `https://arxiv.org/abs/2101.02056` (2021), 23 pp.

[2] J. F. Morgenbesser, J. Shallit, T. Stoll, *Thue–Morse at multiples of an integer*, J. Number Theory **131** (2011), no. 8, 1498–1512.

[3] O. G. Parshina, *On arithmetic index in the generalized Thue–Morse word*, in: S. Brlek, F. Dolce, C. Reutenauer, É. Vandomme (eds.), Combinatorics on Words, Springer, Cham, 2017, 121–131

Jozsef Solymosi

solymosi@math.ubc.ca, (University of British Columbia (Canada))
Joint work with: Noga Alon

Rank of matrices with entries from a multiplicative group

We establish lower bounds on the rank of matrices in which all but the diagonal entries lie in a multiplicative group of small rank. Applying these bounds we show that the distance sets of finite pointsets in R^d generate high rank multiplicative groups and that multiplicative groups of small rank cannot contain large sumsets.

Gökhan Soydan

gsoydan@uludag.edu.tr, (Bursa Uludag University (Turkey))
Joint work with: Elif Kızıldere Mutlu and Maohua Le

The elementary and modular approaches to the generalized Ramanujan-Nagell equation

Let d, k be fixed coprime positive integers with $\min\{d, k\} > 1$. A class of polynomial-exponential Diophantine equations of the form

$$x^2 + d^y = k^z, \ x, y, z \in \mathbb{Z}^+ \tag{1}$$

is usually called the generalized Ramanujan-Nagell equation. It has a long history and rich content (see [3]). In 2014, N. Terai [6] discussed the solution of (1) in the case $d = 2k - 1$. He conjectured that for any k with $k > 1$, the equation

$$x^2 + (2k-1)^y = k^z, \ x, y, z \in \mathbb{Z}^+ \tag{2}$$

has only one solution $(x, y, z) = (k - 1, 1, 2)$. The above conjecture has been verified in some special cases (see [1], [2] and [6]). In this work, firstly, using the modular approach, we prove that if $k \equiv 0 \pmod 4$, $30 < k < 724$ and $2k - 1$ is an odd prime power, then under the GRH, the equation (2) has only one positive integer solution $(x, y, z) = (k-1, 1, 2)$. The above results solve some difficult cases of Terai's conecture concerning the equation (2). Secondly, using various elementary methods in number theory, we give certain criterions which can make the equation (2) to have no positive integer solutions (x, y, z) with $y \in \{3, 5\}$. These results make up the defiency of the modular approach when applied to (2). This talk consists of the results in [4] and [5]. This work was supported by the Research Fund of Bursa Uludağ University under Project No: F-2020/8.

References

[1] M. Bennett and N. Billerey, Sums of two S-units via Frey-Hellegouarch curves, *Math. Comp.* **305** (2017), 1375–1401.

[2] M.-J. Deng, J. Guo and A.-J. Xu, A note on the Diophantine equation $x^2 + (2c-1)^m = c^n$, *Bull. Aust. Math. Soc.* **98** (2018), 188–195.

[3] M. H. Le and G. Soydan, A brief survey on the generalized Lebesgue-Ramanujan-Nagell equation, *Surv. Math. Appl.* **15** (2020), 473–523.

[4] E. K. Mutlu, M. H. Le and G. Soydan, A modular approach to the generalized Lebesgue-Ramanujan-Nagell equation, to appear in Indagationes Mathematicae (2022), https://doi.org/10.1016/j.indag.2022.04.005

[5] E. K. Mutlu, M. H. Le and G. Soydan, An elementary approach to the generalized Lebesgue-Ramanujan-Nagell equation, submitted (2022).

[6] N. Terai, A note on the Diophantine equation $x^2 + q^m = c^n$, *Bull. Aust. Math. Soc.* **90** (2014), 20–27.

Cameron Stewart

cstewart@uwaterloo.ca, (University of Waterloo (Canada))

Laudatio for Professor András Sárközy

In this talk we shall discuss some of the results obtained by Professor András Sárközy over his distinguished career and the influence they have had in combinatorial and analytic number theory. In addition we shall include some personal reminiscences.

Myroslav Stoika

sztojka.miroszlav@kmf.org.ua, (Ferenc Rákóczi II Transcarpathian Hungarian College of Higher Education (Ukraine))

On wild p-groups over local factorial rings

The problem of describing the tame and wild finite groups G over a field R is completely solved in [1]. For a ring R, this problem is completely solved in the cases when R is a ring of p-adic numbers or a complete discrete valuation ring or a ring of formal power series with P-adic coeficients (see [1]–[6]). In many other cases the problem is solved when there are constraints on groups or rings. We consider the case when G is a 2-group and R is local factorial rings of characteristic 0.

References

[1] V. M. Bondarenko, Ju. A. Drozd. The representation type of finite groups Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI), 1977, 71, P. 24-41 (in Russian).

[2] P. M. Gudivok. Modular and integral representations of finite groups Dokl. Akad. Nauk SSSR 1974, 214, P. 993-996 (in Russian).

[3] P. M. Gudivok. Representations of finite groups over a complete discrete valuation ring Trudy Mat. Inst. Steklov, 1978, 148, P. 96-105 (in Russian).

[4] E. Dieterich. Group rings of wild representation type Math. Annn., 1983, 266, N1, P. 1-22.

[5] P. M. Gudivok, V. M. Oros, A. V. Roiter. Representations of finite p-groups over a ring of formal power series with integer p-adic coeficients Ukrain. Mat. Zh., 1992, 44, N6, P. 753-765 (in Russian).

[6] V. M. Bondarenko, P. M. Gudivok. Representations of finite p-groups over a ring of formal power series with integer p-adic coeficients Infinite groups and related algebraic structures, Akad. Nauk Ukrainy, Inst. Mat., Kiev, 1993, P. 514 (in Russian).

Cathy Swaenepoel

cathy.swaenepoel@imj-prg.fr, (Université Paris Cité (France))

Integers with preassigned digits

For an ”interesting” set $\mathcal{S}$ of non negative integers, we will discuss some properties of the integers in $\mathcal{S}$ with preassigned digits.

László Szalay

szalay.laszlo@uni-sopron.hu, (University of Sopron (Hungary) and University J. Selye (Slovakia))

Properties of Motzkin triangle

The Motzkin triangle is established as the zero-free part of a well-defined plane array. The right leg of the triangle is the Motzkin sequence itself, it satisfies a second order linear recurrence relation with linear polynomial coefficients.

We extend this relation in the triangle by proving the existence of a recursive formula for the formation of three arbitrary elements, and construct the corresponding formulae for three connected entries. These recursive formulae have bivariate polynomial coefficients of higher order. The construction method is able to create recurrence rules for other structures.

Márton Szikszai

szikszai.marton@science.unideb.hu, (University of Debrecen (Hungary))

On Higher Power Rational Diophantine Tuples

Let $k \geq 2$. A set of nonzero rationals $\{a_1, a_2, \ldots, a_n\}$ is called a kth-power rational Diophantine n-tuple if for every $1 \leq i < j \leq n$ there exist rationals r_{ij} such that $a_i a_j + 1 = r_{ij}^k$. The case $k = 2$ is classical and studied extensively, giving rise to various generalizations. Surprisingly, one of the most natural of these, namely, letting the exponent to vary, is yet to see serious attention and besides the case of rational integers, it have not seen much attention.

In this talk, we give a very general discussion on the topic of powers different than squares and present a few new results based on analogues of known techniques. We show how simple numeric experimentation reveals the existence of multiple parametric families of triples for any exponent and then attempt to build quadruples out of these. The concept of curves induced by Diophantine pairs is also introduced and we make simple observations about these objects. The usefulness of this more general framework for the special case $k = 2$ is explored very briefly, exposing some blockers and limitations of the ideas.

The talk serves as both a standalone and a prelude to the contributed talk of Gergő Batta under the title "On 3rd Power Rational Diophantine Triples and Quadruples".

Robert F. Tichy

tichy@tugraz.at, (Graz University of Technology (Austria))

Diophantine problems, polynomials and linear recurrences

Starting point is the well-known Pillai's problem which is concerned with the diophantine equation $a^x - b^y = c$. For $c = 1$ this is the famous Catalan equation and since 2004 it is known from Mihailescu's work that $3^2 - 2^3 = 1$ is the only solution in positive integers to this equation. For general c a Pillai's problem is widely open, however many partial results are known. We will report on some special cases and we will extend the problem to linear recurrences, i.e. we replace the powers a^x and b^y by linear reccurrences U_x and V_y (with integer coefficients) satisfying some dominate root condition. We focus on specific sequences such as Fibonacci numbers and their generalizations. It is known that differences $U_x - V_y$ can attain only two different values with the exception of finitely many cases (which can be completely described for certain sequences). Furthermore, a quantitative density version of Pillai's problem is considered and an asymptotic formula for the number of (x, y) sucht that $|U_x - V_y|$ does not exceed T (tending to infinity) is proved. Finally, some connections to diophantine approximation problems and polynomials along prime numbers are discussed.

Robert Tijdeman

tijdeman@math.leidenuniv.nl, (Leiden University (The Netherlands))
Joint work with: Lajos Hajdu

The Diophantine equation $f(x) = g(y)$ for polynomials f, g where f has simple rational roots

We consider the Diophantine equation $f(x) = g(y)$ where both polynomials f and g have rational coefficients and f has simple rational roots. We give conditions for the cases that the equation has infinitely many rational solutions with a bounded denominator and provide examples to illustrate that the conditions are necessary. We show a close connection with the Prouhet-Tarry-Escott problem. Our main tool is the Bilu-Tichy theorem.

Magdaléna Tinková

tinkova.magdalena@gmail.com, (Czech Technical University in Prague (Czech Republic))

Trace and norm of indecomposable integers in cubic orders

Additively indecomposable integers in totally real number fields are a useful tool for the study of quadratic forms over these fields. Except for a few results, we do not know much about them. So far, their structure was fully determined only in the case of real quadratic fields [8, 3] and monogenic simplest cubic fields [5], and we have some partial results for real biquadratic fields [2, 7]. Moreover, the norm of indecomposable integers in these fields is bounded [1], and we can use the discriminant of the field as this bound [6]. However, this bound is often not sharp, and so far, it was improved in the case of quadratic fields [3, 4, 9]. In this talk, we will show similar results for several families of cubic fields. Furthermore, we will also study the minimal trace of indecomposable integers after multiplying by elements of the codifferent.

References

[1] H. Brunotte, *Zur Zerlegung totalpositiver Zahlen in Ordnungen totalreeller algebraischer Zahlkörper*, Arch. Math. (Basel) 41(6), 502–503 (1983).

[2] M. Čech, D. Lachman, J. Svoboda, M. Tinková and K. Zemková, *Universal quadratic forms and indecomposables over biquadratic fields*, Math. Nachr. 292, 540–555 (2019).

[3] A. Dress and R. Scharlau, *Indecomposable totally positive numbers in real quadratic orders*, J. Number Theory 14, 292–306 (1982).

[4] S. W. Jang and B. M. Kim, *A refinement of the Dress-Scharlau theorem*, J. Number Theory 158, 234–243 (2016).

[5] V. Kala and M. Tinková, *Universal quadratic forms, small norms and traces in families of number fields*, in Int. Math. Res. Not. IMRN, to appear.

[6] V. Kala and P. Yatsyna, *On Kitaoka's conjecture and lifting problem for universal quadratic forms*, preprint.

[7] J. Krásenský, M. Tinková and K. Zemková, *There are no universal ternary quadratic forms over biquadratic fields*, Proc. Edinb. Math. Soc. 63 (3), 861-912 (2020).

[8] O. Perron, *Die Lehre von den Kettenbrüchen*, B. G. Teubner, 1913.

[9] M. Tinková and P. Voutier, *Indecomposable integers in real quadratic fields*, J. Number Theory 212, 458–482 (2020).

Árpád Tóth

toth.artano@gmail.com, (Eötvös Loránd University (Hungary))
Joint work with: Márton Erdélyi

Matrix Kloosterman sums

I will talk about a family of exponential sums that arises in the study of the horocyclic flow on the general liner group. This sum is a natural generalization of the classical Kloosterman sum, and share a number of similar properties. I will talk about optimal bounds in this family, giving an explicit version of the "generic purity" phenomenon of

Fouvry-Katz.

László Tóth
ltoth@gamma.ttk.pte.hu, (University of Pécs (Hungary))
Joint work with: Olivier Bordellès

Additive arithmetic functions meet the inclusion-exclusion principle: Asymptotic formulas concerning the GCD and LCM of several integers

We obtain asymptotic formulas for the sums

$$\sum_{n_1,\ldots,n_k \le x} f((n_1,\ldots,n_k))$$

and

$$\sum_{n_1,\ldots,n_k \le x} f([n_1,\ldots,n_k]),$$

involving the GCD and LCM of the integers $n_1,\ldots,n_k$, where f belongs to certain classes of additive arithmetic functions. In particular, we consider the generalized omega function $\Omega_\ell(n) = \sum_{p^\nu || n} \nu^\ell$ investigated by Duncan [2] and Hassani [3], and the functions $A(n) = \sum_{p^\nu || n} \nu p$, $A^*(n) = \sum_{p|n} p$, $B(n) = A(n) - A^*(n)$ studied by Alladi and Erdős [1]. As a key auxiliary result we use an inclusion-exclusion-type identity. For example, we prove that for any fixed integers $k \ge 2$ and $\ell \ge 0$,

$$\frac{1}{x^k} \sum_{n_1,\ldots,n_k \le x} \Omega_\ell([n_1,\ldots,n_k]) = k \log\log x + c + \sum_{j=1}^{N} \frac{a_j}{(\log x)^j} + O\left(\frac{1}{(\log x)^{N+1}}\right),$$

for every $N \ge 1$, where c and a_j $(1 \le j \le N)$ are certain explicit constants.

References

[1] K. Alladi and P. Erdős, On an additive arithmetic function, *Pacific J. Math.* **71** (1977), 275–294.

[2] R. L. Duncan, A class of additive arithmetical functions, *Amer. Math. Monthly* **69** (1962), 34–36.

[3] M. Hassani, Asymptotic expansions for the average of the generalized omega function, *Integers* **18** (2018), Paper No. A23, 12 pp.

Maciej Ulas

maciej.ulas@gmail.com, (Jagiellonian University (Poland))
Joint work with: Bartosz Sobolewski

Values of binary partition function as sums of three squares

Let $b(n)$ counts the number of binary partitions of non-negative integer n, i.e.,

$$b(n) = \#\{(k_1, \ldots, k_m) : \; n = \sum_{i=1}^{m} 2^{k_i}, \; m \in \mathbb{N}_+, k_1 \leq k_2 \leq \ldots \leq k_m\}.$$

We characterize those values of $n \in \mathbb{N}$ such that $b(n)$ can be written as a sum of three squares of integers. The characterization is given in terms of certain regular sequences related to the Prouhet-Thue-Morse sequence. As an application, we prove that

$$\lim_{N \to +\infty} \frac{\#\{n : \; b(n) \text{ is a sum of three squares}\} \cap [0, N]}{N} = \frac{5}{6}.$$

Nóra Varga

nvarga@science.unideb.hu, (University of Debrecen (Hungary))
Joint work with: Lajos Hajdu

Diophantine equations for polynomials with restricted coefficients - power values

In this talk we study of Diophantine equations involving polynomials with restricted coefficients. As a generalization of Littlewood polynomials, we shall consider polynomials whose coefficients are composed of primes coming from a fixed finite set. We shall be interested in perfect power values of such polynomials - that is, in Schinzel-Tijdeman equations and hyper- and superelliptic equations related to them. We shall provide effective upper bounds for the solutions of such equations. For this, we need to combine the effective theory of such equations and the theory of S-unit equations with new assertions concerning the root structures of such polynomials.

Ingrid Vukusic

ingrid.vukusic@stud.sbg.ac.at, (University of Salzburg (Austria))
Joint work with: Volker Ziegler

On a family of unit equations over simplest cubic fields

Let $a \in \mathbb{Z}$ and ρ be a root of $f_a(x) = x^3 - ax^2 - (a+3)x - 1$, then the number field $K_a = \mathbb{Q}(\rho)$ is called a simplest cubic field [1]. In this talk we consider the family of unit equations $u_1 + u_2 = n$ where $u_1, u_2 \in \mathbb{Z}[\rho]^*$ and $n \in \mathbb{Z}$. We completely solve the unit equations under the restriction $|n| \leq \max\{1, |a|^{1/3}\}$.

References

[1] D. Shanks. The simplest cubic fields. *Math. Comp.*, 28:1137–1152, 1974. DOI:10.2307/2005372.

Gary Walsh

gwalsh@uottawa.ca, (University of Ottawa (Canada))

An application of Runge's theorem and Baker's theorem to an effective version of a theorem of Shioda on ranks of elliptic curves

In this talk we will discuss a theorem which extends a number of results in the literature. In particular, we show effectively that for m sufficiently large, an elliptic curve given by $y^2 = f(x) + m^2$, with $f(x)$ a cubic polynomial that splits over $\mathbb{Z}$, has rank at least 2. This result can also be regarded as an effective version of a theorem of Shioda.

Arne Winterhof

arne.winterhof@oeaw.ac.at, (RICAM, Austrian Academy of Sciences (Austria))

Pseudorandom binary sequences: Quality measures and constructions

In their ground-breaking paper [1], Mauduit and Sárközy introduced several measures of pseudorandomness for binary sequences including the *correlation measure of order* k. They also showed that the *Legendre sequence* behaves essentially like a random sequence with respect to these measures. This paper started an important and very successful area of research and has been cited about 200 times.

Besides the correlation measure of order k there are several measures of pseudorandomness which can be used to sieve sequences with undesirable non-random structure including

- *linear complexity*,
- *maximum-order complexity*,
- and *expansion complexity*.

These measures are partly not independent and partly complete each other. First we study their relations. It turns out that the correlation measure of order k is on the top of the hierarchy of pseudorandom measures.

Then we analyze these measures for some sequences including the Legendre sequence, the *Thue-Morse sequence* and the *subsequence of the Thue-Morse sequence along squares*.

For a recent survey on this topic see [2].

References

[1] C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences. I. Measure of pseudorandomness, the Legendre symbol. Acta Arith. 82 (1997), no. 4, 365–377.

[2] L. Mérai, A. Winterhof, Pseudorandom sequences derived from automatic sequences, Cryptogr. Commun., to appear, `https://arxiv.org/abs/2105.03086`.

Yangbo Ye

yangbo-ye@uiowa.edu, (University of Iowa (USA))

Bounds toward Hypothesis S for cusp forms

Iwaniec, Luo, and Sarnak proposed Hypothesis S and its generalization which predicts non-trivial bounds for a smooth sum of the product of an arithmetic sequence $\{a_n\}$ and a fractional exponential function. When a_n is the Fourier coefficient $\lambda_f(n)$ of a fixed holomorphic cusp form f, however, a resonance phenomenon prohibits any improvement of the bound beyond a barrier. It is believed that this resonance barrier could be overcome when the weight k of f tends to infinity. The present paper is a first step toward this goal by proving non-trivial bounds for this sum when k and the summation length X both tend to infinity. No such non-trivial bounds are previously known if the form f is allowed to move. Similar bounds are also proved for linear phases and for Maass forms. The main technology is improved large sieve inequalities over a short interval.

References

[1] https://doi.org/10.1016/j.jnt.2021.07.012 Yangbo Ye, Bounds toward Hypothesis S for cusp forms, *J. Number Theory*, **236** (2022), 128-143.

Cem Yalçın Yıldırım

cyalciny@gmail.com, (Boğaziçi University (Turkey))

Some analogues of pair correlation of zeta zeros

In 1972 H. L. Montgomery introduced the study of the pair correlation of zeros of the Riemann zeta-function $\zeta(s)$ and thereby opened a new direction for studying this function and the relations to the distribution of primes. His main motivation arose from a problem concerning the class numbers of imaginary quadratic fields. Montgomery's work, assuming the Riemann Hypothesis, not only gave results about the simplicity and distribution of the zeta zeros on the critical line, but also revealed connections to random matrix theory and was interpreted by Montgomery as being in accordance with the view (which legend dates back to Hilbert and Pólya) that there is a yet undiscovered linear operator whose eigenvalues characterize the zeros of $\zeta(s)$.

In our study we first present an alternative way to develop Montgomery's argument. This alternative method has the advantage that it can also be applied in other instances for which we provide some examples (parts of it done jointly with my former doctoral student Yunus Karabulut), viz. the correlation of zeta zeros with maxima points of $\zeta(s)$ on the critical line, the pair correlation of these maxima, and the correlation of zeros of one Dirichlet L-function with those of another Dirichlet L-function, and some observations about correlations of zeta zeros with the zeros of $\zeta'(s)$.

In my talk first I will describe Montgomery's work and its impacts on some subjects such as the theory of the Riemann zeta-function including relations with random matrix theory and the distribution of primes. Then I will recount those analogues of pair correlation of zeta zeros that we have worked out.

Volker Ziegler

volker.ziegler@plus.ac.at, (University of Salzburg (Austria))

On a variant of Pillai's problem with binary recurrences and S-units

Let $U = (U_n)_{n\in\mathbb{N}}$ be a fixed binary recurrence with real characteristic roots α, β satisfying $|\alpha| > |\beta|$ and let $p_1, \ldots, p_s$ be fixed distinct prime numbers. In this paper we show that there exist effective computable constants $C^+ \geq 0$ and $C^- \geq 0$ such that the equation

$$U_n - p_1^{x_1} \cdots p_s^{x_s} = c$$

has at most s solutions $(n, x_1, \ldots, x_s)$ if $c > C^+$ and at most $s+1$ solutions $(n, x_1, \ldots, x_s)$ if $c < -C^-$.

Mikuláš Zindulka

mikulas.zindulka@matfyz.cuni.cz, (Charles University (Czech Republic))

Number of elements of small norm in the simplest cubic fields

We work in a family of the **simplest cubic fields** K_a parametrized by one integer parameter a. Our goal is to estimate the number of integral elements (up to conjugation and multiplication by units) whose norm is below a certain bound X. We provide an asymptotic estimate depending on a and X up to a multiplicative constant which is independent of the two parameters.

The study of elements of small norm was initiated in a paper by Lemmermeyer and Pethő [1] who showed that the norm of any non-unit integral element of K_a is at least $2a + 3$ and that the minimum is attained. The result was further extended by Kala and Tinková [2], who gave an estimate for the number of elements with norm $\leq a^2$. The count is much larger than predicted by the **class number formula**.

We give a natural explanation of this discrepancy and show that if $X \geq a^4$, then the number of elements agrees with the heuristics coming from the class number formula.

References

[1] F. Lemmermeyer, A. Pethő, *Simplest Cubic Fields*, Manuscripta Math. 88 (1995), 53–58.

[2] V. Kala, M. Tinková, *Universal Quadratic Forms, Small Norms, and Traces in Families of Number Fields*, Int. Math. Res. (2022).