Contents

General information

Welcome

Welcome to the 29th Journées Arithmétiques held for the first time in Hungary. We hope that you will enjoy the mathematical experience and social programmes of our conference, as well as Hungary's touristical opportunities.

JA2015 Registration and Hospitality Desks

The Registration and Hospitality Desks of the Conference will be open in the following periods and places:

- Sunday, 5th July 10:00-22:00 in the lobby of the Lajos Kossuth Dormitory I
- In the lobby of the Life Science Building, next to the room F015-016
  - Monday, 6th July: 08:30 – 13:00
  - Tuesday, 7th July: 08:30 – 12:00
  - Wednesday, 8th July: 08:30 – 12:00
  - Thursday, 9th July: 08:30 – 13:00
  - Friday, 10th July: 08:30 – 12:00
- On the 3rd floor of the Main Building
  - Monday, 6th July: 13:30 – 18:30
  - Tuesday, 7th July: 13:30 – 18:30
  - Thursday, 9th July: 13:30 – 18:30

Conference rooms

The Scientific programme of the Conference will be held in the following rooms:

- Plenary lectures as well as the Public Lecture will be held in
  - M – Main Lecture Hall – Life Science Building, Lecture Hall F015-016
- The Contributed Talks will be held in:
  - A – Main Building, Lecture Hall I.
  - B – Main Building, Lecture Hall II.
  - C – Main Building, Lecture Hall III.
  - D – Main Building, Lecture Hall IX.
  - E – Main Building, Lecture Hall X.
  - F – Main Building, Lecture Hall XI.
  - G – Main Building, Lecture Hall XII.

Computer facilities

Wireless Internet access will be available all over the buildings of the Main Campus of the University of Debrecen, except the dormitory. The name of the network and the password will be provided with the printed version of the abstract book. In the dormitory wired internet will be available. The UTP connecting cable, username and password will be provided by the dormitory staff.

Lunch

Lunches will be in the Large (Student) Hall of the Canteen. The pre-purchased tickets are inserted in the envelope you get at registration.

Coffee breaks

The morning coffee breaks will be held in the Life Science Building, next to the Main Lecture Hall F015-016.
The afternoon coffee breaks will be held on the 3rd floor of the Main Building.

Public lecture

László LOVÁSZ
Limit structures in graph theory and number theory
Tuesday, 18:40-19:40, Main Lecture Hall, Life Science Building F015-016

The Public Lecture of the 29th Journées Arithmétiques will be given by Professor László LOVÁSZ, the president of the Hungarian Academy of Sciences, former president of the International Mathematical Union, who was awarded among others the Wolf Prize, the Knuth Prize and the Kyoto Prize.

Special issue of the Journal de Théorie des Nombres de Bordeaux

The Journal de Théorie des Nombres de Bordeaux has accepted to publish a special issue of the JA2015 in Debrecen. Manuscripts have to be sent directly to the Journal through the web-page

http://www.emis.de/journals/JTNB/jtnbsubmit_english.html

Submissions has to be done not later than December 31st, 2015. They will be refereed according to the standard rules of the Journal.

Social programme

Welcome Party

On Monday at 20:00 every participant is invited for a Welcome Reception.

Tours

The day of tours is Wednesday, 8th July. The tours will start at 13:30. The buses will wait for the participants in the parking lot next to the Dormitory and (behind) the Canteen.

Conference dinner

Venue: Main Building, Inner Courtyard.
Date: Thursday, 9th of June, 20:00
Conference dinner fee – 50 Euro

Thanks

We would like to thank our sponsors for their kind support. Our sponsors are:

- University of Debrecen
- Student Council of the University of Debrecen
- Compositio Foundation
- Number Theory Foundation
- Hungarian Academy of Sciences
- Section of Mathematics of the Hungarian Academy of Sciences
- Journal de Théorie des Nombres de Bordeaux

Programme

Summary

Programme	**Monday**	**Tuesday**	**Wednesday**	**Thursday**	**Friday**
Morning session	10:00-11:10	9:00-10:00	9:00-10:00	9:00-10:00	9:00-10:00
Coffee break	11:10-11:40	10:00-10:30	10:00-10:30	10:00-10:30	10:00-10:30
Morning session	11:40-12:40	10:30-11:30	10:30-11:30	10:30-12:40	10:30-11:30
Lunch	12:40-14:00	11:30-13:00	11:30-13:00	12:40-14:00	11:30-13:00
Excursions			13:30-		
Afternon session	14:00-15:50	14:00-15:50		14:00-15:50	
Coffee break	15:50-16:20	15:50-16:20		15:50-16:20	
Afternoon session	16:20-18:10	16:20-18:10		16:20-18:10	
Public lecture		18:40-19:40			
Conference dinner				20:00-23:00	
Welcome reception	20:00-22:00				

Monday - Morning session, F015-016

Time	**Speaker**	**Title of the talk**
10:00-10:10		Opening
10:10-11:10	Jan-Hendrik Evertse	Results and open problems related to the Subspace Theorem.
11:10-11:40	*Coffee Break*	
11:40-12:40	Jack Thorne	Modularity of elliptic curves
12:40-14:00	*Lunch*	

Monday - Afternoon session A, Lecture Hall I.

Time	Speaker	Title of the talk
14:00-14:20	Maxim Aleksandrovich Korolev	On the primitive of Hardy's function
14:30-14:50	Jan Büthe	Applications of partial knowledge of the Riemann Hypothesis
15:00-15:20	Paul Young	Bernoulli polynomial convolutions and p-adic Arakawa-Kaneko zeta functions
15:30-15:50	Ayhan Dil	Geometric polynomials: properties and applications to series with zeta values
15:50-16:20	*Coffee Break*	
16:20-16:40	Aleksandar Ivič	Some mean value results for the zeta-function and a divisor problem
16:50-17:10	Kohji Matsumoto	The mixed joint universality for a class of zeta-functions
17:20-17:40	Anders Södergren	Universality of the Epstein zeta function

Monday - Afternoon session B, Lecture Hall II.

Time	Speaker	Title of the talk
14:00-14:20	Sergei Vladimirovich Konyagin	On sum sets of sets having small product set
14:30-14:50	David Joseph Grynkiewicz	A weighted zero-sum problem with quadratic residues
15:00-15:20	Jack Sonn	Quadratic residues and difference sets mod p
15:30-15:50	Thai Hoang Le	Additive bases in groups
15:50-16:20	*Coffee Break*	
16:20-16:40	József Solymosi	Problems in additive combinatorics
16:50-17:10	Sándor Kiss	On the quantitative version of the Erdős-Turán conjecture about the additive representation functions
17:20-17:40	Peter Vincent Hegarty	Permutations destroying arithmetic progressions in finite cyclic groups
17:50-18:10	Artem Uvakin	About two-dimensional sumsets and difference sets

Monday - Afternoon session C, Lecture Hall III.

Time	Speaker	Title of the talk
14:00-14:20	Takao Komatsu	Some explicit formulas of Bernoulli and Cauchy polynomials in terms of Stirling numbers
14:30-14:50	Nazli Yildiz Ikikardes	Certain combinatoric convolution sums arising from Bernoulli and Euler polynomials

15:00-15:20	Yilmaz Simsek	A note on Stirling type numbers and Array type polynomials
15:30-15:50	István Mező	The mode of the Jacobi-Stirling numbers
15:50-16:20	*Coffee Break*	
16:20-16:40	Piotr Miska	Arithmetic properties of the sequence of derangements
16:50-17:10	Gábor Nyul	Monochromatic linear recurrence sequences
17:20-17:40	Eszter Gyimesi	On properties of the r-Dowling polynomials
17:50-18:10	Gabriella Rácz	Recent results on r-Lah polynomials

Monday - Afternoon session D, Lecture Hall IX.

Time	**Speaker**	**Title of the talk**
14:00-14:20	Dong Sung Yoon	Siegel invariants and its applications
14:30-14:50	Giovanni Coppola	Arithmetic bands and weighted Selberg integrals
15:00-15:20	Yumiko Hironaka	Harmonic analysis on the space of p-adic unitary hermitian matrices
15:30-15:50	Yoshinori Hamahata	The transformations of a series in function fields
15:50-16:20	*Coffee Break*	
16:20-16:40	Nigel Byott	Galois module structure of ideals in weakly ramified extensions of local fields
16:50-17:10	G. Griffith Elder	Scaffolds and Hopf-Galois module structure for ramified extensions of degree p
17:20-17:40	Diana Savin	About division quaternion algebras and division symbol algebras
17:50-18:10	Vincenzo Acciaro	Computing normal integral bases of abelian number fields

Monday - Afternoon session E, Lecture Hall X.

Time	**Speaker**	**Title of the talk**
14:00-14:20	Nikolay Moshchevitin	Inequalities for diophantine exponents in small dimensions
14:30-14:50	Oleg German	On multiplicative Diophantine exponents for lattices
15:00-15:20	Jaroslav Hancl	New asymptotic irrationality measure for e and other numbers
15:30-15:50	Tomislav Pejkovic	Quadratic Lagrange spectrum
15:50-16:20	*Coffee Break*	
16:20-16:40	Dzmitry Badziahin	Cantor-winning sets and their applications in Diophantine approximation
16:50-17:10	Stephen Harrap	A problem in non-linear Diophantine approximation
17:20-17:40	Johannes Schleischitz	Diophantine approximation on manifolds
17:50-18:10	Steffen Hojris Pedersen	On a higher dimensional Mahler approximation

Monday - Afternoon session F, Lecture Hall XI.

Time	Speaker	Title of the talk
14:00-14:20	Andrej Dujella	High-rank elliptic curves induced by Diophantine triples
14:30-14:50	Alan Filipin	Some recent results on polynomial Diophantine m-tuples
15:00-15:20	Tim Trudgian	A new bound on Diophantine quintuples
15:30-15:50	Ljubica Baćić	On the number of $D(4)$-quintuples
15:50-16:20	*Coffee Break*	
16:20-16:40	Ana Jurasić	On the size of Diophantine m-tuples for linear polynomials
16:50-17:10	Christoph Anton Hutle	Only finitely many Tribonacci Diophantine triples exist
17:20-17:40	Mariia Monina	About integer Somos-8 and Somos-9 sequences
17:50-18:10	Alexey Ustinov	Double Somos-4

Monday - Afternoon session G, Lecture Hall XII.

Time	Speaker	Title of the talk
14:00-14:20	Fabien Pazuki	Bad reduction of curves with CM jacobians
14:30-14:50	Jannis A. Antoniadis	Arithmetical properties of the Heisenberg curve
15:00-15:20	Keisuke Arai	Points on Shimura curves rational over imaginary quadratic fields in the non-split case
15:30-15:50	Tomasz Jędrzejak	On the torsion of the Jacobians of two families of hyperelliptic curves
15:50-16:20	*Coffee Break*	
16:20-16:40	Junjiro Noguchi	Distribution of entire curves and integral points in open algebraic varieties
16:50-17:10	Sylvain Duquesne	Memory-saving computation of the pairing final exponentiation on BN curves
17:20-17:40	Samuele Anni	On the generalized Fermat equation $x^{2l} + y^{2m} = z^p$
17:50-18:10	Amilcar Pacheco	Effective bounds for a conjecture of Lang: the case of curve

Tuesday - Morning session, F015-016

Time	Speaker	Title of the talk
9:00-10:00	Henri Darmon	Euler Systems
10:00-10:30	*Coffee Break*	
10:30-11:30	David Loeffler	Euler systems: new constructions, results and conjectures

11:30-13:00 *Lunch*

Tuesday - Afternoon session A, Lecture Hall I.

Time	Speaker	Title of the talk
14:00-14:20	Irina Rezvyakova	On Selberg's mollification method in the theory of L-functions
14:30-14:50	Andrew James Corbett	Special L-values and automorphic period integrals
15:00-15:20	Luis Lomelí	On the rationality and holomorphy of Langlands-Shahidi L-functions over function fields
15:30-15:50	Tomokazu Onozuka	On the various mean values of the Dirichlet L-functions
15:50-16:20	*Coffee Break*	
16:20-16:40	G Sudhaams Mohan Reddy	Upper and lower bounds for $\frac{L_d(1)}{L_d(2)}$ and related results
16:50-17:10	Sumaia Saad Eddin	An asymptotic distribution for $\lvert L'/L(1,\chi)\rvert$
17:20-17:40	Ade Irma Suriajaya	Some results on the zeros of the derivatives of the Riemann zeta function and Dirichlet L-functions

Tuesday - Afternoon session B, Lecture Hall II.

Time	Speaker	Title of the talk
14:00-14:20	Paulius Drungilas	On the degree of sum of two algebraic numbers
14:30-14:50	Antonella Perucca	Reductions of algebraic integers
15:00-15:20	Jonas Jankauskas	Simple linear equations in conjugates of a Pisot number
15:30-15:50	Dragan Stankov	Powers of Salem numbers and distribution modulo 1
15:50-16:20	*Coffee Break*	
16:20-16:40	Victoria Zhuravleva	Diophantine approximation with Pisot numbers
16:50-17:10	Tomas Vavra	Number fields generated by Pisot units
17:20-17:40	Adrian Scheerer	Normality in Pisot numeration systems
17:50-18:10	Hajime Kaneko	Arithmetical properties of power series related to β-expansion

Tuesday - Afternoon session C, Lecture Hall III.

Time	Speaker	Title of the talk
14:00-14:20	Florian Luca	On a problem of Pillai with Fibonacci numbers and powers of 2
14:30-14:50	Takafumi Miyazaki	On a three term exponential Diophantine equation
15:00-15:20	Gökhan Soydan	On the Diophantine equation $(x+1)^k + (x+2)^k + ... + (lx)^k = y^n$
15:30-15:50	Péter Olajos	Properties of balancing and generalized balancing numbers
15:50-16:20	*Coffee Break*	

16:20-16:40	Boris Bartolome	On the equation $X^n - 1 = BZ^n$
16:50-17:10	István Pink	On the diophantine equation $1 + 2^a + x^b = y^n$
17:20-17:40	Zsolt Rábai	A note on the shuffle variant of Jesmanowicz' conjecture
17:50-18:10	Csanád Bertók	A Hasse-type principle for exponential Diophantine equations and its applications

Tuesday - Afternoon session D, Lecture Hall IX.

Time	Speaker	Title of the talk
14:00-14:20	Marco Streng	Elliptic divisibility sequences and modular units
14:30-14:50	Ho Yun Jung	Primitive Fricke families and their application to modular function fields
15:00-15:20	Hironori Shiga	One class field via hypergeometric modular function
15:30-15:50	Guillermo Mantilla-Soler	A space of weight 1 modular forms attached to totally real cubic number fields
15:50-16:20	*Coffee Break*	
16:20-16:40	Jolanta Marzec	Siegel modular forms and their fundamental Fourier coefficients
16:50-17:10	Thorsten Paul	The Fourier-Jacobi-decomposition of Eisenstein series of Klingen type
17:20-17:40	Raphael Sebastian Steiner	Supnorms of half-integral weight modular forms
17:50-18:10	Enrico Varela	Representation theory of Drinfeld modular forms

Tuesday - Afternoon session E, Lecture Hall X.

Time	Speaker	Title of the talk
14:00-14:20	Jean-Louis Verger-Gaugry	A Dobrowolski type minoration of the Mahler measure of height 1 trinomials
14:30-14:50	Norbert Kaiblinger	On open problems by Lind and by Taussky-Todd
15:00-15:20	Kostadinka Lapkova	On the k-free values of the polynomial $xy^k + C$
15:30-15:50	Christina Karolus	Explicit bounds for composite lacunary polynomials
15:50-16:20	*Coffee Break*	
16:20-16:40	Rainer Schulze-Pillot	Koecher-Maaßseries and representation of quadratic forms
16:50-17:10	Guram Gogishvili	"Some special classes of positive quaternary quadratic forms, which sharpen general estimates of corresponding singular series"
17:20-17:40	Ketevan Shavgulidze	On the quadratic forms of five variables
17:50-18:10	Teimuraz Vepkhvadze	On the number of representations of numbers by the binary quadratic forms with discriminants -80, -128 and -140

Tuesday - Afternoon session F, Lecture Hall XI.

Time	Speaker	Title of the talk
14:00-14:20	Paul Voutier	Periodic Jacobi-Perron algorithm expansions
14:30-14:50	Maciej Szymon Zakarczemny	Number of solutions in a box of a linear equation in an Abelian group
15:00-15:20	Pee Choon Toh	On certain pairs of q-series identities
15:30-15:50	Rupam Barman	Hypergeometric series in the p-adic setting
15:50-16:20	*Coffee Break*	
16:20-16:40	Stefan Porubský	On common structure of n_k's for which $n_k\alpha \bmod 1 \to x$
16:50-17:10	Ladislav Mišík	Simple sets of distribution functions of ratio sequences
17:20-17:40	Maciej Gawron	On formal inverse of the Prouhet-Thue-Morse sequence
17:50-18:10	Sneh Bala Sinha	Transcendence of generalized Euler-Lehmer constants

Tuesday - Afternoon session G, Lecture Hall XII.

Time	Speaker	Title of the talk
14:00-14:20	Christian Elsholtz	A problem of Ramanujan, Erdős and Kátai on the iterated divisor function
14:30-14:50	Alain Togbe	On P-integers
15:00-15:20	Sanda Bujacic	A variation of a congruence of Subbarao for $n = 2^\alpha 5^\beta$, $\alpha, \beta \geq 0$
15:30-15:50	Titus Hilberdink	Extremality of the completely multiplicative functions
15:50-16:20	*Coffee Break*	
16:20-16:40	Ehud Moshe Baruch	Hecke operators and new forms
16:50-17:10	Aftab Pande	Reductions of Galois representations
17:20-17:40	Adrián Zenteno	Four dimensional Galois representations with large image
17:50-18:10		

Tuesday, Public Lecture

Time	Speaker	Title of the talk
18:40-19:40	László Lovász	Limit structures in graph theory and number theory

Wednesday - Morning session, F015-016

Time	Speaker	Title of the talk
9:00-10:00	James Maynard	Long gaps between primes
10:00-10:30	*Coffee Break*	
10:30-11:30	Julia Wolf	Ramsey multiplicity of patterns in finite abelian groups
11:30-13:00	*Lunch*	

Thursday - Morning session, F015-016

Time	Speaker	Title of the talk
9:00-10:00	Tim Browning	How common are failures of the Hasse principle or weak approximation?
10:00-10:30	*Coffee Break*	
10:30-11:30	Julia Hartmann	Obstructions to Local-Global Principles for Torsors
11:30-11:40	*Break*	
11:40-12:40	Anna Cadoret	Specialization of representations of the étale fundamental group
12:40-14:00	*Lunch*	

Thursday - Afternoon session A, Lecture Hall I.

Time	Speaker	Title of the talk
14:00-14:20	János Pintz	On the distribution of consecutive gaps between primes
14:30-14:50	Ákos Magyar	Prime and almost prime solutions to diophantine systems of high rank
15:00-15:20	Neville Robbins	Some new necessary conditions for the existence of an odd perfect number
15:30-15:50	Stijn Stefan Campbell Hanson	Various extensions of Chen's theorems
15:50-16:20	*Coffee Break*	
16:20-16:40	Markus Hittmeir	Deterministic integer factorization via polynomials over $\mathbb{Z}$
16:50-17:10	Christiaan van de Woestijne	Factorisation of finite graphs and polynomials with nonnegative coefficients
17:20-17:40	Korneel Debaene	Sieving for completely splitting primes

Thursday - Afternoon session B, Lecture Hall II.

Time	Speaker	Title of the talk
14:00-14:20	András Bíró	Class number one problem for Richaud-Degert type fields
14:30-14:50	Günter Lettl	Orders and conductors in algebraic number fields
15:00-15:20	Miho Aoki	Systems of fundamental units of quartic fields and imaginary quadratic fields with class number divisible by five
15:30-15:50	Nathan Jones	The distribution of class groups of imaginary quadratic fields
15:50-16:20	*Coffee Break*	
16:20-16:40	Laura Paladino	Fields generated by torsion points of elliptic curves
16:50-17:10	Yasuhiro Kishi	Imaginary quadratic fields whose ideal class groups have 3-rank at least three
17:20-17:40	Borka Jadrijević	Computing relative power integral bases in a family of quartic extensions of imaginary quadratic fields
17:50-18:10	Tímea Szabó	Power integral bases in quartic fields and quartic extensions

Thursday - Afternoon session C, Lecture Hall III.

Time	Speaker	Title of the talk
14:00-14:20	Maciej Ulas	Primitive integer solutions of certain Diophantine equations
14:30-14:50	Dijana Kreso	Indecomposability of polynomials and Diophantine equations
15:00-15:20	Divyum Sharma	Number of solutions of Thue inequalities
15:30-15:50	Akinari Hoshi	On the simplest number fields and related Thue equations
15:50-16:20	*Coffee Break*	
16:20-16:40	László Szalay	Sum of certain elements in Pascal-type triangles
16:50-17:10	Kevin Henriot	Diophantine equations in dense variables
17:20-17:40	András Bazsó	On a diophantine equation concerning Appell sequences
17:50-18:10	Judit Ferenczik	Equal values of combinatorial numbers

Thursday - Afternoon session D, Lecture Hall IX.

Time	Speaker	Title of the talk
14:00-14:20	Thomas Wright	Carmichael numbers and variants of Korselt's criterion
14:30-14:50	Tamás Lengyel	Arithmetic properties of lacunary sums of binomial coefficients
15:00-15:20	Matthew Charles Lettington	On higher dimensional interlacing Fibonacci sequences, continued fractions and Chebyshev polynomials
15:30-15:50	Mehmet Cenkci	Recurrences and congruences for several degenerate numbers
15:50-16:20	*Coffee Break*	

16:20-16:40	Volker Ziegler	On the number of integers that are the sum of exactly k units
16:50-17:10	Szabolcs Tengely	Rational functions and arithmetic progressions
17:20-17:40	Márton Szikszai	Bounds and formulas for a Jacobsthal-type function in sequences
17:50-18:10	Jasbir Chalal	Rational albime triangles and elliptic curves

Thursday - Afternoon session E, Lecture Hall X.

Time	**Speaker**	**Title of the talk**
14:00-14:20	Alina Carmen Cojocaru	Arithmetic properties of the Frobenius traces of an abelian variety
14:30-14:50	Andrzej Dabrowski	Orders of Tate-Shafarevich groups in quadratic twists of $X_0(49)$
15:00-15:20	Daniel C. Mayer	Index-p Abelinaziation data of p-class tower groups
15:30-15:50	Valentijn Zoe Karemaker	Constructing abelian varieties providing solutions to the inverse Galois problem for symplectic groups
15:50-16:20	*Coffee Break*	
16:20-16:40	Florian Bouyer	How to identify lattices: an introduction
16:50-17:10	Matthew James Spencer	Brauer relations in positive characteristic
17:20-17:40	Ram Krishna Pandey	Direct and inverse problems in subsequence sums

Thursday - Afternoon session F, Lecture Hall XI.

Time	**Speaker**	**Title of the talk**
14:00-14:20	Joerg Thuswaldner	S-adic words, Rauzy fractals, and torus rotations
14:30-14:50	Valerio Talamanca	Symmetries for heights on split tori
15:00-15:20	Damaris Schindler	Del Pezzo surfaces of degree four violating the Hasse principle
15:30-15:50	Péter Maga	Subconvexity for sup-norms of automorphic forms on $PGL(n)$
15:50-16:20	*Coffee Break*	
16:20-16:40	Su-ion Ih	Distribution of integral division points on the algebraic torus
16:50-17:10	Sam Chow	Equidistribution of values of linear forms on a cubic hypersurface
17:20-17:40	Evgeniy Zorin	Rational points and linear forms near manifolds
17:50-18:10	Jun Ueki	Relative genus theory and Iwasawa μ-invariants for rational homology 3-spheres

Thursday - Afternoon session G, Lecture Hall XII.

Time	Speaker	Title of the talk
14:00-14:20	Robert Tichy	Arithmetic dynamical systems
14:30-14:50	Katalin Gyarmati	On the complexity of a family of Legendre sequences with irreducible polynomials
15:00-15:20	Manfred Madritsch	Forms of differing degrees over number fields
15:30-15:50	Elisa Lorenzo Garcia	Statistics for the number of points on biquadratic curves over finite fields
15:50-16:20	*Coffee Break*	
16:20-16:40	Rainer Dietmann	Hilbert cubes in arithmetic sets
16:50-17:10	Qinghai Zhong	The set of minimal distances in Krull monoids
17:20-17:40	Giacomo Cherubini	Error terms in hyperbolic counting
17:50-18:10	Richárd Sebők	On a connection between pseudorandom measures

Friday - Morning session, F015-016

Time	Speaker	Title of the talk
9:00-10:00	Harald Helfgott	The ternary Goldbach conjecture
10:00-10:30	*Coffee Break*	
10:30-11:30	Jared Weinstein	Moduli of p-divisible groups
11:30-13:00	*Lunch*	

Chairmen

Day	Time	Session	Chairman
Monday	10:10–12:40	M	Michel Waldschmidt
Monday	14:00–15:50	A	Aleksandar Ivić
Monday	14:00–15:50	B	József Solymosi
Monday	14:00–15:50	C	Yilmaz Simsek
Monday	14:00–15:50	D	Jean-Louis Verger-Gaugry
Monday	14:00–15:50	E	Paul Voutier
Monday	14:00–15:50	F	László Szalay
Monday	14:00–15:50	G	Junjiro Noguchi
Monday	16:20–18:10	A	Maxim Korolev
Monday	16:20–18:10	B	Sergei Konyagin
Monday	16:20–18:10	C	Takao Komatsu
Monday	16:20–18:10	D	Volker Ziegler
Monday	16:20–18:10	E	Nikolay Moshchevitin
Monday	16:20–18:10	F	Alan Filipin
Monday	16:20–18:10	G	Fabien Pazuki
Tuesday	9:00–11:30	M	Michael Pohst
Tuesday	14:00–15:50	A	Gergely Harcos
Tuesday	14:00–15:50	B	Maciej Ulas
Tuesday	14:00–15:50	C	Jannis A. Antoniadis
Tuesday	14:00–15:50	D	Jasbir Chahal
Tuesday	14:00–15:50	E	Rainer Dietmann
Tuesday	14:00–15:50	F	Stefan Porubský
Tuesday	14:00–15:50	G	Ladislav Mišík
Tuesday	16:20–18:10	A	Kohji Matsumoto
Tuesday	16:20–18:10	B	Oleg German
Tuesday	16:20–18:10	C	Alain Togbé
Tuesday	16:20–18:10	D	Christian Elsholtz
Tuesday	16:20–18:10	E	Alina Cojocaru
Tuesday	16:20–18:10	F	Jaroslav Hančl

Day	Time	Session	Chairman
Tuesday	16:20–18:10	G	Jan Šustek
Wednesday	9:00–11:30	M	János Pintz
Thursday	09:00–12:40	M	Robert Tichy
Thursday	14:00–15:50	A	Florian Luca
Thursday	14:00–15:50	B	Christiaan van de Woestijne
Thursday	14:00–15:50	C	Csaba Rakaczki
Thursday	14:00–15:50	D	Katalin Gyarmati
Thursday	14:00–15:50	E	András Bíró
Thursday	14:00–15:50	F	Ismail Naci Cangul
Thursday	14:00–15:50	G	Andrej Dujella
Thursday	16:20–18:10	A	Günter Lettl
Thursday	16:20–18:10	B	Jörg Thuswaldner
Thursday	16:20–18:10	C	Ákos Magyar
Thursday	16:20–18:10	D	Claude Levesque
Thursday	16:20–18:10	E	Tamás Lengyel
Thursday	16:20–18:10	F	Florian Breuer
Thursday	16:20–18:10	G	Dzmitry Badziahin
Friday	09:00–11:30	M	Imre Ruzsa

List of participants

Participant	**e-mail**	**Time of talk**
Vincenzo Acciaro	v.acciaro@unich.it	Monday, 17:50-18:10
Nikola Adžaga	nadzaga@grad.hr	-
Farkhanda Afzal	farkhanda_imran@live.com	-
Samuele Anni	s.anni@warwick.ac.uk	Monday, 17:20-17:40
Jannis A. Antoniadis	antoniad@uoc.gr	Monday, 14:30-14:50
Miho Aoki	aoki@riko.shimane-u.ac.jp	Thursday, 15:00-15:20
Keisuke Arai	araik@mail.dendai.ac.jp	Monday, 15:00-15:20
Ljubica Baćić	ljubica.bacic@skole.hr	Monday, 15:30-15:50
Salim Badidja	badidja@hotmail.fr	-
Ioan Badulescu	ibadules@univ-montp2.fr	-
Dzmitry Badziahin	dzmitry.badziahin@durham.ac.uk	Monday, 16:20-16:40
Rupam Barman	rupam@maths.iitd.ac.in	Tuesday, 15:30-15:50
Boris Bartolome	Boris.Bartolome@math.u-bordeaux1.fr	Tuesday, 16:20-16:40
Ehud Moshe Baruch	embaruch@math.technion.ac.il	Tuesday, 16:20-16:40
András Bazsó	bazsoa@science.unideb.hu	Thursday, 17:20-17:40
Paloma Bengoechea	paloma.bengoechea@york.ac.uk	-
Mike Bennett	bennett@math.ubc.ca	-
Attila Bérczes	berczesa@science.unideb.hu	-
Christian Berghoff	berghoff@math.uni-bonn.de	-
Csanád Bertók	bertok.csanad@science.unideb.hu	Tuesday, 17:50-18:10
Anne Bertrand Mathis	bertrand@math.univ-poitiers.fr	-
Dávid Bezzeg	-	-
Pierre Bienvenu	py.bienvenu@gmail.com	-
András Bíró	biroand@renyi.hu	Thursday, 14:00-14:20
Iván Blanco Chacón	ivnblanco@gmail.com	-
Dante Bonolis	dante.bonolis@math.ethz.ch	-
Florian Bouyer	f.bouyer@warwick.ac.uk	Thursday 16:20-16:40
Florian Breuer	fbreuer@sun.ac.za	-
Tim Browning	t.d.browning@bristol.ac.uk	Thursday, 9:00-10:00
Yann Bugeaud	bugeaud@math.unistra.fr	-
Sanda Sanda Bujačić	sbujacic@math.uniri.hr	Tuesday, 15:00-15:20
Boris Bukh	bbukh@math.cmu.edu	-
Jan Büthe	jbuethe@math.uni-bonn.de	Monday, 14:30-14:50

Participant	**e-mail**	**Time of talk**
Nigel Byott	N.P.Byott@ex.ac.uk	Monday, 16:20-16:40
Anna Cadoret	anna.cadoret@polytechnique.edu	Thursday, 11:40-12:40
Ismail Naci Cangul	cangul@uludag.edu.tr	-
Mehmet Cenkci	cenkci@akdeniz.edu.tr	Thursday, 15:30-15:50
Jasbir Chahal	travel@mathematics.byu.edu	-
Giacomo Cherubini	giacomo.cherubini@math.ku.dk	Thursday, 17:20-17:40
Kwok Chi Chim	chim@math.tugraz.at	-
Sam Chow	Sam.Chow@bristol.ac.uk	Thursday, 16:50-17:10
Alina Carmen Cojocaru	math.cojocaru@gmail.com	Thursday, 14:00-14:20
Esra Colak	colakesraa@gmail.com	-
Giovanni Coppola	giovanni.coppola@unina.it	Monday, 14:30-14:50
Andrew James Corbett	andrew.corbett@bristol.ac.uk	Tuesday, 14:30-14:50
Andrzej Dąbrowski	dabrowsk@wmf.univ.szczecin.pl	Thursday, 14:30-14:50
Henri Darmon	darmon@math.mcgill.ca	Tuesday, 9:00-10:00
Korneel Debaene	korneeldebaene@hotmail.com	Thursday, 17:20-17:40
Fabian Dehnert	fdehner@uni-math.gwdg.de	-
Dino Destefano	dino@math.ku.dk	-
Rainer Dietmann	Rainer.Dietmann@rhul.ac.uk	Thursday, 16:20-16:40
Ayhan Dil	adil@akdeniz.edu.tr	Monday, 15:30-15:50
Daniel Dombek	daniel.dombek@fit.cvut.cz	-
Emmanouil Doulgerakis	emmanouhld@gmail.com	-
Paulius Drungilas	pdrungilas@gmail.com	Tuesday, 14:00-14:20
Andrej Dujella	duje@math.hr	Monday, 14:00-14:20
Sylvain Duquesne	sylvain.duquesne@univ-rennes1.fr	Monday, 16:50-17:10
G.Griffith Elder	elder@unomaha.edu	Monday, 16:50-17:10
Christian Elsholtz	elsholtz@math.tugraz.at	Tuesday, 14:00-14:20
Jan-Hendrik Evertse	evertse@math.leidenuniv.nl	Monday, 10:10-11:10
Judit Ferenczik	jferenczik@science.unideb.hu	Thursday, 17:50-18:10
Alan Filipin	filipin@grad.hr	Monday, 14:30-14:50
János Folláth	follath.janos@inf.unideb.hu	-
Zrinka Franušić	fran@math.hr	-
István Gaál	gaal.istvan@unideb.hu	-
Maciej Gawron	maciej.gawron@uj.edu.pl	Tuesday, 17:20-17:40
Oleg German	german.oleg@gmail.com	Monday, 14:30-14:50
Guram Gogishvili	guramgog@gmail.com	Tuesday, 16:50-17:10
David Joseph Grynkiewicz	diambri@hotmail.com	Monday, 14:30-14:50
Christelle Guichard	christelle.guichard@ujf-grenoble.fr	-
Katalin Gyarmati	gykati@cs.elte.hu	Thursday, 14:30-14:50
Eszter Gyimesi	gyimesie@science.unideb.hu	Monday, 17:20-17:40
Kálmán Győry	gyory@science.unideb.hu	-
Máté Győry	mate.gyory@gmail.com	-
Lajos Hajdu	hajdul@science.unideb.hu	-
Gábor Halász	halasz.gabor@renyi.mta.hu	-

Participant	**e-mail**	**Time of talk**
Yoshinori Hamahata	hamahata@xmath.ous.ac.jp	Monday, 15:30-15:50
Jaroslav Hančl	hancl@osu.cz	Monday, 15:00-15:20
Stijn Stefan Campbell Hanson	stijnhanson@gmail.com	Thursday, 15:30-15:50
Gergely Harcos	gharcos@renyi.hu	-
Stephen Harrap	s.g.harrap@durham.ac.uk	Monday, 16:50-17:10
Julia Hartmann	hartmann@math.upenn.edu	Thursday, 10:30-11:30
Bo He	bhe@live.cn	-
Peter Vincent Hegarty	hegarty@chalmers.se	Monday, 17:20-17:40
Harald Andres Helfgott	harald.helfgott@gmail.com	Friday, 9:00-10:00
Peter Hellekalek	peter.hellekalek@sbg.ac.at	-
Kevin Henriot	kevin.henriot@gmail.com	Thursday, 16:50-17:10
Titus Hilberdink	t.w.hilberdink@reading.ac.uk	Tuesday, 15:30-15:50
Yumiko Hironaka	hironaka@waseda.jp	Monday, 15:00-15:20
Markus Hittmeir	markus.hittmeir@sbg.ac.at	Thursday, 16:20-16:40
Gábor Horváth	ghorvath@science.unideb.hu	-
Akinari Hoshi	hoshi@math.sc.niigata-u.ac.jp	Thursday, 15:30-15:50
Christoph Anton Hutle	christoph.hutle@gmx.at	Monday, 16:50-17:10
Su-ion Ih	ih@math.colorado.edu	Thursday, 16:20-16:40
Tomohiro Ikkai	gft.1772@gmail.com	-
Aleksandar Ivić	aivic_2000@yahoo.com	Monday, 16:20-16:40
Borka Jadrijević	borka@pmfst.hr	Thursday, 17:20-17:40
Jonas Jankauskas	jonas.jankauskas@gmail.com	Tuesday, 15:00-15:20
Tomasz Jędrzejak	tjedrzejak@gmail.com	Monday 15:30-15:50
Nathan Jones	ncjones@uic.edu	Thursday, 15:30-15:50
Ho Yun Jung	hoyunjung@nims.re.kr	Tuesday, 14:30-14:50
Ana Jurasić	ajurasic@math.uniri.hr	Monday, 16:20-16:40
Roma Kacinskaite	r.kacinskaite@fm.su.lt	-
Norbert Kaiblinger	norbert.kaiblinger@boku.ac.at	Tuesday, 14:30-14:50
Hajime Kaneko	kanekoha@math.tsukuba.ac.jp	Tuesday, 17:50-18:10
Deniz Ali Kaptan	denizalikaptan@gmail.com	-
Valentijn Zoe Karemaker	V.Z.Karemaker@uu.nl	Thursday, 15:30-15:50
Christina Karolus	christina.karolus@sbg.ac.at	Tuesday, 15:30-15:50
Ian Kiming	kiming@math.ku.dk	-
Yasuhiro Kishi	ykishi@auecc.aichi-edu.ac.jp	Thursday, 16:50-17:10
Hershy H. Kisilevsky	hershy.kisilevsky@concordia.ca	-
Sándor Kiss	kisspest@cs.elte.hu	Monday, 16:50-17:10
Martin Klazar	klazar@kam.mff.cuni.cz	-
Takao Komatsu	komatsu@whu.edu.cn	Monday, 14:00-14:20
Sergei Vladimirovich Konyagin	konyagin23@gmail.com	Monday, 14:00-14:20
Maxim Aleksandrovich Korolev	hardy_ramanujan@mail.ru	Monday, 14:00-14:20
Levente Kovács	kovacs.levente@bankszovetseg.hu	-
Dijana Kreso	kreso@math.tugraz.at	Thursday, 14:30-14:50
Tünde Lality-Kovács	tkovacs@science.unideb.hu	-

Participant	**e-mail**	**Time of talk**
Kostadinka Lapkova	lapkova.kostadinka@renyi.mta.hu	Tuesday, 15:00-15:20
Thai Hoang Le	thai-hoang.le@polytechnique.edu	Monday, 15:30-15:50
Philippe Lebacque	philippe.lebacque@univ-fcomte.fr	-
Tamás Lengyel	lengyel@oxy.edu	Thursday, 14:30-14:50
Matthew Charles Lettington	LettingtonMC@cardiff.ac.uk	Thursday, 15:00-15:20
Günter Lettl	guenter.lettl@uni-graz.at	Thursday, 14:30-14:50
Claude Levesque	cl@mat.ulaval.ca	-
Kálmán Liptai	liptaik@ektf.hu	-
David Loeffler	D.A.Loeffler@warwick.ac.uk	Tuesday, 10:30-11:30
Luis Luis Lomelí	lomeli@mpim-bonn.mpg.de	Tuesday, 15:00-15:20
Elisa Lorenzo Garcia	elisa.lorenzo@gmail.com	Thursday, 15:30-15:50
László Lovász	lovasz@cs.elte.hu	-
Florian Luca	florian.luca@wits.ac.za	Tuesday, 14:00-14:20
Piotr Maciak	maciak@math.ku.dk	-
Manfred Madritsch	manfred.madritsch@univ-lorraine.fr	Thursday, 15:00-15:20
Péter Maga	magapeter@gmail.com	Thursday, 15:30-15:50
Ákos Magyar	amagyar@uga.edu	Thursday, 14:30-14:50
Guillermo Mantilla-Soler	g.mantilla691@uniandes.edu.co	Tuesday, 15:30-15:50
Jolanta Marzec	jolanta.marzec@bristol.ac.uk	Tuesday, 16:20-16:40
Kohji Matsumoto	kohjimat@math.nagoya-u.ac.jp	Monday, 16:50-17:10
Daniel C. Mayer	algebraic.number.theory@algebra.at	Thursday, 15:00-15:20
James Maynard	james.maynard@magd.ox.ac.uk	Wednesday, 9:00-10:00
István Mező	istvanmezo81@gmail.com	Monday, 15:30-15:50
Ladislav Mišík	ladislav.misik@osu.cz	Tuesday, 16:50-17:10
Piotr Miska	piotrmiska91@gmail.com	Monday, 16:20-16:40
Vladimir Mitankin	v.mitankin@bristol.ac.uk	-
Takafumi Miyazaki	miyazaki-takafumi@math.cst.nihon-u.ac.jp	Tuesday, 14:30-14:50
Mariia Monina	monina_dvggu@mail.ru	Monday, 17:20-17:40
Nikolay Moshchevitin	moshchevitin@gmail.com	Monday, 14:00-14:20
Yuri Nesterenko	nester@mi.ras.ru	-
Junjiro Noguchi	noguchi@ms.u-tokyo.ac.jp	Monday, 16:20-16:40
Gábor Nyul	gnyul@science.unideb.hu	Monday, 16:50-17:10
Péter Olajos	matolaj@uni-miskolc.hu	Tuesday, 15:30-15:50
Tomokazu Onozuka	m11022v@math.nagoya-u.ac.jp	Tuesday, 15:30-15:50
Amilcar Pacheco	amilcar@acd.ufrj.br	Monday, 17:50-18:10
Laura Paladino	paladino@mail.dm.unipi.it	Thursday, 16:20-16:40
Aftab Pande	aftab.pande@gmail.com	Tuesday, 16:50-17:10
Ram Krishna Pandey	ramkpandey@gmail.com	Thursday, 17:20-17:40
Tomos Parry	tomos.parry1729@hotmail.co.uk	-
Thorsten Paul	thorstenpaul@math.uni-sb.de	Tuesday, 16:50-17:10
Fabien Pazuki	fabien.pazuki@gmail.com	Monday, 14:00-14:20
Steffen Hojris Pedersen	steffenh@math.au.dk	Monday, 17:50-18:10

Participant	e-mail	Time of talk
Tomislav Pejkovic	pejkovic@math.hr	Monday, 15:30-15:50
Antonella Perucca	antonella.perucca@mathematik.uni-regensburg.de	Tuesday, 14:30-14:50
Gyöngyvér Péter	-	-
Attila Pethő	pethoe@inf.unideb.hu	-
István Pink	pinki@science.unideb.hu	Tuesday, 16:50-17:10
Ákos Pintér	apinter@science.unideb.hu	
János Pintz	pintz@mta.renyi.hu	Thursday, 14:00-14:20
Michael Erich Pohst	pohst@math.tu-berlin.de	-
Stefan Porubský	sporubsky@hotmail.com	Tuesday, 16:20-16:40
Zsolt Rábai	zsrabai@science.unideb.hu	Tuesday, 17:20-17:40
Gabriella Rácz	racz.gabriella@gmail.hu	Monday, 17:50-18:10
Csaba Rakaczki	matrcs@uni-miskolc.hu	-
Wayne Raskind	raskind@wayne.edu	-
G Sudhaams Mohan Reddy	dr.sudhamshreddy@gmail.com	Tuesday, 16:20-16:40
László Remete	remetel42@gmail.com	-
Irina Rezvyakova	irezvyakova@gmail.com	Tuesday, 14:00-14:20
Christophe Ritzenthaler	ritzenthalerchristophe@gmail.com	-
Neville Robbins	nrobbins@sfsu.edu	Thursday, 15:00-15:20
Imre Ruzsa	ruzsa@renyi.hu	-
Sumaia Saad Eddin	sumaia.saad_eddin@jku.at	Thursday 16:50-17:10
Diana Savin	dianet72@yahoo.com	Monday, 17:20-17:40
Adrian Scheerer	scheerer@math.tugraz.at	Tuesday, 17:20-17:40
Klaus Scheicher	klaus.scheicher@boku.ac.at	-
Damaris Schindler	Damaris.Schindler@hcm.uni-bonn.de	Thursday, 15:00-15:20
Andrzej Schinzel	schinzel@impan.pl	-
Johannes Schleischitz	johannes.schleischitz@boku.ac.at	Monday, 17:20-17:40
Rainer Schulze-Pillot	schulzep@math.uni-sb.de	Tuesday, 16:20-16:40
Richárd Sebők	sebokr@cs.elte.hu	Thursday, 17:50-18:10
Divyum Sharma	divyum@math.tifr.res.in	Thursday, 15:00-15:20
Ketevan Shavgulidze	ketevan.shavgulidze@tsu.ge	Tuesday, 17:20-17:40
Hironori Shiga	shiga@math.s.chiba-u.ac.jp	Tuesday, 15:00-15:20
Ilya D. Shkredov	ilya.shkredov@gmail.com	-
Denis Simon	denis.simon@unicaen.fr	-
Yilmaz Simsek	ysimsek@akdeniz.edu.tr	Monday, 15:00-15:20
Sneh Bala Sinha	snehbala@hri.res.in	Tuesday, 17:50-18:10
Benjamin Smith	smith@lix.polytechnique.fr	-
Ignacio Sols	isols@mat.ucm.es	-
József Solymosi	solymosi@math.ubc.ca	Monday, 16:20-16:40
Jack Sonn	sonn.jack@gmail.com	Monday, 15:00-15:20
Gökhan Soydan	gsoydan@uludag.edu.tr	Tuesday, 15:00-15:20
Anders Södergren	sodergren@math.ku.dk	Monday, 17:20-17:40
Matthew James Spencer	m.j.spencer@warwick.ac.uk	Thursday, 16:50-17:10

Participant	**e-mail**	**Time of talk**
Dragan Stankov	dstankov@rgf.bg.ac.rs	Tuesday, 15:30-15:50
Raphael Sebastian Steiner	raphael.steiner@bristol.ac.uk	Tuesday, 17:20-17:40
Cameron Leigh Stewart	cstewart@uwaterloo.ca	-
Philipp Stopp	stopp@math.uni-sb.de	-
Marco Streng	streng@math.leidenuniv.nl	Tuesday, 14:00-14:20
Paul Surer	paul.surer@boku.ac.at	-
Ade Irma Suriajaya	adeirmasuriajaya@yahoo.com	Tuesday, 17:20-17:40
Jan Šustek	jan.sustek@osu.cz	-
Tibor Szabó	tszabo@ukf.sk	-
Tímea Szabó	szabo.timea@science.unideb.hu	Thursday, 17:50-18:10
László Szalay	szalay.laszlo@emk.nyme.hu	Thursday, 16:20-16:40
Endre Szemerédi	szemered@nyuszik.rutgers.edu	-
Márton Szikszai	szikszai.marton@science.unideb.hu	Thursday, 17:20-17:40
Vera T. Sós	sos@renyi.hu	-
Valerio Talamanca	valerio@mat.uniroma3.it	Thursday, 14:30-14:50
Niclas Technau	technau@math.tugraz.at	-
Szabolcs Tengely	tengely@science.unideb.hu	Thursday, 16:50-17:10
Jack Thorne	thorne@dpmms.cam.ac.uk	Monday, 11:40-12:40
Joerg Thuswaldner	joerg.thuswaldner@unileoben.ac.at	Thursday, 14:00-14:20
Robert Tichy	tichy@tugraz.at	Thursday, 14:00-14:20
Rob Tijdeman	tijdeman@math.leidenuniv.nl	-
Alain Togbe	atogbe@pnc.edu	Tuesday, 14:30-14:50
Pee Choon Toh	peechoon.toh@nie.edu.sg	Tuesday, 15:00-15:20
Berke Topacogullari	btopaco@uni-goettingen.de	-
János Tóth	tothj@selyeuni.sk tothj@ujs.sk	-
Tim Trudgian	timothy.trudgian@anu.edu.au	Monday, 15:00-15:20
Jun Ueki	uekijun46@gmail.com	Thursday, 17:50-18:10
Maciej Ulas	maciej.ulas@gmail.com	Thursday, 14:00-14:20
Alexey Ustinov	ustinov.alexey@gmail.com	Monday, 17:50-18:10
Artem Uvakin	artemuvakin@gmail.com	Monday, 17:50-18:10
Enrico Varela	varela@math.uni-sb.de	Tuesday, 17:50-18:10
Nóra Varga	nvarga@science.unideb.hu	-
Tomas Vavra	t.vavra@seznam.cz	Tuesday, 16:50-17:10
Teimuraz Vepkhvadze	t-vepkhvadze@hotmail.com	Tuesday, 17:50-18:10
Jean-Louis Verger-Gaugry	Jean-Louis.Verger-Gaugry@univ-smb.fr	Tuesday, 14:00-14:20
Pankaj Vishe	pankaj.vishe@york.ac.uk	-
Paul Voutier	paul.voutier@gmail.com	Tuesday, 14:00-14:20
Michel Waldschmidt	michel.waldschmidt@imj-prg.fr	-
Victor Weenink	v.weenink@planet.nl	-
Jared Weinstein	jaredsweinstein@gmail.com	Friday, 10:30-11:30
Christiaan van de Woestijne	c.vandewoestijne@unileoben.ac.at	Thursday, 16:50-17:10
Julia Wolf	julia.wolf@bristol.ac.uk	Wednesday, 10:30-11:30

Participant	**e-mail**	**Time of talk**
Thomas Wright	tjw980@yahoo.com	Thursday, 14:00-14:20
Yongli Xing	ylxing@cugb.edu.cn	-
Nazli Yildiz Ikikardes	nyildizikikardes@gmail.com	Monday, 14:30-14:50
Dong Sung Yoon	dsyoon@nims.re.kr	Monday, 14:00-14:20
Paul Young	paul@math.cofc.edu	Monday, 15:00-15:20
Maciej Szymon Zakarczemny	mzakarczemny@pk.edu.pl	Tuesday, 14:30-14:50
Adrián Zenteno	matematicazg@ciencias.unam.mx	Tuesday, 17:20-17:40
Sarah Zerbes	s.zerbes@ucl.ac.uk	-
Anthoula Zervou	zervouanthi@hotmail.gr	-
Qinghai Zhong	qinghai.zhong@uni-graz.at	Thursday, 16:50-17:10
Huilin Zhu	hlzhu@xmu.edu.cn	-
Victoria Zhuravleva	victoria.zhuravleva@me.com	Tuesday, 16:20-16:40
Volker Ziegler	volker.ziegler@sbg.ac.at	Thursday, 16:20-16:40
Evgeniy Zorin	evgeniy.zorin@york.ac.uk	Thursday, 17:20-17:40

Abstracts

Computing normal integral bases of abelian number fields

Vincenzo Acciaro

Università di Chieti-Pescara

v.acciaro@unich.it

Coauthors: Leonardo Cangelmi

Let L be an abelian number field of finite degree with Galois group G. We show how to compute a normal integral basis for L, if there is at least one, assuming that the group G and an integral basis for L are known.

On the generalized Fermat equation $x^{2l} + y^{2m} = z^p$

Samuele Anni

University of Warwick

s.anni@warwick.ac.uk

Coauthors: Samir Siksek

In this talk I will show that the generalized Fermat equation $x^{2l}+y^{2m} = z^p$ has no non-trivial primitive solutions for primes $l, m \geq 5$ and $3 \leq p \leq 13$. This is achieved by relating a putative solution to a Frey curve over a real subfield of the p-th cyclotomic field, and studying its mod l representation using modularity and level lowering. In particular, I will describe, on the one hand, the modularity theorem for semistable elliptic curves over totally real number field used and, on the other hand, the computation with Hilbert modular forms done.

Arithmetical properties of the Heisenberg curve

Jannis A. Antoniadis

University of Crete

antoniad@uoc.gr

Coauthors: Aristeidis Kontogeorgis

We consider some arithmetical properties of the Heisenberg Curve, such as ramification, genus, group of automorphisms and holomorphic differentials.

Systems of fundamental units of quartic fields and imaginary quadratic fields with class number divisible by five

Miho Aoki

Shimane University

aoki@riko.shimane-u.ac.jp

Coauthors: Yasuhiro Kishi

In general, a large amount of calculation is required to obtain a system of fundamental units for a given number field. S. Kuroda [3] showed that a system of fundamental units of quartic fields which are bicyclic extensions over $\mathbb{Q}$ is given by that of quadratic subfields. After that, some results for families of quartic fields have been obtained (for example [4]). We consider a certain parametric quartic polynomial $f(X)$. First, we give the systems of fundamental units of the quartic fields which are constructed by adjoining a root of $f(X)$. Next, by the same manner as in [2], we give a family of imaginary quadratic fields with class number divisible by 5 using the roots of $f(X)$.

References

[1] M. Aoki and Y. Kishi, *On systems of fundamental units of certain quartic fields*, to appear in Int. J. Number Theory.

[2] Y. Kishi, *A new family of imaginary quadratic fields whose class number is divisible by five*, J. Number Theory 128 (2008), no. 8, 2450–2458.

[3] S. Kuroda, *Über den Dirichletschen Körper*, J. Fac. Sci. Imp. Univ. Tokyo Sect. I. 4 (1943), 383–406.

[4] K. Nakamula, *Certain quartic fields with small regulators*, J. Number Theory 57 (1996), no. 1, 1–21.

Points on Shimura curves rational over imaginary quadratic fields in the non-split case

Keisuke Arai

Tokyo Denki University

araik@mail.dendai.ac.jp

For an imaginary quadratic field k of class number > 1, Jordan proved that there are only finitely many isomorphism classes of rational indefinite quaternion division algebras B such that the associated Shimura curve M^B has k-rational points and k splits B. Here, we study the case where k does not split B, and obtain an analogous result by imposing a certain congruent condition on the discriminant of B.

On the number of $D(4)$-quintuples

Ljubica Baćić

Primary school Nikola Andrić

ljubica.bacic@skole.hr

Coauthors: Alan Filipin

We call the set of m positive distinct integers a $D(4)$-m-tuple if the product of any of its two elements increased by 4 is a perfect square. The folklore conjecture states that there exists no $D(4)$-quintuple. In this talk we will present how to improve the known bound on the number

of D(4)-quintuples, illustrating the more efficient way of counting the number of m-tuples using divisor sums. More precisely, we prove that there are at most $7 \cdot 10^{36}$ $D(4)$-quintuples.

Cantor-winning sets and their applications in Diophantine approximation

Dzmitry Badziahin

Durham University

dzmitry.badziahin@durham.ac.uk

Winning sets were invented by W. Schmidt in the 1960's. On one hand they share several remarkable properties:

1. They have full Hausdorff dimension.
2. Countable intersection of winning sets is again winning and therefore has full Hausdorff dimension.
3. The property of being winning is invariant under bi-Lipschitz homeomorphisms.

On the other there are natural examples of Schmidt winning sets in the area of Diophantine approximation. For example the set of badly approximable real numbers and more generally the set of badly approximable points in $\mathbb{R}^n$ is winning. This immediately gives a lot of information about the structure of these sets.

Quite recently various sets were introduced in Diophantine approximation which share similar properties to 1 and 2 of Schmidt winning sets but can not be shown (at least straightforwardly) to be Schmidt winning. For example in 2014 it was shown by Badziahin, Velani and independently by Beresnevich that a countable intersection of the following sets has full Hausdorff dimension:

$$\mathbf{Bad}(i,j) \cap \mathcal{L},$$

where

$$\mathbf{Bad}(i,j) := \{\mathbf{x} \in \mathbb{R}^2 \ : \ \liminf_{q\to\infty} q \cdot \max\{||qx_1||^{1/i}, ||qx_2||^{1/j}\} > 0\}$$

and $\mathcal{L}$ is a non-degenerate planar curve.

In the talk I shall introduce a notion of Cantor-winning sets and show that they share the same properties 1 – 3 as Schmidt winning sets. Finally we relate Cantor-winning sets with so called generalised badly approximable sets appeared in Diophantine approximation. In particular they include the example given above.

Hypergeometric series in the p-adic setting

Rupam Barman

Indian Institute of Technology Delhi

rupam@maths.iitd.ac.in

In [5, 6], Dermot McCarthy defined a function ${}_nG_n[\cdots]$ using the Teichmüller character of finite fields and quotients of the p-adic gamma function, which can best be described as an analogue of hypergeometric series in the p-adic setting. He also showed how results involving Gaussian hypergeometric series can be extended to a wider class of primes using the function ${}_nG_n[\cdots]$.

In this paper, we give certain transformation formulas and summation identities for the function ${}_nG_n[\cdots]$ which are not implied from the analogous hypergeometric functions over finite

fields. We will first express the number of points on certain families of elliptic curves and hyperelliptic curves, and then we will deduce the transformations and summation identities. Finally, we will deduce some special values of the G-fucntion.

References

[1] Rupam Barman, Neelam Saikia, and Dermot McCarthy, *Summation identities and special values of hypergeometric series in the p-adic setting*, J. Number Theory (accepted).

[2] Rupam Barman and Neelam Saikia, *Certain transformations for hypergeometric series in the p-adic setting*, Int. J. Number Theory, DOI: 10.1142/S1793042115500359.

[3] Rupam Barman and Neelam Saikia, *p-adic gamma function and the trace of Frobenius of elliptic curves*, J. Number Theory 140 (7) (2014), 181–195.

[4] Rupam Barman and Neelam Saikia, *p-adic gamma function and the polynomials x^d+ax+b and $x^d+ax^{d-1}+b$*, Finite Fields Appl. 29 (2014), 89–105.

[5] Dermot McCarthy, *The trace of Frobenius of elliptic curves and the p-adic gamma function*, Pacific J. Math. 261 (1) (2013), 219–236.

[6] Dermot McCarthy, *Extending Gaussian hypergeometric series to the p-adic setting*, Int. J. Number Theory 8 (7) (2012), 1581–1612.

On the equation $X^n - 1 = BZ^n$

Boris Bartolomé

Université de Bordeaux, Universität Göttingen

Boris.Bartolome@stud.uni-goettingen.de

Coauthors: Preda Mihăilescu

We consider the Diophantine equation $X^n - 1 = BZ^n$, where $B \in \mathbb{Z}$ is understood as a parameter. We prove that if the equation has a solution, then either the Euler totient of the radical, $\varphi(\mathrm{rad}(B))$, has a common divisor with the exponent n, or the exponent is a prime and the solution stems from a solution to the diagonal case of the Nagell–Ljunggren equation: $\frac{X^n-1}{X-1} = n^e Y^n,\ e \in \{0, 1\}$. This allows us to apply recent results on this equation to the binary Thue equation in question. In particular, we can then display parametrized families for which the Thue equation has no solution. The first such family was proved by Bennett in his seminal paper on binary Thue equations [Be].

References

[Be] M. A. Bennet, *Rational Approximation To Algebraic Numbers Of Small Height: The Diophantine Equation $|ax^n - by^n| = 1$*, J. Reine Angew. Math., 535 (2001), 1-49.

Hecke operators and new forms

Ehud Moshe Baruch

Technion, Israel Institute of Technology

embaruch@math.technion.ac.il

We show that the space of new forms of weight $2k$ on $\Gamma_0(N)$ can be characterized as a common eigenspace for certain Hecke operators coming from primes p dividing the level N. The result is motivated by a study of a p-adic Hecke algebra acting on irreducible representations of $GL(2, \mathbb{Z}_p)$.

On a diophantine equation concerning Appell sequences

András Bazsó

University of Debrecen

bazsoa@science.unideb.hu

Coauthors: István Pink

In the talk we present some recent results obtained on the diophantine equation $P_n(x) = g(y)$ where P_n and g are polynomials with rational coefficients, $\deg g \geq 3$, and P_n is a member of an Appell sequence.

A Hasse-type principle for exponential Diophantine equations and its applications

Csanád Bertók

University of Debrecen

bertok.csanad@science.unideb.hu

Coauthors: Lajos Hajdu

In the talk, first we propose a conjecture, similar to Skolem's conjecture, on a Hasse-type principle for exponential Diophantine equations. Namely, consider the equation

$$a_1 b_{11}^{\alpha_{11}} \cdots b_{1l}^{\alpha_{1l}} + \ldots + a_k b_{k1}^{\alpha_{k1}} \cdots b_{kl}^{\alpha_{kl}} = c \tag{1}$$

in non-negative integers $\alpha_{11}, \ldots, \alpha_{1l}, \ldots, \alpha_{k1}, \ldots, \alpha_{kl}$, where a_i, b_{ij}, are non-zero integers for every $i = 1, \ldots, k$ and $j = 1, \ldots, l$, and c is an integer. Our conjecture is that if the equation above has no solutions, then there exists an integer $m \geq 2$ such that the congruence

$$a_1 b_{11}^{\alpha_{11}} \cdots b_{1l}^{\alpha_{1l}} + \ldots + a_k b_{k1}^{\alpha_{k1}} \cdots b_{kl}^{\alpha_{kl}} \equiv c \pmod{m} \tag{2}$$

has no solutions in non-negative integers α_{ij}, $i = 1, \ldots, k$, $j = 1, \ldots, l$.

In the talk we present a result showing that in a sense, the conjecture is valid for "almost all" equations. Further, based upon the conjecture we propose a general method for the solution of exponential Diophantine equations, relying on a generalization of a result of Erdős, Pomerance and Schmutz concerning Carmichael's λ function.

Finally, we illustrate how our method works, by solving a problem of Terai concerning the Diophantine equation

$$(4m^2 + 1)^x + (5m^2 - 1)^y = (3m)^z$$

in non-negative integers m, x, y. Terai proved that if $m \not\equiv 3 \pmod 6$ or $m \leq 20$, then the equation has the only solution $(x, y, z) = (1, 1, 2)$, and conjectured that this should hold for all m. Later, the conjecture was proved by Su and Li for $m > 90$. By using our method, we solve the remaining cases, which gives a complete (affirmative) proof to Terai's conjecture.

Class number one problem for Ruchaud-Degert type fields

András Bíró

Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences

biroand@renyi.hu

Coauthors: Kostadinka Lapkova

We will discuss the possibility of solving unconditionally the class number one problem for the special real quadratic number fields called Richaud-Degert type fields.

How to identify lattices: an introduction

Florian Bouyer

University of Warwick

f.bouyer@warwick.ac.uk

Arithmetic geometers often studies the Picard Group, $\mathrm{Pic}(X)$, of a surface X. For K3 surfaces, the Picard group is also a lattice, and as such after finding the Picard group it can be useful to describe it as a lattice.

In this talk I will first introduce lattices and give some background knowledge. Then, by using a couple of explicit Picard Group, I will work through a couple of examples on how one can identify a given lattice. This is ongoing work as part of my PhD thesis.

How common are failures of the Hasse principle or weak approximation?

Tim Browning

University of Bristol

t.d.browning@bristol.ac.uk

Coauthors: Martin Bright, Dan Loughran

A family of Diophantine equations over a number field k is said to satisfy the Hasse principle if checking solubility over all completions of k is a sufficient condition for checking solubility over k. Such a family is said to satisfy weak approximation if the k-rational solutions are dense in the space of local solutions. These fundamental properties both hold for smooth quadrics, for example, but even within the class of equations defining geometrically rational varieties there are many examples in the literature showing that either one can fail. In this talk I will discuss the frequency of counter-examples to the Hasse principle and weak approximation for some well-known families of Diophantine equations.

A variation of a congruence of Subbarao for $n = 2^\alpha 5^\beta, \ \ \alpha, \beta \geq 0$

Sanda Bujačić

University of Rijeka

sbujacic@math.uniri.hr

Euler's totient function of a positive integer $n > 1$, denoted as $\varphi(n)$, is defined to be the number of positive integers less than n that are coprime to n. Function σ of a positive integer n is defined to be the sum of all the positive integer divisors of n.

There are many open problems concerning the characterization of the positive integers n fulfilling certain congruences involving $\varphi(n)$ and $\sigma(n)$. M. V. Subbarao deals with the problem finding composite integers n such that

$$n\sigma(n) \equiv 2 \pmod{\varphi(n)}.$$

A. Dujella and F. Luca deal with the similar problem, or more precisely, they deal with the congruence which is similar to Subbarao's congruence, namely

$$n\varphi(n) \equiv 2 \pmod{\sigma(n)}. \tag{1}$$

They prove that there are only finitely many such n whose prime factors belong to a fixed finite set $\mathcal{P}$.

In this work, I deal with the congruence (1) and I prove that, if the fixed finite set of prime factors of a positive integer n is $\mathcal{P} = \{2, 5\}$, then there are only finitely many positive integers of the form $2^\alpha 5^\beta$, $\alpha, \beta \geq 0$, that satisfy the congruence (1). Those numbers are $n = 1, 2, 5, 8$.

Applications of partial knowledge of the Riemann Hypothesis

Jan Büthe

Universität Bonn

jbuethe@math.uni-bonn.de

We present some applications of partial knowledge of the Riemann Hypothesis, resp. knowledge of part of the zeros of the Riemann zeta function. This includes a *graded* version of the well-known conditional Schoenfeld bound for the prime counting function $\pi(x)$ which only assumes the correctness of the RH up to a certain height. As an algorithmic application we provide an efficient method for calculating limited range approximations to $\pi(x)$ and related functions.

Galois module structure of ideals in weakly ramified extensions of local fields

Nigel Byott

University of Exeter

N.P.Byott@ex.ac.uk

Coauthors: Griff Elder, Lindsay Childs

Let K be a local field with perfect residue field of characteristic $p > 0$, and let L be a totally and weakly ramified Galois extension of K. Let $\mathcal{P}$ be the maximal ideal of the valuation ring $\mathcal{O}$ of L. For each $h \in \mathbb{Z}$, the ideal $\mathcal{P}^h$ is a module over its associated order

$$\mathcal{A}_h = \{\alpha \ : \ \alpha \cdot x \in \mathcal{P}^h \text{ for all } x \in \mathcal{P}^h\}.$$

Under a mild hypothesis in the unequal characteristic case, we can determine completely the values of h for which $\mathcal{P}^h$ is free over $\mathcal{A}_h$, along with additional structural information about the ring $\mathcal{A}_h$. This is an application of the method of Galois scaffolds.

Specialization of representations of the étale fundamental group

Anna Cadoret

Ecole Polytechnique

anna.cadoret@polytechnique.edu

Let S be a smooth, separated, geometrically connected scheme over a finitely generated field k of characteristic p, G a reductive group over $\mathbb{Z}[N^{-1}]$ and R a topological ring of characteristic prime to pN. A continuous representation $\rho : pi_1(S) \to G(R)$ of the Ãľtale fundamental group of S can be regarded as an object parametrizing a families of Galois representations of the residue fields of the points of S, namely $\rho_s : \pi_1(s) \to \pi_1(S) \xrightarrow{\rho} G(R)$. Given a property P of the ρ_s one is interested in describing the arithmetico-geometric properties of the locus of all $s \in S$ having P.

Such problems arise naturally in the study of representation attached to the étale cohomology of smooth, proper schemes $X \to S$ and are closely related to the problem of bounding uniformly arithmetico-geometric invariants (e.g. torsion or rank of abelian varieties, rank of Néron-Severi group, motivated motivic Galois group etc.) of X_s, $s \in S$. In most cases, what one should expect is predicted by the corpus of motivic conjectures like the Tate, the Hodge or the AndrÃľ-Oort ones. I will present an overview of techniques and recent results, focussing to the case where S is a curve.

Recurrences and congruences for several degenerate numbers

Mehmet Cenkci

Akdeniz University

cenkci@akdeniz.edu.tr

We study Howard's results to review some recurrence relations for several degenerate numbers. We also deduce some congruences by making use of these recurrences.

Rational albime triangles and elliptic curves

Jasbir Chalal

Brigham Young University

travel@mathematics.byu.edu

We shall show how to use the arithmetic of elliptic curves to describe all rational albime triangles.

Error terms in hyperbolic counting.

Giacomo Cherubini

University of Copenhagen

giacomo.cherubini@math.ku.dk

We study the error term $e_\Gamma(s, z, w)$ in the hyperbolic lattice point counting problem. While the leading term of the counting function grows proportionally to e^s, the error term is conjectured to be not bigger than $O(e^{s(1/2+\varepsilon)})$, for any $\varepsilon > 0$. In analogy to a result of Hill-Parnovski we show that for Γ cocompact the average of the L^2 norm of $e_\Gamma(s, z, w)$ admits an asymptotic that is consistent with the conjecture. We also extend the work of Phillips-Rudnick and study an integrated version $E(s, z, w)$ of the error, for which it is possible to show pointwise sharp bounds and also the existence of a limiting distribution.

Equidistribution of values of linear forms on a cubic hypersurface

Sam Chow

University of Bristol

Sam.Chow@bristol.ac.uk

Recently Sargent used ergodic methods to establish the equidistribution of values of real linear forms on a rational quadric, subject to modest conditions. His ideas stemmed from quantitative refinements of Margulis' proof of the Oppenheim conjecture. Such techniques do not readily apply to higher degree hypersurfaces. We use analytic methods to obtain similar results for a cubic hypersurface. The motivation for these problems is to make precise the concept that points on our hypersurface are evenly distributed. We are led to consider a hybrid system comprising

a cubic equation and several linear inequalities. Our approach is to use the Hardy–Littlewood circle method in unison with the Davenport–Heilbronn circle method.

Arithmetic properties of the Frobenius traces of an abelian variety

Alina Carmen Cojocaru

University of Illinois at Chicago

math.cojocaru@gmail.com

Coauthors: R. Davis, A. Silverberg, K. E. Stange

Given an abelian variety $A/\mathbb{Q}$, with a trivial endomorphism ring (over the algebraic closure of $\mathbb{Q}$), we investigate the arithmetic properties of the coefficients of the p-Weil polynomials of A, as p varies.

Arithmetic bands and weighted Selberg integrals

Giovanni Coppola

University of Neaples

giovanni.coppola@unina.it

Coauthors: Maurizio Laporta

An arithmetic function f is called a *sieve function of range* Q if it is the convolution product of the constantly 1 function and g such that $g(q) \ll_\varepsilon q^\varepsilon$, $\forall \varepsilon > 0$, for $q \leq Q$, and $g(q) = 0$ for $q > Q$, i.e.

$$f(n) := \sum_{\substack{q|n \\ q\leq Q}} g(q).$$

For example, the GPY (Goldston-Pintz-Yıldırım) truncated divisor sum Λ_R involves sieve functions of range R.

In a joint work with Maurizio Laporta (see [1]), we have started the study of the distribution of f over short *arithmetic bands* (a.b.s),

$$\bigcup_{1\leq a\leq H} \{n \in (N, 2N] : n \equiv a \,(\mathrm{mod}\, q)\},$$

with $H = o(N)$ as $N \to \infty$, in order to give applications to both the correlations and to the so-called *weighted Selberg integrals* of f, on which we have concentrated our recent research. Indeed, non-trivial bounds for the quantity

$$\sum_{a\leq H} \Big(\sum_{\substack{N<n\leq 2N \\ n\equiv a \,(\mathrm{mod}\ q)}} f(n) - \frac{1}{q} \sum_{N<n\leq 2N} f(n)\Big),$$

individually on fixed q, imply the corresponding $q-$averaged version. This, in turn, entails non-trivial bounds for the *weighted Selberg integral*

$$J_{w,f}(N, H) := \sum_{N<x\leq 2N} \Big| \sum_n w_H(n - x)f(n) - M_f(x, w_H)\Big|^2,$$

where w_H is a real valued *weight*, that is uniformly bounded (as $H \to \infty$) and vanishing outside $[-H, H]$, while $M_f(x, w_H) = \sum_a w_H(a) \sum_{q\leq Q} g(q)/q$ is the expected (short intervals) *mean-value* of f. In particular, by such an alternative method, we recover the non-trivial bound for $J_{w,f}(N, H)$ that we established in [2].

References

[1] Giovanni Coppola and Maurizio Laporta, *Sieve functions in arithmetic bands*, submitted, http://arxiv.org/abs/1503.07502.
[2] Giovanni Coppola and Maurizio Laporta, *Symmetry and short interval mean-squares*, submitted, http://arxiv.org/abs/1312.5701.

Special L-values and automorphic period integrals

Andrew J. Corbett
University of Bristol
andrew.corbett@bristol.ac.uk

Period integrals of automorphic forms describe a wide range of phenomena, from the Fourier coefficients of modular forms to explicit interpretations of L-functions. We are interested in a deep conjecture of Gross–Prasad that describes the behaviour of certain integrals in terms of a central L-value. A recent work of Yifeng Liu has refined this conjecture by posing an explicit formula which vastly generalises the prototypical work of Waldspurger on GL_2-forms. Liu's refinement remains difficult to prove, even for specific groups. In this talk we review the conjecture and describe our results regarding automorphic forms on GSp_4, where one finds Siegel modular forms. We prove such an explicit formula for the Bessel period of a variety of lifts.

Orders of Tate-Shafarevich groups in quadratic twists of $X_0(49)$

Andrzej Dąbrowski
University of Szczecin
dabrowsk@wmf.univ.szczecin.pl
Coauthors: T. Jędrzejak, L. Szymaszkiewicz

We present the results of our search for the orders of Tate-Shafarevich groups for the quadratic twists of $X_0(49)$. The calculations may be served as an appendix to the results by J. Coates et al. [Proceed. LMS 110 (2015)] and Gonzales-Avilés [Trans. AMS 349 (1997)].

Euler systems

Henri Darmon
McGill University
darmon@math.mcgill.ca

The notion of "Euler system" was first introduced by Kolyvagin in the late 80's in his seminal work on the Birch and Swinnerton-Dyer conjecture for (modular) elliptic curves of analytic rank at most one. In this lecture I will give a non-technical overview of some of the main ideas in the subject, with an emphasis on the more recent developments and on their application to the Birch and Swinnerton-Dyer conjecture.

Sieving for completely splitting primes

Korneel Debaene
Ghent University
korneeldebaene@hotmail.com

The well-known Brun-Titchmarsh inequality gives an upper bound for the number of primes in an arithmetic progression, or in other words, primes with a certain splitting behaviour in a certain cyclotomic field. This upper bound is off by a factor 2 asymptotically, but its merit is that

it is effective. When one turns ones attention to the completely splitting primes of some other families of fields, the asymptotic density is known by Cebotarev, but the question of proving an effective upper bound is certainly a non-trivial one. Let l be an odd prime, then we are concerned with primes p which are 1 mod l, for which a certain prime q is an l-th power mod p. We describe the proof of an effective Brun-Titchmarsh-style upper bound for this set of primes, whose main ingredients are a Reciprocity law, theorems on counting lattice points and the Selberg Sieve.

Hilbert cubes in arithmetic sets

Rainer Dietmann
University of London
Rainer.Dietmann@rhul.ac.uk
Coauthors: Christian Elsholtz

A Hilbert cube is an iterated sumset of the form

$$a_0 + \{0, a_1\} + ... + \{0, a_d\}.$$

In this talk we discuss how large the dimension d of a Hilbert cube in 'interesting' arithmetic sets such as the squares in the interval $[1, N]$, squarefull numbers in $[1, N]$ or pure powers in $[1, N]$ can be. The proofs of our results combine ingredients on sumset growth as well as Diophantine input, bounds for character sums and an application of the larger sieve.

Geometric polynomials: properties and applications to series with zeta values

Ayhan Dil
Akdeniz University
adil@akdeniz.edu.tr
Coauthors: Khristo N. Boyadzhiev

We provide several properties of the geometric polynomials discussed in earlier works of the authors. Further, the geometric polynomials are used to obtain a closed form evaluation of certain series involving Riemann's zeta function.

On the degree of sum of two algebraic numbers

Paulius Drungilas
Vilnius University
pdrungilas@gmail.com
Coauthors: Artūras Dubickas, Chris Smyth, Florian Luca

We study the set of triplets $(a, b, c) \in \mathbb{N}^3$ for which there exist three algebraic numbers α, β, γ, with degrees a, b, c (over $\mathbb{Q}$), respectively, such that $\alpha+\beta+\gamma = 0$. Such triplets are called *sum-feasible*. In particular, we describe all the sum-feasible triplets (a, b, c) satifying $a \leq b \leq c$, $b \leq 7$ (cf. [1,2]). We also investigate a related problem of describing the set of triplets $(a, b, c) \in \mathbb{N}^3$ for which there exist number fields K and L of degrees a and b, respectively, such that the degree of the compositum KL equals c.

References

[1] P. Drungilas, A. Dubickas, C.J. Smyth, *A degree problem for two algebraic numbers and their sum,* Publ. Mat. **56**(2) (2012), 413–448.
[2] P. Drungilas, A. Dubickas, F. Luca, *On the degree of compositum of two number fields,* Math. Nachr. **286**(2-3) (2013), 171–180.

High-rank elliptic curves induced by Diophantine triples

Andrej Dujella

University of Zagreb

duje@math.hr

Coauthors: Juan Carlos Peral

We study the possible structure of the groups of rational points on elliptic curves of the form $y^2 = (x + ab)(x + ac)(x + bc)$, where a, b, c are non-zero rationals such that the product of any two of them is one less than a square. There are exactly four types of possible torsion groups for elliptic curves of this form. In each case, we construct examples and parametric families of elliptic curves with relatively high rank. In particular, we describe recent joint work with Juan Carlos Peral, with construction of an elliptic curve over the field of rational functions $\mathbb{Q}(t)$ with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and generic rank equal to 4, and an elliptic curve over $\mathbb{Q}$ with the same torsion group and rank 9. Both results improve previous records for ranks of curves with this torsion group.

Memory-saving computation of the pairing final exponentiation on BN curves

Sylvain Duquesne

University of Rennes 1

sylvain.duquesne@univ-rennes1.fr

Coauthors: Loubna Ghammam

Tate pairing computation is made of two steps. The first one, the Miller loop, is an exponentiation in the group of points of an elliptic curve. The second one, the final exponentiation, is an exponentiation in the multiplicative group of a large finite field extension.

In this talk, we describe and improve efficient methods for computing the hardest part of this second step for the most popular curves in pairing-based cryptography, namely Barreto-Naehrig curves.

We present the methods given in the literature and their complexities. However, the necessary memory resources are not always given whereas it can be an important constraint depending on the context. Therefore, we determine the memory resources required by these known methods and we present new variants which require less memory resources (up to 37%). Moreover, some of these new variants are providing algorithms which are also more efficient than the original ones.

Scaffolds and Hopf-Galois module structure for ramified extensions of degree p

Griff Elder

University of Nebraska at Omaha

elder@unomaha.edu

Coauthors: Nigel Byott, Lindsay Childs

The Galois module structure of the ring of integers in a ramified Galois extension L of degree p over a local field K of a characteristic p was determined by B. de Smit and L. Thomas in 2007. Important for their analysis is a naturally occuring scaffold for the action of the group algebra $K[\mathrm{Gal}(L/K)]$ on L. Scaffolds arise naturally for other ramified extensions of degree p (inseparable, or separable and in both characteristics). In this talk, I will exhibit scaffolds for the Hopf-Galois structures involved, and discuss the implications for Hopf-Galois module structure.

A problem of Ramanujan, Erdős and Kátai on the iterated divisor function

Christian Elsholtz

Graz University of Technology

elsholtz@math.tugraz.at

Coauthors: Yvonne Buttkewitz, Kevin Ford, Jan-Christoph Schlage-Puchta

We determine asymptotically the maximal order of $\log d(d(n))$, where $d(n)$ is the number of positive divisors of n. We have

$$\max_{n\le x} \log d(d(n)) = \frac{\sqrt{\log x}}{\log_2 x}\left(c + O\frac{\log_3 x}{\log_2 x}\right),$$

where

$$c = \left(8\sum_{j=1}^{\infty}\log^2(1+1/j)\right)^{1/2} = 2.7959802335\ldots.$$

This solves a problem first put forth by Ramanujan in 1915.

Results and open problems related to the Subspace Theorem

Jan-Hendrik Evertse

Universiteit Leiden

evertse@math.leidenuniv.nl

In 1972, W.M. Schmidt published his famous generalization of the Thue-Siegel-Roth theorem on the approximation of algebraic numbers by rationals, known as the Subspace Theorem. This was extended by Schlickewei in 1977 to include p-adic absolute values. This general p-adic Subspace Theorem turned out to be a very powerful tool in number theory and Diophantine geometry. We shall discuss the recent developments on the Subspace Theorem, and also discuss a conjectural refinement and some of its consequences.

Equal values of combinatorial numbers

Judit Ferenczik

University of Debrecen

jferenczik@math.unideb.hu

Coauthors: Ákos Pintér

Let S_k^n be the Stirling number of the second kind with positive integer parameters n and k, i. e. S_k^n is the number of partition of n elements into k non-empty sets. We formulate the following conjecture concerning common values of Stirling numbers.

Conjecture. *Let $1 < a < b$ fixed integers. Then all the solutions of equation $S_a^x = S_b^y$ with $x > a, y > b$ are $S_5^6 = S_2^5 = 15$ and $S_{90}^{91} = S_2^{15} = 4095$.*

Extending our earlier result, we prove the conjecture for $\max(a, b) < 300$. The proof is based on Baker-method, elementary estimations and grid computational technique.

Some recent results on polynomial Diophantine m-tuples

Alan Filipin

University of Zagreb

filipin@grad.hr

Coauthors: Ana Jurasić

Let a, b and c be non-zero polynomials with integer coefficients such that there exist three polynomials r, s and t from $\mathbb{Z}[X]$ such that $ab-1=r^2$, $ac-1=s^2$ and $bc-1=t^2$. Moreover, let $d \in \mathbb{Z}[X]$ be a polynomial such that there exist $x, y, z \in \mathbb{Z}[X]$ such that $ad+1=x^2$, $bd+1=y^2$ and $cd+1=z^2$, i.e. $\{a, b, c, d\}$ is a $D(-1;1)$-quadruple. In this talk we prove that d is uniquely determined by a, b and c. More precisely, the only possibilities for d are $d=0$, $d=-(a+b+c)+2abc \pm 2rst$. Except that, we will also discuss some other recent results on the topic.

On formal inverse of the Prouhet-Thue-Morse sequence

Maciej Gawron

Jagiellonian University

maciej.gawron@uj.edu.pl

Coauthors: Maciej Ulas

Let p be a prime number and consider a p-automatic sequence $\mathbf{u}=(u_n)_{n\in\mathbb{N}}$ and its generating function $U(X)=\sum_{n=0}^{\infty} u_n X^n \in \mathbb{F}_p[[X]]$. Moreover, let us suppose that $u_0=0$ and $u_1 \neq 0$ and consider the formal power series $V \in \mathbb{F}_p[[X]]$ which is a compositional inverse of $U(X)$, i.e. $U(V(X))=V(U(X))=X$. In this note we initiated the study of arithmetic properties of the sequence of coefficients of the power series $V(X)$. We are mainly interested in the case when $u_n=t_n$, where $t_n=s_2(n) \pmod 2$ and $\mathbf{t}=(t_n)_{n\in\mathbb{N}}$ is the Prouhet-Thue-Morse sequence defined on two letters alphabet $\{0,1\}$. More precisely, we study the sequence $\mathbf{c}=(c_n)_{n\in\mathbb{N}}$ which is the sequence of coefficients of the compositional inverse of the generating function of the sequence $\mathbf{t}$. This sequence is clearly 2-automatic. We present a characterization of an increasing sequence $\mathbf{a}$ characterizing solutions of the equation $c_n=1$. In particular, we get that this sequence is 2-regular. We also prove that an increasing sequence characterizing solutions of the equation $c_n=0$ is not k-regular for any k. Moreover, we present a result concerning some density properties of a sequence related to $\mathbf{a}$.

On multiplicative Diophantine exponents for lattices

Oleg N. German

Moscow State University

german@mech.math.msu.su

The variety of existing Diophantine exponents indicates how well the space of solutions to a system of k linear forms in d variables, $k<d$, can be approximated by rational subspaces. One of the standard ways to estimate this is to study the product of the values of the linear forms at nonzero integer points. At the same time, for $k=d$ no exponents have been investigated. Though the extreme case, when the corresponding product is bounded away from zero, is closely connected to the Oppenheim and Littlewood conjectures.

In our talk we will give a definition of Diophantine exponents for lattices and prove a transference theorem connecting exponents corresponding to dual lattices.

Some special classes of positive quaternary quadratic forms, which sharpen general estimates of corresponding singular series

Guram Gogishvili

Saint Andrew The First-called Georgian University

guramgog@gmail.com

Let f be any positive definite, integral, primitive, quaternary quadratic form of the determinant d. We consider the main term of formulas for the number of representations $r(f,m)$ of $m \in \mathbb{N}$ by f. The main term expressed by the so-called singular series $\rho(f,m)$ can be represented as an infinite product of definite quantities $\chi(p)$ over all primes p. The formulas for the $\chi(p)$ (even under more general assumptions) are obtained by Malysev [3]. These formulas are simplified in some cases and represented in the convenient form in [1]. The estimates of $\rho(f,m)$ with respect to d and m are important for the investigation of the asymptotic behavior of $r(f,m)$, determination of one-class genera of the quadratic forms f, the existence of the so-called Gauss type formulas for $r(f,m)(r(f,m) = \rho(f,m))$ and in other applications. In the paper [3] some estimates of $\chi(p), p \geq 2$, are given. They yield $\rho(f,m) = O(d^{\frac{1}{2}} m^{1+\varepsilon})$ for any $\varepsilon > 0$. Some analogous results are obtained by various authors too. In the paper [2] we essentially improved the existing results and proved

$$\rho(f,m) = O(d_0^{-\frac{1}{3}} d_1^{-\frac{1}{2}} m \ln b(d_1) \ln\ln b(m)),$$

where d_0 and d_1 are special coprime factors of d, $d_0 d_1 = d$, $b(d_1)$ and $b(m)$ are the products of distinct prime factors respectively of d_1 and m.

In the present talk we consider some important classes of the quaternary forms and give the corresponding estimates for $\rho(f,m)$, which sharpen the previous estimates.

References

[1] G. P. Gogishvili, *The summation of a singular series that is connected with diagonal quadratic forms with four variables* (Russian) Trudy Tbilis. Mat. Inst. Razmadze, 38 (1970), 5-30.

[2] G. Gogishvili, *New estimates of the singular series corresponding to positive quaternary quadratic forms* Georgian Mathematical Journal, 13 (2006), Number 4, 687-691.

[3] A. Malyshev, *On the representation of integers by positive quadratic forms* (Russian) Trudy Mat. Inst. Steklov, 65 (1962), 212 pp.

A weighted zero-sum problem with quadratic residues

David J. Grynkiewicz

University of Memphis

diambri@hotmail.com

Coauthors: François Hennecart

Given a ring R and a subset $A \subseteq R$, the A-weighted Davenport constant is the least integer $\mathsf{D}_A(G)$ such that any sequence of terms from R of length $\mathsf{D}_A(R)$ has a nontrivial subsequence $g_1 \cdot \ldots \cdot g_\ell$, where the $g_i \in R$ are the terms of the subsequence, such that

$$0 = a_1 g_1 + \ldots + a_\ell g_\ell$$

for some $a_i \in A$. When $A = \{1\}$, this gives the usual Davenport Constant studied in Combinatorial Number Theory. We discuss the ring $R = \mathbb{Z}/n\mathbb{Z}$ with weight set $U_n^2 = \{u^2 : u \in U_n\}$, the set of all squares of invertible elements. Extending results of Adhikari, David and Urroz and of Chintamani and Moriya, we determine that $\mathsf{D}_{U_n^2}(\mathbb{Z}/n\mathbb{Z}) = 2\Omega(n) + 1$ when $\gcd(n, 10) = 1$ or $\gcd(n, 6) = 1$, where $\Omega(n)$ counts the number of prime divisors of n with multiplicity, and give a slightly larger upper bound for general odd n divisible by both 5 and 3. Surprisingly, the proof involves using a counter-example to the result to construct a pairwise balanced block design with $\lambda = 1$ having parameters for which no such design exists.

On the complexity of a family of Legendre sequences with irreducible polynomials

Katalin Gyarmati
Eötvös Loránd University
gykati@cs.elte.hu

In crypthography one often needs large families of binary sequences. First Goubin, Mauduit and Sárközy succeeded in constructing large families of pseudorandom binary sequences with proved strong pseudorandom properties. The construction studied by them was the following:

Construction. *Let $K \geq 1$ be an integer and p be a prime number. If $f \in \mathbb{F}_p[x]$ is a polynomial with degree $1 \leq k \leq K$ and no multiple zero in $\overline{\mathbb{F}_p}$, then define the binary sequence $E_p(f) = E_p = (e_1, \ldots, e_p)$ by*

$$e_n = \begin{cases} \left(\frac{f(n)}{p}\right) & \text{for } (f(n), p) = 1 \\ +1 & \text{for } p \mid f(n). \end{cases} \tag{1}$$

Let $\mathcal{F}(K, p)$ denote the set of all sequences obtained in this way.

Goubin, Mauduit and Sárközy proved that under certain not too restrictive conditions on the polynomial f, the sequences constructed in this way have strong pseudorandom properties. Since then many other families have been constructed, but still this seems to be the most satisfactory construction.

In many applications of cryptography it is not enough to know that the family contains many binary sequences with strong pseudorandom properties; it is also important that the family has a "rich", "complex" structure, there are many "independent" sequences in it. Ahlswede, Khachatrian, Mauduit and Sárközy introduced the f-complexity measure ("f" for family) in order to study pseudorandom properties of large families of binary sequences. This measure was the following:

Definition. The f-complexity of a family $\mathcal{F}$ of binary sequences $E_N \in \{-1, +1\}^N$ is defined as the greatest integer j so that for any $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_j) \in \{-1, +1\}^j$ and for any $i_1, i_2, \ldots, i_j \in \mathbb{Z}$ with $1 \leq i_1 < i_2 < \cdots < i_j \leq N$ there is at least one $E_N = (e_1, e_2, \ldots, e_N) \in \mathcal{F}$ for which

$$e_{i_1} = \varepsilon_1, \ e_{i_2} = \varepsilon_2, \ldots, e_{i_j} = \varepsilon_j.$$

The f-complexity of $\mathcal{F}$ is denoted by $\Gamma(F)$. (If there is no $j \in \mathbb{N}$ with the property above, then we set $\Gamma(\mathcal{F}) = 0$.)

Ahlswede, Khachatrian, Mauduit and Sárközy observed that

$$\Gamma(\mathcal{F}) \leq \frac{\log |\mathcal{F}|}{\log 2}$$

Using this we get

$$\Gamma(\mathcal{F}(K,p)) \le \frac{K}{\log 2}\log p + 1.$$

In 2009 I proved the following:

Theorem 1.

$$\Gamma(\mathcal{F}(K,p)) \ge \frac{K-1}{2\log 2}\log p - O(K\log(K\log p)). \tag{2}$$

In this talk, answering a question of Gábor Halász I will prove a sharpening of Theorem 1: The bound in (2) is optimal apart from constant factor only for $K \le p^{1/2}$ (because of the error term $O(K\log(K\log p))$). However in certain applications it is also important that we can achieve the optimal bound for families $\mathcal{F}(K,p)$ for larger K's. In order to achieve this I will restrict $\mathcal{F}(K,p)$ to a certain subfamily of it which contains sequences with even stronger pseudorandom properties but its f-complexity measure is still optimal even for very large K's. I propose the use of irreducible polynomials:

Definition. Define $E_p(f)$ by (1). Let

$$\mathcal{F}_{irred}(k,p) = \{E_p(f) : f \text{ is monic irreducible polynomial over } \mathbb{F}_p, \\ \deg\ f = k\}.$$

In the present talk I will prove that the f-complexity measure of $\mathcal{F}_{irred}(k,p)$ is optimal apart from constant factor:

Theorem 2. *Let p be an odd prime and k be a positive integer. Define $c = 1/2$ if $k \le \frac{p^{1/4}}{10\log p}$ and $c = 5/2$ if $k > \frac{p^{1/4}}{10\log p}$ then*

$$\Gamma(\mathcal{F}_{irred}(k,p)) \ge \min\left\{p,\ \frac{k-c}{2\log 2}\log p\right\}. \tag{3}$$

This theorem shows that $\mathcal{F}_{irred}(k,p)$ can be very useful in the applications: Following from an earlier result of Goubin, Mauduit and Sárközy for $k = o(\frac{p^{1/2}}{\log p})$ every sequence in it has strong pseudorandom properties and by Theorem 2 for every k it has optimal f-complexity measure. Since $\mathcal{F}(K,p) \supset \mathcal{F}_{irred}(K,p)$ thus we also have

Corollary. *Let p be an odd prime and K be an integer. Define $c = 1/2$ if $K \le \frac{p^{1/4}}{10\log p}$ and $c = 5/2$ if $K > \frac{p^{1/4}}{10\log p}$ then*

$$\Gamma(\mathcal{F}(K,p)) \ge \min\left\{p,\ \frac{K-c}{2\log 2}\log p\right\}.$$

This theorem considerably improves on Theorem 1 and it is optimal apart from constant factor for every K and not only for small K's. The proof uses character sums over finite fields.

On properties of the r-Dowling polynomials

Eszter Gyimesi

University of Debrecen

gyimesie@science.unideb.hu

Coauthors: Gábor Nyul

As a generalization of T. A. Dowling's Whitney numbers, I. Mező introduced r-Whitney numbers. If $W_{m,r}(n,k)$ denotes an r-Whitney number of the second kind, then we can define r-Dowling polynomials as $D_{n,m,r}(x) = \sum_{k=0}^{n} W_{m,r}(n,k)x^k$. Since r-Whitney numbers are in fact generalizations of Stirling numbers, r-Dowling polynomials can be viewed as generalizations of Bell polynomials.

Our recently given combinatorial interpretation of r-Whitney numbers allows us to study them and the r-Dowling polynomials from a completely new viewpoint, this way we could prove many unknown identities for them. In our talk, we will survey the previously known properties, and present our new results.

The transformations of a series in function fields

Yoshinori Hamahata

Okayama University of Science

hamahata@xmath.ous.ac.jp

Let

$$\eta(z) = e^{\pi iz/12}\prod_{n=1}^{\infty}\left(1-e^{2\pi inz}\right) \qquad (\mathrm{Im}(z)>0)$$

be the Dedekind η-function. R. Dedekind described the transformation of $\log\eta(z)$ under the substitution $z' = (az+b)/(cz+d)$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. To be more exact, he proved that for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ with $a \neq 0, c > 0$,

$$\log\eta\left(\frac{az+b}{cz+d}\right) = \log\eta(z) + \frac{1}{2}\log\left(\frac{cz+d}{i}\right) + \frac{\pi i(a+d)}{12c} - \pi i D(a,c), \tag{1}$$

where $D(a,c)$ is the Dedekind sum defined by

$$D(a,c) = \frac{1}{4c}\sum_{k=1}^{c-1}\cot\left(\frac{\pi ak}{c}\right)\cot\left(\frac{\pi k}{c}\right)$$

for coprime integers a and $c>0$. We can use (1) to prove the so-called reciprocity law given by

$$D(a,c)+D(c,a) = -\frac{1}{4}+\frac{1}{12}\left(\frac{a}{c}+\frac{c}{a}+\frac{1}{ac}\right)$$

for coprime positive integers a and c.

An analogy exists between number fields and function fields. For example, $A := \mathbb{F}_q[T], K := \mathbb{F}_q(T)$, and $K_\infty := \mathbb{F}_q((1/T))$ are analogous to $\mathbb{Z}, \mathbb{Q}$, and $\mathbb{R}$, respectively. A few years ago, we introduced a function field analog $s(a,c)$ of $D(a,c)$, and established its reciprocity law. In this

talk, we use the Dedekind sum $s(a,c)$ in function fields to describe the transformation of a certain series under the substitution $z' = (az+b)/(cz+d)$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(A)$.

New asymptotic irrationality measure for e and other numbers

Jaroslav Hančl

University of Ostrava

hancl@osu.cz

Coauthors: Ondřej Kolouch, Tapani Matala-aho, Marko Leinonen, Kalle Leppälä

Let α be a real number and set $J_\alpha(N) = N\|N\alpha\|$ where $\|\alpha\|$ denotes the distance from α to the nearest integer. For the Napier's constant e we prove that there exists a positive constant C such that

$$J_e(N) > \frac{\log(\frac{4}{e}\log N) - \log\log(\frac{4}{e}\log N) + \frac{\log\log(\frac{4}{e}\log N)}{\log(\frac{4}{e}\log N)} + \frac{\log^2\log(\frac{4}{e}\log N)}{\log^2(\frac{4}{e}\log N)} - C(\frac{\log\log\log N}{\log^2\log N})}{2\log N}$$

for all big enough integers N and for infinitely many values of N we have

$$J_e(N) < \frac{\log(\frac{4}{e}\log N) - \log\log(\frac{4}{e}\log N) + \frac{\log\log(\frac{4}{e}\log N)}{\log(\frac{4}{e}\log N)} + \frac{\log^2\log(\frac{4}{e}\log N)}{\log^2(\frac{4}{e}\log N)} + C(\frac{\log\log\log N}{\log^2\log N})}{2\log N}.$$

Similarly we obtain results for certain powers of e, $\tanh 1$ and a ratio of modified Bessel functions.

Various extensions of Chen's theorems

Stijn S.C. Hanson

Australian National University

stijnhanson@gmail.com

In 1973, Jingrun Chen proved that every sufficiently large even number N can be written as a sum of a prime and a number with no more than two prime factors. In an almost identical proof, he also showed that there are infinitely many primes p such that $p+2$ contains no more than two prime factors. In this talk I will describe some work-in-progress on both of these problems, building on the work of Cai; Heath-Brown; and Li.

A problem in non-linear Diophantine approximation

Stephen Harrap

University of Durham

s.g.harrap@durham.ac.uk

Coauthors: Simon Kristensen, Mumtaz Hussain

Metric Diophantine approximation of a single linear form is in a first instance concerned with the (Lebesgue and Hausdorff) measure of the set of real vectors $(x_1,\dots,x_n) \in \mathbb{R}^n$ for which there are infinitely many integer vectors $(q_1,\dots,q_n,p) \in \mathbb{Z}^{n+1}$ satisfying the inequality

$$|q_1x_1 + \cdots + q_nx_n - p| < \psi(H(\mathbf{q})). \tag{1}$$

Here, $\psi : \mathbb{N} \to \mathbb{R}_{>0}$ denotes a monotonic arithmetic function decreasing to zero and $H(\mathbf{q})$ denotes the naive height of the vector $\mathbf{q}$; i.e. $H(\mathbf{q}) = \max\{|q_1|,\dots,|q_n|\}$. The set is well studied. Its Lebesgue measure was given by the famous zero–one law of Groshev in 1938 and its Hausdorff

measure was calculated by Dickinson & Velani in 1997. If one restricts the set of real numbers by putting restrictions on the set of integer vectors for which (1) is required to have infinitely many solutions, the problem is less studied. In this talk I discuss some new Lebesgue and Hausdorff measure results for the set of vectors satisfying infinitely many fully non-linear Diophantine inequalities. The set in question is also associated with a class of linear inhomogeneous partial differential equations whose solubility is related to a certain Diophantine condition. The failure of the Diophantine condition guarantees the existence of a smooth solution.

Obstructions to local-global principles for torsors

Julia Hartmann

University of Pennsylvania

hartmann@math.uppen.edu

Local-global principles in algebra and number theory are motivated by analogous principles in geometry, by which certain properties of a space can be detected locally. Torsors often classify algebraic structures, and local-global principles for torsors provide such principles for the corresponding structures (e.g. quadratic forms and central simple algebras).

Classically, this has been studied in the case of global fields (number fields and function fields over finite fields). This talk, on recent and ongoing work with David Harbater and Daniel Krashen, will focus on the case of semi-global fields (one-variable function fields over complete discretely valued fields, e.g. p-adic function fields). Obstructions to the corresponding local-global principles can be measured by a variant of the Tate-Shafarevich group, and we are interested in properties such as finiteness and triviality.

Permutations destroying arithmetic progressions in finite cyclic groups

Peter Hegarty

Chalmers University of Technology, University of Gothenburg

hegarty@chalmers.se

Coauthors: Anders Martinsson

Let G be an abelian group, S a subset of G, $f : S \to S$ a function and $\mathcal{L}$ a linear equation with integer coefficients. We say the function f *destroys* the arithmetic pattern $\mathcal{L}$ if, whenever $(s_1, \ldots, s_k) \in S^k$ is a non-trivial solution to $\mathcal{L}$, then $(f(s_1), \ldots, f(s_k))$ is not a solution to $\mathcal{L}$. Perhaps the most natural yet interesting cases are: $\mathcal{L} : x + y - 2z = 0$ (3-term APs), f is a permutation and either $G = \mathbb{Z}$, $S = \mathbb{N}$ or $G = \mathbb{Z}_n$. The study of such functions was initiated by myself in a paper 11 years ago [1] (and presented at JA in 2003). I will describe what is currently known and present some recent progress on perhaps the stand-out conjecture from [1], which states that a permutation of $\mathbb{Z}_n$ destroying 3-term APs exists if and only if $n \notin \{2, 3, 5, 7\}$. We can now prove that such a permutation exists if $n \geq 138474903511296$!!

References

[1] P. Hegarty, *Permutations avoiding arithmetic patterns*, Electron. J. Combin. **11** (2004), Paper #39, 21

The ternary Goldbach conjecture

Harald Andres Helfgott

Paris VI/VII

harald.helfgott@gmail.com

The ternary Goldbach conjecture (1742) asserts that every odd number greater than 5 can be written as the sum of three prime numbers. Following the pioneering work of Hardy and Littlewood, Vinogradov proved (1937) that every odd number larger than a constant C satisfies the conjecture. In the years since then, there has been a succession of results reducing C, but only to levels much too high for a verification by computer up to C to be possible ($C > 10^{1300}$). My work proves the conjecture. We will go over the main ideas in the proof.

Diophantine equations in dense variables

Kevin Henriot

University of British Columbia

khenriot@math.ubc.ca

We discuss the problem of finding solutions to certain translation-invariant diophantine equations in sparse subsets of integers. We are initially interested in the diagonal system

$$\lambda_1 x_1 + \cdots + \lambda_s x_s = 0,$$
$$\lambda_1 x_1^2 + \cdots + \lambda_s x_s^2 = 0,$$

where the λ_i are non-zero integer coefficients such that $\lambda_1 + \cdots + \lambda_s = 0$. Under slight non-degeneracy conditions, this system possesses non-trivial solutions in any subset of $\{1, \ldots, N\}$ of density at least $(\log N)^{-c}$. Our approach to this problem relies on the circle method, the energy increment strategy from additive combinatorics, and the restriction phenomenon from harmonic analysis. We explain how this framework can be extended to cover more general systems.

Extremality of the completely multiplicative functions

Titus Hilberdink

University of Reading

t.w.hilberdink@reading.ac.uk

In many optimization problems involving quadratic forms where there is some multiplicative structure, there seems to be a tendency for the optimal to appear at a 'multiplicative' point. We investigate when this happens and suggest some reasons for this phenomenom, by looking at the geometrical nature of the square-summable completely multiplicative functions.

Harmonic analysis on the space of p-adic unitary hemitian matrices

Yumiko Hironaka

Waseda University

hironaka@waseda.jp

Coauthors: Yasushi Komori

Let k'/k be an unramified quadratic extension of p-adic fieds, consider hermitian and unitary matrices with respect to k'/k. Denote by $a^* \in M_{nm}(k')$ the conjugate transpose of a matrix $a \in M_{mn}(k')$ and by j_m the matrix whose all anti-diagonal entries are 1 and others are 0 in

$GL_m(k')$. Set

$$
\begin{aligned}
&G = U(j_m) = \left\{ g \in GL_m(k') \;\middle|\; g j_m g^* = j_m \right\}, \quad K = G(\mathcal{O}_{k'}),\\
&X = \left\{ x \in G \mid x^* = x,\ \Phi_{x j_m}(t) = \Phi_{j_m}(t) \right\},\\
&(\Phi_y(t) \text{ is the characteristic polynomial of matrix } y)\\
&g \cdot x = g x g^*, \quad (g \in G,\ x \in X).
\end{aligned}
$$

We analyse the G-space X on the basis of *spherical functions* on X, which are K-invariant common eigenfunctions on X with respect to Hecke algebra $\mathcal{H}(G, K)$.

The above action $\cdot$ of G can be continued to the algebraic group $G(\overline{k})$ and the space X can be regarded as the set of k-rational point of $G(\overline{k}) \cdot j_m$.

The Weyl group W of G is isomorphic to $S_n \ltimes \{\pm 1\}^n$ and the root structure of G is of type C_n if $m = 2n$ and BC_n if $m = 2n + 1$, where $n = \left[\frac{m}{2}\right]$.

In the following we assume that k has odd residual characteristic (cf. Remark at the end). Denote by π the prime element of k and by q the cardinality of the residue class field of k.

Theorem. (Cartan decomposition) *The K-orbits in X are parametrized by*

$$\Lambda_n^+ = \left\{ \lambda \in \mathbb{Z}^n \mid \lambda_1 \geq \cdots \geq \lambda_n \geq 0 \right\},$$

and represented by

$$x_\lambda = Diang(\pi^{\lambda_1}, \ldots, \pi^{\lambda_n}, (1), \pi^{-\lambda_n}, \ldots, \pi^{-\lambda_1}) \in X$$

for each λ.

For $x \in X$ and $s \in \mathbb{C}^n$, we consider the following integral

$$\omega(x; s) = \int_K \prod_{i=1}^{n} |d_i(k \cdot x)|^{s_i} \, dk, \tag{1}$$

where $d_i(y)$ as the determinant of the lower right i by i block of y and dk is the Haar measure on K. The right hand side is absolutely convergent if $\Re(s_i) \geq 0,\ 1 \leq i \leq n$, and continued to a rational function of $q^{s_i},\ 1 \leq i \leq n$. Let B be the Borel subgroup of G consisting of upper triangular matrices. Since $d_i(x)$ is a relative B-invariants on X associated with character $\psi_i(p) = N_{k'/k}(d_i(p))$ of B, we see $\omega(x; s)$ is a spherical function on X which satisfies

$$
\begin{aligned}
&f * \omega(x; s) = \lambda_s(f) \omega(x; s),\\
&\lambda_s(f) = \textstyle\int_B f(p) \prod_{i=1}^{n} |\psi_i(p)|^{-s_i} \, \delta(p) dp, \quad (f \in \mathcal{H}(G, K))
\end{aligned}
\tag{2}
$$

where dp is the left invariant measure on B with modulus character δ. We introduce the new variable $z \in \mathbb{C}^n$ related to s by

$$
\begin{aligned}
&s_i = -z_i + z_{i+1} - 1 + \tfrac{\pi\sqrt{-1}}{\log q} \ \ (i < n),\\
&s_n = \begin{cases} -z_n - \frac{1}{2} + \frac{\pi\sqrt{-1}}{\log q} & (m = 2n)\\ -z_n - 1 + \frac{\pi\sqrt{-1}}{2 \log q} & (m = 2n + 1), \end{cases}
\end{aligned}
\tag{3}
$$

and write $\omega(x; z) = \omega(x; s)$.

As for roots, set $\Sigma_s^+ = \{ e_i \pm e_j \mid 1 \le i < j \le n \}$, $\Sigma_\ell^+ = \{ 2e_i \mid 1 \le i \le n \}$ and $\Sigma^+ = \Sigma_s^+ \cup \Sigma_\ell^+$, where e_i is the i-th unit vector in $\mathbb{Z}^n$ and $\langle \alpha, z \rangle = \sum_{i=1}^n \alpha_i z_i$ for $\alpha \in \mathbb{Z}^n$ and $z \in \mathbb{C}^n$.

Using a general expression formula (cf. [1] Theorem 2.5), we obtain the following explicit formula.

Theorem. (Explicit formula) *For each $\lambda \in \Lambda_n^+$, one has*

$$\omega(x_\lambda; z) = c_n \cdot \prod_\alpha \frac{1 - q^{\langle \alpha, z-1 \rangle}}{1 + q^{\langle \alpha, z \rangle}} \cdot q^{\langle \lambda, z_0 \rangle} \cdot Q_\lambda(z; t),$$

where c_n is an explicitly given constant depending on the parity of m, α runs over the set Σ_s^+ for even m and Σ^+ for odd m,

$$Q_\lambda(z;t) = \sum_{\sigma \in W} \sigma \left(q^{-\langle \lambda, z \rangle} c(z;t) \right), \quad c(z;t) = \prod_{\alpha \in \Sigma^+} \frac{1 - t_\alpha q^{\langle \alpha, z \rangle}}{1 - q^{\langle \alpha, z \rangle}}$$

$$t_\alpha = \begin{cases} t_s & \text{if } \alpha \in \Sigma_s^+ \\ t_\ell & \text{if } \alpha \in \Sigma_\ell^+, \end{cases} \qquad t_s = -q^{-1}, \quad t_\ell = \begin{cases} q^{-1} & \text{if } m = 2n \\ -q^{-2} & \text{if } m = 2n+1. \end{cases}$$

We see $Q_\lambda(z;t)$ is Hall-Littlewood polynomial of type C_n up to constant multiple, belongs to $\mathcal{R} = \mathbb{C}[q^{\pm z_1}, \ldots, q^{\pm z_n}]^W$, and forms an orthogonal $\mathbb{C}$-basis when λ runs over Λ_n^+ (for $t_\alpha \in \mathbb{R}$ with $|t_\alpha| < 1$) (cf. [2]-Appendix, [4]).

Theorem. *(1) The spherical Fourier transform*

$$\widehat{\ } : \mathcal{S}(K \backslash X) \longrightarrow \mathcal{R}, \ \varphi \longmapsto \widehat{\varphi}(z) = \int_X \varphi(x) \Psi(x; z) dx$$

$$(\Psi(x;z) = \frac{\omega(x;z)}{\omega(1_m; z)}, \ \ dx \text{ is a } G\text{-invariant measure})$$

is an $\mathcal{H}(G,K)$-module isomorphism, and $\mathcal{S}(K\backslash X)$ is a free $\mathcal{H}(G,K)$-module of rank 2^n.

(2) *The set $\left\{ \Psi(x; z+u) \,\middle|\, u \in \{0, \pi\sqrt{-1}/\log q\}^n \right\}$ forms a basis of spherical functions on X corresponding to z via λ_z.*

(3) (Plancherel formula) *Set the measure $d\mu(z)$ on $\mathfrak{a}^* = \left(\sqrt{-1} \left(\mathbb{R} / \frac{2\pi}{\log q} \mathbb{Z} \right) \right)^n$ by*

$$d\mu(z) = \frac{1}{2^n n!} \frac{w_n(-q^{-1}) w_{m'}(-q^{-1})}{(1+q^{-1})^{m'}} \cdot \frac{1}{c(z;t)} dz,$$

$$w_r(t) = \prod_{i=1}^r (1 - t^i), \ m' = \left[\frac{m+1}{2} \right].$$

Then, by an explicitly given normalization of dx depending on the parity of m, one has

$$\int_X \varphi(x) \overline{\psi(x)} dx = \int_{\mathfrak{a}^*} \widehat{\varphi}(z) \overline{\widehat{\psi}(z)} d\mu(z) \quad (\varphi, \psi \in \mathcal{S}(K\backslash X)).$$

(4) (Inversion formula) *For $\varphi \in \mathcal{S}(K\backslash X)$, one has*

$$\varphi(x) = \int_{\mathfrak{a}^*} \widehat{\varphi}(z) \Psi(x; z) d\mu(z), \ x \in X.$$

Remark. If k is dyadic, X has K-orbits without any diagonal elements. Nevertheless we have the similar results when $k = \mathbb{Q}_2$ and m is even. The spherical function $\omega(x; s)$ for even m has a close relation to hermitian p-adic Siegel singular series.

References

[1] Y. Hironaka *Spherical functions on p-adic homogeneous spaces*, "Algebraic and Analytic Aspects of Zeta Functions and L-functions", MSJ Memoirs **21** (2010), 50-72.
[2] Y. Hironaka and Y. Komori *Spherical functions on the space of p-adic unitary hermitian matrices*, Int. J. Number Theory, **10** (2014), 513-558.
[3] Y. Hironaka and Y. Komori *Spherical functions on the space of p-adic unitary hermitian matrices II, the case of odd size*, Commentarri Mathematici Univ. Sancti Pauli, **63** (2014), 47-78.
[4] I. G. Macdonald *Orthogonal polynomials associated with root systems*, Séminaire Lotharingien de Combinatoire **45** (2000), Article B45a.

Deterministic integer factorization via polynomials over $\mathbb{Z}$

Markus Hittmeir
UniversitÃdt Salzburg
markus.hittmeir@sbg.ac.at

Let $N \in \mathbb{N}$ be a composite number. In this talk we discuss the problem of constructing polynomials $f \in \mathbb{Z}[X]$ such that as many $x \in \mathbb{Z}$ as possible satisfy $1 < \gcd(f(x), N) < N$. We present an optimal solution, which leads to a deterministic factorization algorithm with the complexity $\mathcal{O}(N^{1/4+\epsilon})$. Strassen's well known factorization method turns out to be a special case of this algorithm. We also talk about related open problems and the possibility to improve the bound.

On the simplest number fields and related Thue equations

Akinari Hoshi
Niigata University
hoshi@math.sc.niigata-u.ac.jp

Let $m \geq -1$ be an integer. In [1], a correspondence between integer solutions to the parametric family of cubic Thue equations

$$X^3 - mX^2Y - (m+3)XY^2 - Y^3 = \lambda,$$

where $\lambda > 0$ is a divisor of $m^2 + 3m + 9$, and isomorphism classes of the simplest cubic fields is given. By this correspondence and R. Okazaki's result which claims that the simplest cubic fields are non-isomorphic to each other except for $m = -1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389$, we obtain exactly 66 non-trivial solutions with $xy(x+y) \neq 0$ to the cubic Thue equations for positive divisors λ of $m^2 + 3m + 9$. As a consequence of the correspondence, we also get another proof of Okazaki's result.

I will talk about a generalization of the cubic case to the quartic and sextic cases.

References

[1] Akinari Hoshi, *On correspondence between solutions of a family of cubic Thue equations and isomorphism classes of the simplest cubic fields*, J. Number Theory **131** (2011) 2135–2150.
[2] Akinari Hoshi, *On the simplest sextic fields and related Thue equations*, Funct. Approx. Comment. Math. **47** (2012) 35–49.

Only finitely many Tribonacci Diophantine triples exist

Christoph Hutle
University of Salzburg
christoph.hutle@sbg.ac.at
Coauthors: Florian Luca, Nurettin Irmak, Laszlo Szalay

One of the oldest problems in Number Theory is the question of Diophantus, which is about constructing sets of rationals or integers with the property that the product of any two of its distinct elements plus 1 is square. Recently several variations of this problem have been investigated. The problem of finding bounds on the size m for Diophantine m-tuples with values in linear recurrences is one such variation.

In this talk, we will consider the Tribonacci sequence $\{T_n\}_{n\geq 0}$ given by $T_0 = T_1 = 0,\ T_2 = 1$ and $T_{n+3} = T_{n+2} + T_{n+1} + T_n$ for all $n \geq 0$. We show that there exist only finitely many Diophantine triples with values in $\{T_n\}_{n\geq 0}$. By C. A. Gomez Riuz and F. Luca, it is already known, that there are no Diophantine quadruples with values in the Tribonacci sequence.

The proof is not constructive, since it is based on a version of the Subspace Theorem, one of the most important results in Diophantine Approximation. So it does neither give an upper bound on the number of solutions nor an algorithm to find them.

Distribution of integral division points on the algebraic torus

Su-ion Ih
University of Colorado at Boulder
ih@math.colorado.edu
Coauthors: Philipp Habegger

I will talk about the distribution of heights of integral division points on the algebraic torus.

Some mean value results for the zeta-function and a divisor problem

Aleksandar Ivić
Serbian Academy of Sciences
aivic_2000yahoo.com
Coauthors: Wenguang Zhai

Let $d(n)$ be the number of divisors of n, $\gamma = -\Gamma'(1)$ be Euler's constant, let

$$\Delta(x) := \sum_{n\leq x} d(n) - x(\log x + 2\gamma - 1)$$

denote the error term in the classical Dirichlet divisor problem, and let $\zeta(s)$ denote the Riemann zeta-function. It is shown that

$$\int_0^T \Delta(t)|\zeta(\tfrac{1}{2} + it)|^2\,dt \ll T(\log T)^4.$$

Further, if $2 \leq k \leq 8$ is a fixed integer, then we prove the asymptotic formula

$$\int_1^T \Delta^k(t)|\zeta(\tfrac{1}{2} + it)|^2\,dt = c_1(k)T^{1+\frac{k}{4}}\log T + c_2(k)T^{1+\frac{k}{4}} + O_\varepsilon(T^{1+\frac{k}{4}-\eta_k+\varepsilon}),$$

where $c_1(k)$ and $c_2(k)$ are explicit constants, and where

$$\eta_2 = 3/20, \eta_3 = \eta_4 = 1/10,$$

$$\eta_5 = 3/80,\ \eta_6 = 35/4742,\ \eta_7 = 17/6312,\ \eta_8 = 8/9433.$$

The results depend on the power moments of $\Delta(t)$ and $E(T)$, the classical error term in the asymptotic formula for the mean square of $|\zeta(\frac{1}{2}+it)|$. The work is a continuation of [1] and [2], preprint available at `arXiv:1502.00406`.

References

[1] A. Ivić, *On some mean value results for the zeta-function and a divisor problem*, to appear in Filomat, preprint available at `arXiv:1406.0604`.

[2] W. Zhai, *On higher-power moments of* $\Delta(x)$, Acta Arith. **112** (2004), 367-395; II. ibid. **114** (2004), 35-54; III ibid. **118** (2005), 263-281, and IV, Acta Math. Sinica, Chin. Ser. **49** (2006), 639-646.

Computing relative power integral bases in a family of quartic extensions of imaginary quadratic fields

Borka Jadrijević

University of Split

`borka@pmfst.hr`

Coauthors: Zrinka Franušić

Let M be an imaginary quadratic field with ring of integers $\mathbb{Z}_M$. Let ξ be a root of the polynomial

$$f(x) = x^4 - 2cx^3 + 2x^2 + 2cx + 1,\ c \in \mathbb{Z}_M,\ c \neq 0.$$

We consider an infinite family of octic fields $K_c = M(\xi)$ with ring of integers $\mathbb{Z}_{K_c}$. Since the integral basis of K_c is not known in a parametric form, our goal is to determine all generators of the relative power integral basis of $\mathcal{O} = \mathbb{Z}_M[\xi]$ over $\mathbb{Z}_M$ (instead of $\mathbb{Z}_{K_c}$ over $\mathbb{Z}_M$). We show that our problem reduces to solving the system of relative Pellian equations

$$cV^2 - (c+2)U^2 = -2\mu,\ cZ^2 - (c-2)U^2 = 2\mu,$$

where μ is an unit in M. We solve the system completely and find that all non-equivalent generators of the power integral basis of $\mathcal{O}$ over $\mathbb{Z}_M$ are given by $\alpha = \xi,\ 2\xi - 2c\xi^2 + \xi^3$ for $|c| \geq 159108$.

Simple linear equations in conjugates of a Pisot number

Jonas Jankauskas

University of Waterloo

Vilnius University

`jonas.jankauskas@gmail.com`

Coauthors: A. Dubickas, K. G. Hare

We show that the number $\alpha = (1+\sqrt{3+2\sqrt{5}})/2$ with minimal polynomial x^4-2x^3+x-1 is the only Pisot number whose four distinct conjugates $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ satisfy the additive relation $\alpha_1 + \alpha_2 = \alpha_3 + \alpha_4$. This implies that there exists no two non-real conjugates of a Pisot number with the same imaginary part and also that at most two conjugates of a Pisot number can have the same real part. On the other hand, we prove that similar four term equations $\pm\alpha_1+\alpha_2+\alpha_3+\alpha_4 = 0$ cannot be solved in conjugates of a Pisot number α. We also show that the roots of the Siegel's polynomial $x^3 - x - 1$ are the only solutions to the three term equation $\alpha_1 + \alpha_2 + \alpha_3 = 0$ in

conjugates of a Pisot number. It will be shown that similar ternary equation $\alpha_1 = \alpha_2 + \alpha_3$ has no solutions in conjugates of a Pisot number. In addition to this, all solutions to the three term equations $\alpha_1 = \alpha_2 + \alpha_3$ and $\alpha_1 + \alpha_2 + \alpha_3 = 0$ in conjugate algebraic numbers (not necessarily Pisot) of degree $d \leq 8$ will be described.

On the torsion of the Jacobians of two families of hyperelliptic curves

Tomasz Jędrzejak
University of Szczecin
tjedrzejak@gmail.com

Consider two families of hyperelliptic curves (over $\mathbb{Q}$) $C^{n,a} : y^2 = x^n + a$ and $C_{n,a} : y^2 = x(x^n + a)$, and their Jacobians $J^{n,a}$, $J_{n,a}$ respectively. We give the partial characterization of the torsion part of $J^{n,a}(\mathbb{Q})$ and $J_{n,a}(\mathbb{Q})$. More precisely, we show that the only prime factors of the orders of such groups are 2 and prime divisors of n (we also give the upper bounds for the exponents). Moreover, we give the complete description of the torsion part of $J_{8,a}(\mathbb{Q})$. Namely, we show that $J_{8,a}(\mathbb{Q})_{tors} = J_{8,a}(\mathbb{Q})[2]$.

The main ingredients in the proofs are explicit computations of zeta functions of these curves in some cases, which are of independent interest, and applications of the Chebotarev Density Theorem.

The distribution of class groups of imaginary quadratic fields

Nathan Jones
University of Illinois at Chicago
ncjones@uic.edu
Coauthors: S. Holmin, P. Kurlberg, C. Macleman, K. Petersen

Which abelian groups occur as the class group of some imaginary quadratic field? Inspecting tables of M. Watkins on imaginary quadratic fields of class number up to 100, one finds that some abelian groups do not occur as the class group of any imaginary quadratic field (for instance $(\mathbb{Z}/3\mathbb{Z})^3$ does not). In this talk, I will combine heuristics of Cohen-Lenstra together with a refinement of a conjecture of Soundararajan to make precise predictions about the asymptotic distribution of imaginary quadratic class groups, partially addressing the above question. I will also present some numerical evidence of the resulting conjectures.

Primitive Fricke families and their application to modular function fields

Ho Yun Jung
National Institute for Mathematical Sciences
hoyunjung@nims.re.kr
Coauthors: Koo, Shin

In this talk, we develop an equivalent condition for a primitive Fricke family of level N to be totally primitive when N is different from 4. Furthermore, we present generators of the function field of the modular curve of level N in terms of Fricke and Siegel functions. By using the functions belonging to Fricke families, we shall construct generators of the ray class fields over imaginary quadratic fields as an application of class field theory.

On the size of Diophantine m-tuples for linear polynomials

Ana Jurasić

University of Rijeka

ajurasic@math.uniri.hr

Coauthors: Alan Filipin

Diophantus of Alexandria was the first who studied the problem of finding sets with the property that the product of any two of its distinct elements increased by 1 is a perfect square. Such a set consisting of m elements is therefore called a Diophantine m-tuple. Diophantus found the first Diophantine quadruple consisting of rational numbers $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$, while the first Diophantine quadruple of integers, the set $\{1, 3, 8, 120\}$, was found by Fermat. In the case of rational numbers no upper bound for the size of such sets is known. In integer case which is the most studied, Dujella proved that there does not exist a Diophantine sextuple and there are only finitely many Diophantine quintuples. The folklore conjecture is that there does not exist a Diophantine quintuple over the integers. Many generalizations of this problem were also considered, for example by adding a fixed integer n instead of 1, looking at kth powers instead of squares, or considering the problem over other domains than $\mathbb{Z}$ or $\mathbb{Q}$.

Definition. Let $m \geq 2$, $k \geq 2$ and let R be a commutative ring with 1. Let $n \in R$ be a nonzero element and let $\{a_1, \ldots, a_m\}$ be a set of m distinct nonzero elements from R such that $a_i a_j + n$ is a kth power of an element of R for $1 \leq i < j \leq m$. The set $\{a_1, \ldots, a_m\}$ is called a kth power Diophantine m-tuple with the property $D(n)$ or simply a kth power $D(n)$-m-tuple in R.

Diophantus found the first such set, a second power $D(256)$-quadruple $\{1, 33, 68, 105\}$. The natural question (investigated by Dujella and other authors) is to find upper bounds for the number of elements of such sets.

The first polynomial variant of the above problem was studied by Jones for the case $R = \mathbb{Z}[X]$, $k = 2$ and $n = 1$. In this case, Dujella and Fuchs proved that there does not exist a second power Diophantine quintuple. There were also considered other variants of such a polynomial problem (by Dujella and Luca, Dujella and Jurasić and other authors). Dujella and Fuchs, jointly with Tichy and later with Walsh, considered the case $R = \mathbb{Z}[X]$, $k = 2$ and n is a linear polynomial from $\mathbb{Z}[X]$. They proved that in this case $m \leq 12$. Jurasić handled the case where n is a quadratic polynomial in $\mathbb{Z}[X]$ and proved that in this case $m \leq 98$.

We considered the case $R = \mathbb{K}[X]$, where $\mathbb{K}$ is any field of characteristic 0, $k = 2$ and n is a linear polynomial from $\mathbb{K}[X]$. Without loss of generality we assumed that $\mathbb{K}$ is algebraically closed. Notice that if $\mathbb{K}$ is a field of characteristic $p \neq 0$, then if α is a root of a polynomial $f \in \mathbb{K}[X]$ it is also α^p. In that case we could not obtain some results where the factorisation of a polynomial is considering. In case of R a polynomial ring it is usually assumed that, for constant n, not all polynomials $a_1, a_2, ..., a_m$ are constant. For linear n this condition is trivially satisfied. Moreover, at most one polynomial a_i for $i \in \{1, ..., m\}$ in such a polynomial $D(n)$-m-tuple is constant. Otherwise, we would have two different constants a and b for which $ab + n = r^2$, where $r \in \mathbb{K}[X]$. It is not possible, because then $\deg(n) = 1 = 2\deg(r)$.

We intended to prove that $m < \infty$, i.e. we wanted to find some good upper bound for m. For brevity, instead of second power $D(n)$-m-tuple in $\mathbb{K}[X]$, we refer to a polynomial $D(n)$-m-tuple. We have the following theorem.

Theorem. *There are at most* 16 *elements in a polynomial $D(n)$-m-tuple for a linear polynomial*

n, *i.e.*

$$m \leq 16.$$

In the proof of this Theorem, we follow the strategy used for linear and quadratic n in the ring $\mathbb{Z}[X]$. In those investigations the relation "$<$" between the elemsnts of $\mathbb{Z}[X]$ was used. Instead of that, in $\mathbb{K}[X]$ we have to use the relation "$\leq$" between the degrees of its elements. We first estimate the number of polynomials with given degree k in a polynomial $D(n)$-m-tuple and consider separate cases depending on k. Then, we adapt the gap principle for the degrees of the elements of a polynomial $D(n)$-m-tuple, proved by Dujella, Fuchs and Tichy for the ring $\mathbb{Z}[X]$, to $\mathbb{K}[X]$. Combining those results with an upper bound for the degree of the largest element in a polynomial $D(n)$-quadruple, obtained by Dujella, Fucshs and Walsh for $\mathbb{Z}[X]$ and also valid in $\mathbb{K}[X]$, we finally prove the Theorem.

References

[1] A. Dujella, C. Fuchs, R. F. Tichy: *Diophantine m-tuples for linear polynomials*, Period. Math. Hungar. **45** (2002), 21-33.

[2] A. Dujella, C. Fuchs, G. Walsh: *Diophantine m-tuples for linear polynomials. II. Equal degrees*, J. Number Theory, **120** (2006), 213-228.

[3] A. Jurasić: *Diophantine m-tuples for quadratic polynomials*, Glas. Mat. Ser. III, **46** (2011), 283-309.

On open problems by Lind and by Taussky-Todd

Norbert Kaiblinger

University of Natural Resources and Life Sciences

norbert.kaiblinger@boku.ac.at

Lind's problem is a finite analogue of Lehmer's problem on integer polynomials of minimal Mahler measure. Taussky-Todd's problem is concerned with circulant determinants. We show the relation between these open problems. It leads us to a remark by Jacobi on his biquadratic analogue of Fermat's two squares theorem.

Arithmetical properties of power series related to β-expansion

Hajime Kaneko

Tsukuba University

kanekoha@math.tsukuba.ac.jp

The notion of the β-expansions of real numbers, which was introduced by Rényi in 1957, has important roles in various areas. However, it is generally difficult to investigate the digits in the β-expansions of given real numbers. For instance, Borel conjectured for every integer $b \geq 2$ that any algebraic irrational number is normal in base-b, which is still open.

In our talk, we consider the case where β is a Pisot or Salem number. First, we give lower bounds for the numbers of nonzero digits in the β-expansions of algebraic numbers. Consequently, we obtain criteria for the transcendence of certain power series at algebraic points. Moreover, we study further properties such as algebraic independence and linear independence over $\mathbb{Q}(\beta)$.

Constructing abelian varieties providing solutions to the inverse Galois problem for symplectic groups

Valentijn Karemaker

Utrecht University

V.Z.Karemaker@uu.nl

Coauthors: S. Arias-de-Reyna, C. Armana, L. Thomas, M. Rebolledo, N. Vila

Given a prime number ℓ, we show how to construct a three-dimensional abelian variety $A/\mathbb{Q}$ such that the attached Galois representation $\rho_{A,\ell}\colon G_{\mathbb{Q}} \to \mathrm{GSp}(A[\ell]) \cong \mathrm{GSp}(6,\mathbb{F}_\ell)$ is surjective. This provides an explicit solution to the inverse Galois problem for the symplectic groups $\mathrm{GSp}(6,\mathbb{F}_\ell)$.

The representation $\rho_{A,\ell}$ is surjective if its image contains both a non-trivial transvection and an element of non-zero trace and irreducible characteristic polynomial. Thus, we construct the abelian variety $A/\mathbb{Q}$ as the Jacobian of a smooth genus three curve over $\mathbb{Q}$ with prescribed reductions modulo two distinct primes p and q, which provide us with these two elements.

Explicit bounds for composite lacunary polynomials

Christina Karolus

University of Salzburg

christina.karolus@sbg.ac.at

Let $f, g, h \in \mathbb{C}[x]$ be non-constant complex polynomials satisfying $f(x) = g(h(x))$ and let f be lacunary in the sense that it has at most l non-constant terms. Zannier proved in [*Invent. Math.* **174 (1)** (2008), 127-138] that there exists a function $B_1(l)$ on $\mathbb{N}$, depending only on l and with the property that $h(x)$ can be written as the ratio of two polynomials having each at most $B_1(l)$ terms. Here, we give explicit estimates for this function or, more precicely, we prove that one may take for instance

$$B_1(l) = (4l)^{(2l)^{(3l)^{l+1}}}.$$

Imaginary quadratic fields whose ideal class groups have 3-rank at least three

Yasuhiro Kishi

Aichi University of Education

ykishi@auecc.aichi-edu.ac.jp

Let $n \geq 9$ be an integer and let $k := \mathbf{Q}(\sqrt{4-3^n})$ an imaginary quadratic field. In [1], the author showed that if $n \equiv 3 \pmod 6$, then the 3-rank of the ideal class group of k is at least two. In this talk, we shall prove that if $n \equiv 3 \pmod{18}$ and some additional conditions hold, then the 3-rank of the ideal class group of k is at least three.

References

[1] Y. Kishi, *On the ideal class group of certain quadratic fields*, Glasgow Math. J. **52** (2010), no. 3, 575–581.

On the quantitative version of the Erdős - Turán conjecture about the additive representation functions

Sándor Z. Kiss

Eötvös Loránd University

kisspest@cs.elte.hu

Let A be a set of nonnegative integers. For a positive integer n let $R_A(n)$ denote the number of representations of n as the sum of two terms from A. One of the famous conjecture of Erdős and Turán asserts that if $R_A(n)$ is positive from a certain point on, then it cannot be bounded. There is a quantitative version of the Erdős - Turán conjecture formulated by Erdős and Fuchs. We improve a recent result of Haddad and Helou about the quantitative version of the Erdős - Turán conjecture.

Some explicit formulas of Bernoulli and Cauchy polynomials in terms of Stirling numbers

Takao Komatsu

Wuhan University

komatsu@whu.edu.cn

The integral values of Bernoulli polynomials are expressed in terms of some extended Stirling numbers of the second kind. The integral values of Cauchy polynomials are expressed in terms of some extended Stirling numbers of the first kind. Several relations between the integral values of Bernoulli polynomials and those of Cauchy polynomials are obtained in terms of Stirling numbers of both kinds.

On sum sets of sets having small product set

Sergei V. Konyagin

Steklov Institute of Mathematics

konyagin23@gmail.com

Coauthors: I. D. Shkredov

We improve a result of Solymosi on sum–products in $\mathbb{R}$, namely, we prove that $\max\{|A+A|, |AA|\} \gg |A|^{\frac{4}{3}+c}$, where $c > 0$ is an absolute constant. New lower bounds for sums of sets with small product set are found. Previous results are improved effectively for sets $A \subset \mathbb{R}$ with $|AA| \leq |A|^{4/3}$.

On the primitve of Hardy's function

Maxim Aleksandrovich Korolev

Steklov Mathematical Institute of Russian Academy of Sciences

hardy_ramanujan@mail.ru

Let $Z(t)$ be Hardy's function, that is, $Z(t) = e^{i\vartheta(t)}\zeta\big(\frac{1}{2}+it\big)$, and let $F(T)$ be its integral:

$$F(T) = \int_{2\pi}^{T} Z(t)dt.$$

The estimate $F(T) \ll T^{7/8}$ was obtained by G.H. Hardy and J.E. Littlewood in proving the fact that $\zeta(s)$ has infinitely many zeros on the critical line. In 2004, A. Ivic proved that $F(T) \ll T^{1/4+\varepsilon}$ and conjectured that $F(T) = \Omega_{\pm}(T^{1/4})$. In 2007, the author proved that $|F(T)| <$

$18.2T^{1/4}$ for sufficiently large T and, moreover, that

$$F(T) \,=\, (-1)^N\sqrt{N}\mathfrak{K}(\alpha) \,+\, O\big(N^{1/3}\ln N\big),$$

where $T = 2\pi(N+\alpha)^2$, $N \in \mathbb{N}$, $0 \leqslant \alpha < 1$, that is,

$$N \,=\, \left[\sqrt{\frac{T}{2\pi}}\right], \quad \alpha = \left\{\sqrt{\frac{T}{2\pi}}\right\}.$$

Here $\mathfrak{K}(\alpha)$ denotes some function which satisfy to the equation $\mathfrak{K}(\alpha) = K(\alpha)$ for any fixed α, $0 \leqslant \alpha < 1$,

$$K(\alpha) \,=\, \begin{cases} 0, & \text{if } \ 0 \leqslant \alpha < 1/4,\ 3/4 < \alpha < 1, \\ 2\pi, & \text{if } \ 1/4 < \alpha < 3/4, \\ 4\pi/3, & \text{if } \ \alpha = 1/4, \\ 2\pi/3, & \text{if } \ \alpha = 3/4. \end{cases}$$

In particular, this proves the above conjecture of A. Ivic.

In 2009-2011, M. Jutila undertook a much more deep analysis of the behavior of the functions $F(T)$ and $\mathfrak{K}(\alpha)$. In particular, he obtained the following formula for $\mathfrak{K}(\alpha)$, which is uniform on α, $0 \leqslant \alpha < 1$:

$$\mathfrak{K}(\alpha) \,=\, K_0(\alpha) + \int_{-0.5}^{0.5} w(u)\beta(u)\big(K_0(\alpha+u) - K_0(\alpha)\big)du,$$

where $K_0(\alpha) = K(\alpha)$ for $\alpha \neq 1/4, 3/4$, $K_0(1/4) = K_0(3/4) = \pi$,

$$\beta(u) \,=\, \frac{1}{\pi}\int_0^{+\infty} \cos\big(Ax^3 - 2\pi xu\big)dx, \quad A = \frac{\pi}{12}\sqrt{\frac{2\pi}{T}},$$

is Airy function, $w(u)$ is a smooth weight function such that $w(u) = 1$ for $|u| \leqslant 1/4$, $w(u) = 0$ for $|u| \geqslant 1/2$ and $w^{(k)}(u) \ll_k 1$ for sufficiently many derivatives. M. Jutila also note that "...in a neighborhood of length about $T^{1/3}$ of any point $T = 2\pi(N + j/4)^2$ with N a natural number and $j = 1$ or 3, the function $F(T)$ jumps an amount $\asymp T^{1/4}$ upwards and downwards and *the above* theorem moreover indicates how these jumps take place...".

In the talk, we present a new expression for the function $\mathfrak{K}(\alpha)$ which is free of smooth factor $w(u)$. The advantage of this expression is that it uncovers the features of the oscillations of $\mathfrak{K}(\alpha)$ near the points 1/4 and 3/4 and allow us to demonstrate the effects discovered by M. Jutila in a very precise form.

As a corollaries, we obtain a new unimprovable bound for $|F(T)|$, a new formula for the sum

$$\sum_{t_n \leqslant T} Z(t_n)$$

over Gram points t_n, and some other results.

Indecomposability of polynomials and Diophantine equations

Dijana Kreso

Graz University of Technology

kreso@math.tugraz.at

Given a field K, a polynomial $f(x) \in K[x]$ is said to be indecomposable over K if it can not be represented as a functional composition of lower degree polynomials in $K[x]$. In this talk we discuss several methods for proving indecomposability of polynomials. These are described in a joint survey paper with Robert F. Tichy. We further discuss the applications in Diophantine equations. In particular, we present results on indecomposability of truncated binomial expansions and on finiteness of solutions of Diophantine equations with truncated binomial expansions. The latter results come from a joint work with Arturas Dubickas.

References

[1] Dijana Kreso, Robert F. Tichy, *Functional composition of polynomials: indecomposability, Diophantine equations and lacunary polynomials*, submitted, arxiv:1503.05401.

On the k-free values of the polynomial $xy^k + C$

Kostadinka Lapkova

Alfréd Rényi Institute of Mathematics

lapkova.kostadinka@renyi.mta.hu

Consider the polynomials $f(x, y) = xy^k + C$ for $k \geq 2$ and any nonzero integer constant C. We are interested in deriving an asymptotic formula for the k-free values of $f(x, y)$ when $x, y \leq H$. The strongest tool we would use is a recent generalization of the determinant method due to Reuss.

Additive bases in groups

Thái Hoàng Lê

École polytechnique

thai-hoang.le@polytechnique.edu

Coauthors: Victor Lambert, Alain Plagne

Let $\mathbb{N}$ be the set of all nonnegative integers. A set $A \subset \mathbb{N}$ is called a basis of $\mathbb{N}$ if everysufficiently large integer is a sum of h elements from A, for some h. The smallest such h is called the order of A. For example, the squares form a basis of order 4 and the primes form a basis of order 3 of $\mathbb{N}$. Erdős and Graham asked the following questions. If A is a basis of $\mathbb{N}$ and $a \in A$, when is $A \setminus \{a\}$ still a basis? It turns out that this is the case for all $a \in A$ except a finite number of exceptions. If $A \setminus \{a\}$ is still a basis, what can we say about its order? These questions and related questions have been extensively studied. In this talk, we address these questions in the more general setting of an abelian group in place of $\mathbb{N}$.

Arithmetic properties of lacunary sums of binomial coefficients

Tamás Lengyel
Occidental College
lengyel@oxy.edu

We study lacunary sums of binomial coefficients, $T_n = T(n; m, j, i) = \sum_{k=0}^{n} \binom{km+j}{i}$, where n, m, i, j are nonnegative integers with $j < m$, from the point of view of some arithmetic properties of these sums. We develop new recurrence relations and analyze some p-adic properties for a prime p. The main tools are generating functions, recurrence relations and some congruential and divisibility properties of the binomial coefficients. For instance, we prove the recurrence relation

$$\sum_{s=0}^{i+2} \binom{i+2}{s} (-1)^s T_{n-s} = 0, n \geq i+2.$$

and that n divides $T(n; m, j, i)$ while $n(n+1)$ divides $T(n; m, j, i)$ if $0 \leq j < i$. We use these facts to derive some properties of the sequence $\{\nu_p(T_n)\}_{n \geq 0}$.

On higher dimensional interlacing Fibonacci sequences, continued fractions and Chebyshev polynomials

Matthew Charles Lettington
Cardiff University
LettingtonMC@cardiff.ac.uk
Coauthors: M. W. Coffey, J. L. Hindmarsh, J. Pryce

We study higher-dimensional interlacing Fibonacci sequences and their corresponding multi-dimensional continued fractions, generated via both Chebyshev type functions and m-dimensional recurrence relations. For each integer m, there exist both rational and integer versions of these sequences, where the underlying p-adic structure of the rational sequence enables the integer sequence to be recovered. In particular, for the positive index sequences, one can clear fractions if one knows the prime divisors of $2m+1$; in the negative index case the "excess" prime factors can be removed using Weisman's congruence. When $2m+1$ is a prime these two processes come into alignment.

From either the rational or the integer sequences we can construct a continued fraction vector in $\mathbb{Q}^m$, which converges to an irrational algebraic point in $\mathbb{R}^m$. The sequence terms can be expressed as simple recurrences, trigonometric sums, binomial polynomials and as sums over ratios of powers of the diagonals of the regular unit n-gon. These sequences also exhibit a "rainbow type" quality, corresponding to the Fleck numbers at negative indices and the m-dimensional Fibonacci numbers at positive indices.

It is shown that the families of orthogonal generating polynomials defining the recurrence relations employed, are divisible by the minimal polynomials of certain algebraic numbers, and the three-term recurrences and differential equations for these polynomials are derived. Further results relating to the Christoffel-Darboux formula, Rodrigues' formula and raising and lowering operators are also discussed Furthermore, it is shown that the Mellin transforms of these polynomials satisfy a functional equation of the form $p_n(s) = \pm p_n(1-s)$, and have zeros only on the critical line Re $s = 1/2$.

Orders and conductors in algebraic number fields

Günter Lettl

Karl-Franzens-Universität

guenter.lettl@uni-graz.at

We consider the problem to find all orders (i.e. subrings of the ring of integers of finite index) in an algebraic number field. In 2014, this was done by C. Prabpayak for all pure cubic number fields. We present recent results on arbitrary cubic number fields.

Euler systems: new constructions, results and conjectures

David Loeffler

University of Warwick

D.A.Loeffler@warwick.ac.uk

One of the central open problems in number theory is the Birch–Swinnerton-Dyer conjecture, which predicts that the rank of the group of rational points of an elliptic curve is equal to the order of vanishing of its L-function at s = 1. This was proved by Kolyvagin when the order of vanishing is 0 or 1, using a tool called an 'Euler system'. Euler systems are families of classes in Galois cohomology satisfying certain compatibility conditions, mirroring the Euler products of L-functions.

Kolyvagin's work led to conjectures predicting Euler systems in other arithmetic contexts, which would have similarly powerful applications; sadly these have proved difficult to construct. However, recent breakthroughs have led to some new examples of Euler systems. I will describe a new Euler system associated to the Rankin convolution of two modular forms, constructed by Lei, Zerbes and myself (drawing on earlier work of Flach and Bertolini–Darmon–Rotger), and some applications of this new Euler system to classical arithmetic problems.

On the rationality and holomorphy of Langlands-Shahidi L-functions over function fields

Luis Lomelí

Max-Planck Institute for Mathematics

lomeli@mpim-bonn.mpg.de

We use the theory of Eisenstein series over a global function field k, with field of constants $\mathbb{F}_q$, to prove that all Langlands-Shahidi automorphic L-functions over function fields are rational in the variable q^{-s}. After incorporating twists by highly ramified characters, our automorphic L-functions become polynomials in $\{q^{-s}, q^s\}$. We then specialize to a quasi-split classical group $\mathbf{G}_n$. Let π be a globally generic cuspidal automorphic representations of $\mathbf{G}_n$ and τ a cuspidal (unitary) automorphic representation of GL_m ($\mathrm{Res}\,\mathrm{GL}_m$ in the case $\mathbf{G}_n$ is a unitary group), then $L(s, \pi \times \tau)$ is holomorphic for $\Re(s) > 1$.

Statistics for the number of points on biquadratic curves over finite fields

Elisa Lorenzo García

Universiteit Leiden

e.lorenzo.garcia@math.leidenuniv.nl

Coauthors: Giulio Meleleo, Piermarco Milione

A basic question about a curve over a finite field is how many points it has, and for a family of curves one can study the distribution of this statistic. We will give concrete examples of

families in which this distribution is known or predicted, and compute the distribution law for the concrete family of biquadratic curves.

Limit structures in graph theory and number theory

László Lovász

Eötvös Loránd University

lovasz@cs.elte.hu

Assigning limit objects to growing sequences of discrete structures has emerged as a useful method in graph theory, number theory, computer science, and other areas. In this talk we illustrate the basic idea of this method on the example of graphs, and descibe some applications to number theory, including the sketch of a proof of Szemeredi's Theorem by Elek and Szegedy.

On a problem of Pillai with Fibonacci numbers and powers of 2

Florian Luca

University of the Witwatersrand

florian.luca@wits.ac.za

Coauthors: Mahadi Ddamulira, Mihaja Diarisoa Rakotomalala

Pillai proved that given coprime positive integers a and b, there are only finitely many integers c having more than one representation of the form $a^x - b^y$ with positive integers $x,\ y$. In my talk, I will report on a variation of Pillai's question with Fibonacci numbers and powers of 2. Namely, we find all integers c having more than one representation as $F_n - 2^m$, with integers $n \geq 2,\ m \geq 2$, where $\{F_n\}_{n\geq 1}$ is the sequence of Fibonacci numbers

Forms of differing degrees over number fields

Manfred Madritsch

Université de Lorraine

manfred.madritsch@univ-lorraine.fr

Coauthors: Christopher Frei

Consider a system of m forms of degree d in n variables over the integers. Using the circle method Birch gave an asymptotic formula for the number of integer solutions to this system in a homogeneously expanding box provided n is large compared to m and d. An analogous result over arbitrary number fields was proved by Skinner. In joint work with C. Frei, we combine Skinner's techniques with a recent generalization of Birch's theorem by Browning and Heath-Brown, where they allow the forms to have differing degrees.

We discuss the main ingredients of the proof as well as consequences of this result to the Hasse principle, weak approximation and Manin's conjecture.

Subconvexity for sup-norms of automorphic forms on $PGL(n)$

Péter Maga

Georg-August-Universität

maga.peter@renyi.mta.hu

Coauthors: Valentin Blomer

As it was proved by Sarnak, the supnorm of eigenfunctions of the Laplacian on a compact symmetric Riemannian manifold can be estimated from above by an appropriate power (given in terms of some invariants of the space) of their Laplace eigenvalue. Examples show that Sarnak's

exponent is sharp in some cases. However, when the space has also arithmetic symmetries (i.e. Hecke operators) and we restrict to joint eigenfunctions of the Laplacian and the Hecke operators, one might expect a better exponent. We prove that a better exponent exists for automorphic forms on $PGL(n, \mathbf{R})$.

Prime and almost prime solutions to diophantine systems of high rank

Ákos Magyar
University of Georgia
amagyar@uga.edu

Coauthors: B. Cook, T. Titichetrakun

Let $\mathcal{F}$ be a family of r integral forms of degree k in n variables $\mathbf{x} = (x_1, ..., x_n)$. The classical works of Birch and Schmidt establish an asymptotic formula for the number of integer solutions to the diophantine system $\mathcal{F}(\mathbf{x}) = \mathbf{v}$, assuming the system is large with respect to certain notions of rank.

We show that under the same conditions one can estimate from below the number of almost prime solutions $\mathbf{x}$, when each of the x_i's has a bounded number of prime factors depending only on the parameters k and r. The main tool is to count the weighted number of solutions endowed with weights which are concentrated on almost prime numbers. If the rank of the system is sufficiently large then one can also establish a general local to global type statement for the asymptotic number of solutions, under the stronger restriction that the coordinates of the solutions are primes. The key new ingredient is a regularization process which brings the system to a suitable form when one can apply estimates for exponential sums over the primes.

A space of weight 1 modular forms attached to totally real cubic number fields.

Guillermo Mantilla-Soler
Universidad de los Andes
g.mantilla691@uniandes.edu.co

The main goal of this talk is to exhibit a canonical subspace of a space of weight 1 modular forms that is parametrized by the set of isomorphism classes of cubic fields of a fixed fundamental discriminant. In case that the fields have ramification at infinity, the construction is known and I will briefly recall it. Here, using the theory of integral traces, I will show how to construct such a subspace for cubic fields with no ramification at infinity i.e., totally real cubic fields.

Siegel modular forms and their fundamental Fourier coefficients

Jolanta Marzec
University of Bristol
jolanta.marzec@bristol.ac.uk

We investigate Siegel modular forms with respect to different congruence subgroups and the existence of the, so called, fundamental Fourier coefficients. These coefficients are especially interesting because of their relations with nice Bessel models and central values of L-functions (Gan-Gross-Prasad type conjectures). To examine the fundamental Fourier coefficients we work with automorphic representations attached to Siegel modular forms, making use of the relation between Bessel periods and Fourier coefficients. Our method yields many relations between Fourier coefficients that may be of independent interest.

The mixed joint universality for a class of zeta-functions

Kohji Matsumoto

Nagoya University

kohjimat@math.nagoya-u.ac.jp

Coauthors: Roma Kačinskaitė

For $m \in \mathbb{N}$, attach $g(m) \in \mathbb{N}$, and, for $j \in \mathbb{N}$ with $1 \le j \le g(m)$, let $f(j,m) \in \mathbb{N}$ and $a_m^{(j)} \in \mathbb{C}$. Denote by p_m the mth prime number, and let $s = \sigma + it$ be a complex variable. The zeta-function $\widetilde{\varphi}(s)$ introduced by author [3] is defined by the polynomial Euler product

$$\widetilde{\varphi}(s) = \prod_{m=1}^{\infty} A_m^{-1}(p_m^{-s}), \tag{1}$$

where A_m's are polynomials given by $A_m(x) = \prod_{j=1}^{g(m)}(1 - a_m^{(j)} x^{f(j,m)})$. Suppose that $g(m) \le c p_m^{\alpha}$, $|a_m^{(j)}| \le p_m^{\beta}$ with $c > 0$, and some non-negative constants α and β. Note that this form of Euler product includes, as special cases, many important zeta or L-functions appearing in number theory.

The infinite product (1) converges absolutely for $\sigma > \alpha + \beta + 1$. Therefore the shifted function $\varphi(s) = \widetilde{\varphi}(s + \alpha + \beta)$ convergent absolutely for $\sigma > 1$. We assume that $\varphi(s)$ can be continued meromorphically to $\sigma \ge \sigma_0$, and satisfies certain moderate conditions.

Let $\mathfrak{B} = \{b_m : m \in \mathbb{N} \cup \{0\}\}$ be a periodic sequence of complex numbers with minimal period $l \in \mathbb{N}$, and let $\gamma \in \mathbb{R}$, $0 < \gamma \le 1$, be a fixed parameter. Then the function $\zeta(s, \gamma; \mathfrak{B})$ introduced by A. Laurinčikas and A. Javtokas [1] is defined, for $\sigma > 1$, by the series

$$\zeta(s, \gamma; \mathfrak{B}) = \sum_{m=0}^{\infty} \frac{b_m}{(m + \gamma)^s}.$$

From the periodicity of $\mathfrak{B}$ we have $\zeta(s, \gamma; \mathfrak{B}) = \frac{1}{l^s} \sum_{k=0}^{l-1} b_k \zeta(s, (k+\gamma)/l)$, $\sigma > 1$, where $\zeta(s, \gamma)$ is the classical Hurwitz zeta-function. Therefore, the function $\zeta(s, \gamma; \mathfrak{B})$ is a linear combination of the functions $\zeta(s, \gamma)$, and the last equality gives the analytic continuation for $\zeta(s, \gamma; \mathfrak{B})$ to the whole complex plane, where it is regular, except, maybe, for a simple pole at $s = 1$ with residue $b := \frac{1}{l} \sum_{k=0}^{l-1} b_k$.

In this talk, we first discuss a mixed joint limit theorem. Let D_φ be the set of all $s \in \mathbb{C}$ whose real part is $> \sigma_0$ but does not equal to the real part of any of the poles of $\varphi(s)$. Let D' be the half-plane $\sigma > 1/2$ if $\zeta(s, \gamma; \mathfrak{B})$ is entire. If $s = 1$ is a pole of $\zeta(s, \gamma; \mathfrak{B})$, then we exclude the line $\Re s = 1$ from the half-plane $\sigma > 1/2$ and denote the remaining part by D'.

For any domain D, denote by $H(D)$ the set of holomorphic functions defined on D. Let D_1 be an open subset of D_φ, and D_2 be an open subset of D'. For any Borel subset A of $H(D_1) \times H(D_2)$, define

$$P_T(A) = \frac{1}{T} \mu \left\{ \tau \in [0, T] \mid (\varphi(s_1 + i\tau), \zeta(s_2 + i\tau, \gamma; \mathfrak{B})) \in A \right\}, \tag{2}$$

where μ denotes the 1-dimensional Lebesgue measure. Then our mixed joint limit theorem is as follows.

Theorem 1. *If γ is a transcendental number, then the probability measure P_T defined by* (2) *converges weakly to a certain measure P, which can be constructed explicitly.*

This Theorem 1 is an essential tool for the proof of the mixed joint universality theorem. However, to prove the universality, the notion of $\varphi(s)$ is too general at present, so we have to add further assumptions. Among them, the most important assumption is the existence of the limit

$$\lim_{x\to\infty}\frac{1}{\pi(x)}\sum_{p\le x}|c(p)|^2, \tag{3}$$

where $\pi(x)$ denotes the number of prime numbers up to x, and $c(p)$ is the pth Dirichlet expansion coefficient of $\varphi(s)$. J. Steuding [6] introduced a class (the "Steuding class") of L-functions satisfying (3) and some other conditions (polynomial order estimate, Euler product etc.) and proved the universality for those L-functions.

Let $\varphi(s)$ be in the Steuding class, and let σ^* be the infimum of all σ for which

$$\frac{1}{2T}\int_{-T}^{T}|\varphi(\sigma+it)|^2dt\sim\sum_{m=1}^{\infty}|c(m)|^2m^{-2\sigma}$$

holds. Let K_1 be a compact subset of the strip $\sigma^*<\Re s<1$, K_2 be a compact subset of the strip $1/2<\Re s<1$, both with connected complements. Let f_j be a continuous function defined on K_j $(j=1,2)$, holomorphic in the interior of K_j, and especially f_1 is non-vanishing on K_1. For $\varepsilon>0$, let $\mathcal{I}_\varepsilon(T)$ be the set of all $\tau\in[0,T]$ such that

$$\max_{s\in K_1}|\varphi(s+i\tau)-f_1(s)|<\varepsilon,\quad \max_{s\in K_2}|\zeta(s+i\tau,\gamma;\mathfrak{B})-f_2(s)|<\varepsilon.$$

Theorem 2. *Let $\varphi(s)$ be in the Steuding class, and γ be a transcendental number. Then for any K_1, K_2, f_1, f_2 and ε as above, we have*

$$\liminf_{T\to\infty}\frac{1}{T}\mu(\mathcal{I}_\varepsilon(T))>0.$$

This is a kind of mixed joint universality theorem. Roughly speaking, this theorem implies that any target functions f_1 and f_2 can be approximated simultaneously by a suitable vertical shift τ of φ and ζ, respectively. Moreover, the set of such τ is of positive lower density.

The word "mixed" is used to express that φ has the Euler product, while ζ does not have. In the theory of universality, the situation is sharply different whether the zeta (or L) function has the Euler product, or not. (For example, in Theorem 2, the non-vanishing condition is assumed only for f_1.) Therefore it is remarkable that the joint universality property holds for two zeta-functions, one of them has Euler product and the other does not have.

This type of universality was first discovered by H. Mishou [4], and also by J. Sander and J. Steuding [5] (independently of each other), in the case when φ is the Riemann zeta-function and ζ is a Hurwitz zeta-function. A generalization to the case of periodic coefficients was done by the coauthor and A. Laurinčikas [2]. Our Theorem 2 gives a further generalization in this direction.

References

[1] A. Javtokas and A. Laurinčikas, *On the periodic Hurwitz zeta-function*, Hardy-Ramanujan J. **29** (2006), 18-36.

[2] R. Kačinskaitė and A. Laurinčikas, *The joint distribution of periodic zeta-functions*, Studia Sci. Math. Hung. **48** (2011), 257-279.

[3] K. Matsumoto, *Value-distribution of zeta-functions* in Analytic Number Theory, Proc. Japanese-French Sympos., Tokyo, 1988, K. Nagasaka and E. Fouvry (Eds.), Lecture Notes in Math. **1434**, Springer, 1990, 178–187.
[4] H. Mishou, *The joint value-distribution of the Riemann zeta function and Hurwitz zeta functions*, Liet. Mat. Rink. **47** (2007), 62-80.
[5] J. Sander and J. Steuding, *Joint universality for sums and products of Dirichlet L-functions*, Analysis **26** (2006), 295-312.
[6] J. Steuding, *Value-Distribution of L-Functions*, Lecture Notes in Math. **1877**, Springer, 2007.

Index-p Abelinaziation data of p-class tower groups

Daniel C. Mayer
Karl-Franzens-Universität Graz
algebraic.number.theory@algebra.at

Given a fixed prime p, the multiplet of abelian type invariants of the p-class groups of all unramified cyclic degree-p extensions of a number field K is called its IPAD $\tau^{(1)}(K)$ (index-p abelianization data).

Using IPADs, we introduce a series of sophisticated new techniques for identifying the p-capitulation type $\kappa(K)$ of K, the second p-class group G_p^2 (the Galois group of the maximal metabelian unramified p-extension) or even the p-class field tower group G_p^∞ (the Galois group of the maximal unramified pro-p extension) of a number field K:

- pattern recognition via Artin transfers [1],
- multiple-layered transfer target types $\tau(K)$ (TTTs) [2],
- multiple-layered transfer kernel types $\kappa(K)$ (TKTs) [2],
- iterated IPADs $\tau^{(2)}(K)$ of second order,
- arithmetically structured coclass trees of finite p-groups,
- uni-polarization and stabilization in coclass trees [2],
- periodic multifurcations in descendant trees [1],
- and various kinds of pruning strategies [1].

One of our central results for $p = 3$ is a Main Theorem which gives a complete overview of all possible IPADs $\tau^{(1)}(K)$ and multi-layered TTTs $\tau(K)$ of an arbitrary number field K with 3-class group $\mathrm{Cl}_3(K)$ of type $(3,3)$ in the form of several infinite sequences together with polycyclic pc-presentations for the corresponding metabelianization $G/G'' \simeq G_p^2$ of the 3-tower group $G = G_p^\infty$ of K [3].

We conclude with definite highlights in computational number theory. By means of iterated IPADs $\tau^{(2)}(K)$ of second order we determine the exact length of the 3-class tower of the quadratic fields $\mathbb{Q}(\sqrt{342\,664})$ and $\mathbb{Q}(\sqrt{-3\,896})$, which resisted all attempts up to now [1].

Research supported by the Austrian Science Fund (FWF): P 26008-N25

References

[1] M. R. Bush and D. C. Mayer, 3-*class field towers of exact length* 3, J. Number Theory **147** (2015), 766–777, DOI 10.1016/j.jnt.2014.08.010.

[2] D. C. Mayer, *The distribution of second p-class groups on coclass graphs*, J. Théor. Nombres Bordeaux **25** (2013), no. 2, 401–456, DOI 10.5802/jtnb842. (27th Journées Arithmétiques, Faculty of Mathematics and Informatics, Univ. of Vilnius, Lithuania, 2011.)

[3] D. C. Mayer, *Principalization algorithm via class group structure*, J. Théor. Nombres Bordeaux **26** (2014), no. 2, 415–464.

Long gaps between primes

James Maynard

University of Oxford

james.maynard@magd.ox.ac.uk

Coauthors: K. Ford, B. Green, S. Konyagin, T. Tao

Let p_n denote the n^{th} prime. We show that for sufficiently large X

$$\max_{p_n \leq X} (p_{n+1} - p_n) \gg \frac{\log X \log\log X \log\log\log\log X}{\log\log\log X}.$$

Our proof relies on a probablisitic argument, utilizing sieve estimates related to bounded gaps between primes and a hypergraph covering lemma based on the Rödl nibble.

The mode of the Jacobi-Stirling numbers

István Mező

Nanjing University

istvanmezo81@gmail.com

The Jacobi-Stirling numbers were discovered by W.N. Everitt and his co-workers in 2007 during studying the spectral analysis of the second order Jacobi differential operator. It turned out in the same study that these newly defined numbers possess many properties of the classical Stirling numbers of the second kind: they have similar recurrence relation, they are connecting coefficients between specific polynomials, can be expressed by forward differences, and that they are strongly connected to the Bernoulli numbers and to the elementary and complete symmetric functions. Later G.E. Andrews and his co-workers found a nice set partition theoretical interpretation for them.

It is also known that these numbers form unimodal sequences with a peak or a plateau of two points. In our talk we give asymptotical estimations for the maximizing index. Moreover, we present a conjectural expression for the sharpest estimation possible. We discuss these problems for the first kind Jacobi-Stirling numbers, too.

Simple sets of distribution functions of ratio sequences

Ladislav Mišík

University of Ostrava

ladislav.misik@osu.cz

Coauthors: David Krčmarský, Zuzana Václavíková

There are various methods how to describe and characterize distribution of elements of sets of positive integers. One of the most interesting is that using the set of all distribution functions

$G(X_n)$ of the corresponding ratio block sequence (X_n), introduced in [1]. One of the most challenging problem in this theory is that of characterization of all possible such sets $G(X_n)$.

In this contribution we study the case when $G(X_n)$ contains a distribution function which is a limit of a subsequence of step distribution functions along a large subset of indices. Some sufficient conditions under which $G(X_n)$ is either small in a metric sense, or simple in algebraic structure are discussed. As a corollary we obtain a new characteriztion in the case of asymptotic distribution, i.e. $G(X_n)$ being a singleton.

References

[1] O. Strauch, J. Tóth, *Distribution functions of ratio sequences*, Publ. Math. Debrecen **58** (2001), no. 4, 751–778.

Arithmetic properties of the sequence of derangements

Piotr Miska

Jagiellonian University

piotr.miska@uj.edu.pl

The sequence of derangements is given by a formula $D_0 = 1, D_n = nD_{n-1} + (-1)^n, n > 0$. It is a classical object appearing in combinatorics and number theory.

For each nonnegative integer n we have $n - 1|D_n$. In particular, p-adic valuation of D_n is estimated from below by p-adic valuation of $n-1$ for each prime number p. We prove that there are infinitely many prime numbers p such that $v_p(D_n) > v_p(n-1)$ for some positive integer n. Moreover, we give the description of p-adic valuation of $\frac{D_n}{n-1}$ for a given prime number p.

We show that for each positive integer d there exists polynomial $f_d \in \mathbb{Z}[X]$ such that $D_n = (n-d+1)...(n-1)nD_{n-d} + (-1)^n f_d(n)$ for all integers $n \geq d$. Furthermore we prove that if $d > 3$, then f_d has exactly $d-1$ distinct real roots, among which there is exactly one rational root, namely 1.

On a three term exponential Diophantine equation

Takafumi Miyazaki

Nihon University

miyazaki-takafumi@math.cst.nihon-u.ac.jp

We first give a brief introduction about the exponential Diophantine equation $a^x + b^y = c^z$ for fixed positive integers a, b and c. In particular, we see a problem proposed by N.Terai concerning the triples (a, b, c) satisfying $a^2 + b^2 = c^r$ for some integer $r > 1$. After that we state our result on the equation. The result can be regarded as a relevant analogue to the work of F. Luca concerning Terai's problem. If time permits, we sketch the proof. This is a joint work with F. Luca.

About integer Somos-8 and Somos-9 sequences

Mariia Monina

Institute of Applied Mathematics, Khabarovsk Division

monina@iam.khv.ru

For integer $k \geq 4$ Somos-k sequence is generated by quadratic recurrence relation of the form

$$S_{n+k}S_n = \sum_{j=1}^{[k/2]} \alpha_i S_{n+k-j}S_{n+j}$$

with constant α_i and $S_1, \ldots, S_k$ are initial data.

For particular choices of the coefficients and the initial data, such recurrences can yield sequences of integers. Fomin and Zelevinsky [1] proved integrality of Somos-k for cases $k = 4, 5, 6, 7$ with integer coefficients and initial data is equal ± 1. In the case $k = 4, 5$ this result was expanded by Swart and Hone [2] on some sets of rational coefficients and integer initial data.

Using results of [3] we proved the following statement.

Let S_n be Somos-4 sequence and a, b, l be nonzero integer numbers. Then

$$T_n = aS_n + bS_{n+2l}$$

is an integer Somos-8 or Somos-9 sequence.

This work was supported by the RFBR (project no. 14-01-00203)

References

[1] S. Fomin and A. Zelevinsky, *The Laurent Phenomenon*, Adv. Appl. Math. **28** (2002) 119-144.

[2] S. Swart and A.N.W. Hone, *Integrality and the the Laurent phenomenon for Somos-4 sequences*, arXiv: math/0508094v4 [math. NT], 18.12.2006.

[3] V. Bykovskii, *Elliptic systems of sequences and functions*, *http : //www.skoltech.ru/app/data/uploads/sites/*29/2015/02/.

Inequalities for diophantine exponents in small dimensions

Nikolay Moshchevitin

Moscow Lemonosov State University

moshchevitin@gmail.com

Coauthors: D. Gayfulin

We consider a vector $\Theta = (\theta_1, ..., \theta_n), n \geq 2$ and suppose that the numbers $1, \theta_1, ..., \theta_n$ are linearly independent over $\mathbb{Z}$. Put

$$\psi_\Theta(t) = \min_{q \in \mathbb{Z}_+, q \leq t} \max_{1 \leq j \leq n} ||q\theta_j||.$$

We consider the ordinary Diophantine exponent $\omega = \omega(\Theta)$ and the uniform Diophantine exponent $\hat{\omega} = \hat{\omega}(\Theta)$ defined as

$$\omega = \omega(\Theta) = \sup \left\{ \gamma : \liminf_{t \to +\infty} t^\gamma \psi_\Theta(t) < +\infty \right\},$$

$$\hat{\omega} = \hat{\omega}(\Theta) = \sup\left\{\gamma : \limsup_{t\to+\infty} t^{\gamma}\psi_{\Theta}(t) < +\infty\right\}.$$

For $n = 2$ the optimal inequality between $\hat{\omega}$ and ω was obtained by V. Jarník. The optimality of Jarník's inequality was proved by M. Laurent. In dimension $n = 3$ the optimal inequality was obtatined by N. Moshchevitin and W.M. Schmidt and L. Summerer. The optimality of this inequality follows from a general result by D. Roy.

We will discuss some new inequalities in dimension $n = 4$ which seem to be optimal in a certain sense.

Distribution of entire curves and integral points in open algebraic varieties

Junjiro Noguchi

University of Tokyo

noguchi@ms.u-tokyo.ac.jp

We will discuss the value distribution of entire (holomorphic) curves and the distribution of integral points on algebraic varieties. In our paper [1] we proved a theorem on this subject, but later there was found some gap in the proof. Here we fix it and improve the statement with better estimate. We discuss the following results in [2]: Let X be a complex projective algebraic manifold, and let $D_i, 1 \le i \le l$, be effective reduced divisors on X in general position. Let $W \subset X$ be a subvariety and set $W' = W \setminus \bigcup_{D_i \not\supset W} D_i$.

Theorem. *Assume that either (i) there is a non-constant entire curve $f : \mathbf{C} \to W'$ with Zariski dense image, or (ii) everything is defined over a number field k and there is a Zariski-dense S-integral subset in W'. Then we have that*

$$\mathrm{rank}\{D_i|_W; D_i \not\supset W\} + q(W) \leqq \dim W + \mathrm{rank}_{\mathbf{Z}}\{c_1(D_i)\}.$$

Theorem. *Let the notation be as above. Assume that D_i are ample and that $l \geqq 2\dim W + \mathrm{rank}_{\mathbf{Z}}\{c_1(D_i)\}$. Then,* (i) *there is no non-constant entire curve $f : \mathbf{C} \to W'$, and* (ii) *over number filed k, every S-integral subset of W' is finite.*

References

[1] J. Noguchi and J. Winkelmann, *Holomorphic curves and integral points off divisors*, Math. Z. **239** (2002), 593-610.

[2] J. Noguchi and J. Winkelmann, *Nevanlinna Theory in Several Complex Variables and Diophantine Approximation*, Grundl. der Math. Wiss. Vol. 350, pp. xiv+416, Springer, Tokyo-Heidelberg-New York-Dordrecht-London, 2014.

Monochromatic linear recurrence sequences

Gábor Nyul

University of Debrecen

gnyul@science.unideb.hu

Coauthors: Csanád Bertók, Bettina Rauf

A classical theorem of van der Waerden states that for any positive integers k and r, if we colour the positive integers with r colours, then there exists a strictly increasing monochromatic arithmetic progression of length k. The similar question can be raised for arbitrary family of positive integer sequences.

H. Harborth and S. Maasberg studied this problem for sequences satisfying the Fibonacci recurrence. Together with B. Rauf, we extended their results for higher order linear recurrence sequences with positive integer coefficients. Choosing an arbitrary recurrence relation, we gave a positive or negative answer for all but finitely many pairs (k, r), which covered all possibilities in the Fibonacci and tribonacci cases.

Together with Cs. Bertók, we strengthened the above results under a certain additional assumption, and we gave a complete answer for infinitely many recurrences, especially in the multibonacci case. Moreover, we also studied binary linear recurrences having coefficients of both signs.

References

[1] G. Nyul and B. Rauf, *On the existence of van der Waerden type numbers for linear recurrence sequences with constant coefficients*, Fibonacci Quarterly **53** (2015), 53–60.

About triangular numbers

Péter Olajos

University of Miskolc

matolaj@uni-miskolc.hu

Coauthors: Zsolt Rábai

We are investigated the following equation:

$$\triangle_n^2 + \triangle_m^2 = \triangle_k^2,$$

where $\triangle_n = \dfrac{n(n+1)}{2}$, that is $\triangle_n$ is a triangle number. Until now there is only one well known solution which is the following:

$$\triangle_{132}^2 + \triangle_{143}^2 = \triangle_{164}^2.$$

Using simple properties of triangular numbers we have had two ways to solve the equation above. In both cases we got parametric elliptic curves of degree 3 or 4. In this talk we will try to illustrate tools for solving this equation, because our conjecture is that there are only one solution of this equation.

On the various mean values of the Dirichlet L-functions

Tomokazu Onozuka

Nagoya University

m11022v@math.nagoya-u.ac.jp

Coauthors: T. Okamoto

Let χ be a Dirichlet character modulo $k \geq 2$ and $L(s, \chi)$ be the Dirichlet L-function. For positive integers m, n with the same parity, the mean value $\sum_{\substack{\chi \pmod k \\ \chi(-1)=(-1)^m}} L(m, \chi)L(n, \overline{\chi})$ has been studied by some mathematicians, and Liu and Zhang gave the explicit formula in 2006. In 2013, Alkan considered the mean value $\sum_{\substack{\chi_1,\chi_2 \pmod k \\ \chi_1(-1)=\chi_2(-1)=-1}} L(1, \chi_1)L(1, \chi_2)L(2, \overline{\chi_1\chi_2})$ for $k > 2$, and he gave the explicit formula. In this talk, we give the explicit formula for the mean value $\sum_{\substack{\chi_1,\chi_2 \pmod k \\ \chi_1(-1)=(-1)^m,\ \chi_2(-1)=(-1)^n}} L(m, \chi_1)L(n, \chi_2)L(m+n, \overline{\chi_1\chi_2})$ in the case $m, n \in \mathbb{N}$ and $k > 2$. Furthermore, applying those results on mean values of Dirichlet L-functions, we also give an explicit formula for certain mean values of double Dirichlet L-functions.

Effective bounds for a conjecture of Lang : the case of curve

Amilcar Pacheco

Universidade Federal do Rio de Janeiro

amilcar@acd.ufrj.br

Coauthors: Fabien Pazuki

Let X be a curve of genus $d \geq 2$ defined over a global field K of characteristic $p > 2d + 1$. We also assume X/K to be non-isotrivial. Let J be its Jabobian variety, K_s a separable closure of K and Γ a subgroup of $J(K_s)$ such that $\Gamma/p\Gamma$ is finite. We give an explicit bound for the number of points of $X \cap \Gamma$.

Fields generated by torsion points of elliptic curves

Laura Paladino

University of Pisa

paladino@mail.dm.unipi.it

Coauthors: Andrea Bandini

Let K be a field and let $\mathcal{E}$ be an elliptic curve defined over K. Let m be a positive integer, coprime with $char(K)$ if $char(K) \neq 0$. We denote by $\mathcal{E}[m]$ the m-torsion subgroup of $\mathcal{E}$ and by $K(\mathcal{E}[m])$ the field obtained by extending K with the coordinates of the m-torsion points of $\mathcal{E}$. Let $\{P_1, P_2\}$ be a generating set for $\mathcal{E}[m]$, with $P_i := (x_i, y_i)$, for $i \in \{1, 2\}$. Then $K(\mathcal{E}[m]) = K(x_1, y_1, x_2, y_2)$. We prove that $K(\mathcal{E}[m]) = K(x_1, \zeta_m, y_2)$, for any odd $m \geq 5$, where ζ_m is a primitive m-th root of unity. If K is a number field and $\mathcal{E}$ does not have complex multiplication, we show that for all but finitely many primes p, the generating set $\{x_1, \zeta_p, y_2\}$ of $K(\mathcal{E}[p])$ is minimal among the subsets of $\{x_1, y_1, x_2, y_2, \zeta_p\}$. We also show some particular cases (when m is a small integer) and some applications to modular curves.

Redcutions of Galois representations

Aftab Pande

Universidade Federal do Rio de Janeiro

aftab.pande@gmail.com

Given $\overline{\rho} : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}/p)$ whose image contains $SL_2(\mathbb{Z}/p)$ it was shown by Ramakrishna that there exists a deformation $\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_p[[T_1, T_2, ..., T_r, ..]])$ whose image contains $SL_2(\mathbb{Z}_p[[T_1, T_2, ..., T_r, ..]])$. We modify his results for the case where $\overline{\rho}$ is reducible.

Direct and inverse problems in subsequence sums

Ram Krishna Pandey

Indian Institute of Technology, Roorkee

ramkpandey@gmail.com

Coauthors: Raj Kumar Mistri, Om Pakash

Let A be a finite subset of an abelian group G and $h, r \geq 1$ are integers. The generalized h-fold sumset, denoted by $h^{(r)}A$, is the sum of h elements of A, where each element appears in the sum can have at most r copies. If $G = \mathbb{Z}$, then the lower bounds for $|h^{(r)}A|$ and the structure of the sets A for which this lower bound is attained will be presented. Furthermore, let $A = (\underbrace{a_0, \ldots, a_0}_{r \text{ copies}}, \underbrace{a_1, \ldots, a_1}_{r \text{ copies}}, \ldots, \underbrace{a_{k-1}, \ldots, a_{k-1}}_{r \text{ copies}})$ be a finite sequence of integers with k distinct terms, $a_0 < a_1 < \cdots < a_{k-1}$. The sum of all the terms of a subsequence of length at least one

of the sequence A is said to be the subsequence sum of A. The set of all subsequence sums of A is denoted by $S(r, A)$. The direct problem for subsequence sums is to find the lower bound for $|S(r, A)|$ in terms of the number of distinct terms in the sequence A. The inverse problem for subsequence sums is to determine the structure of the finite sequence A of integers for which $|S(r, A)|$ is minimal. We shall present both these problems as well.

The Fourier-Jacobi-decomposition of Eisenstein series of Klingen type

Thorsten Paul

Saarland University

thorstenpaul@math.uni-sb.de

The space of Siegel modular forms of degree n and weight k has a decomposition in a direct sum

$$M_n^k = \oplus_{m=0}^n M_{n,m}^k,$$

where the space $M_{n,m}^k$ corresponds to the space of cusp forms of degree m and weight k. A Siegel modular form of degree n has Fourier-Jacobi expansions of degree $r \leq n$. The spaces of Jacobi forms have (by work of Dulinski) similar decompositions.

We want to describe how these decompositions fit together, meaning to compute the decomposition of a Fourier-Jacobi-coefficient of a siegel modular form in $M_{n,m}^k$.

Bad reduction of curves with CM jacobians

Fabien Pazuki

University of Bordeaux, University of Copenhagen

fabien.pazuki@gmail.com

Coauthors: Philipp Habegger

An abelian variety defined over a number field and having complex multiplication (CM) has potentially good reduction everywhere. If a curve of positive genus which is defined over a number field has good reduction at a given finite place, then so does its jacobian variety. However, the converse statement is false already in the genus 2 case, as can be seen in Namikawa and Ueno's classification table of fibres in pencils of curves of genus 2. In this joint work with Philipp Habegger, our main result states that this phenomenon prevails for certain families of curves.

We prove the following result: Let $\mathbb{F}$ be a real quadratic number field. Up to isomorphisms there are only finitely many curves C of genus 2 defined over the algebraic closure of the rationals with good reduction everywhere and such that the jacobian $\mathrm{Jac}(C)$ has CM by the maximal order of a quartic, cyclic, totally imaginary number field containing $\mathbb{F}$. Hence, except for finitely many examples, such a curve will always have stable bad reduction at some prime whereas its jacobian has good reduction everywhere. A remark is that one can exhibit infinite families of genus 2 curves with CM jacobian such that the endomorphism ring is the ring of algebraic integers in a cyclic extension of the rationals of degree 4 that contains $\mathbb{F}$ for some specific $\mathbb{F}$.

On a higher dimensional Mahler approximation

Steffen Hojris Pedersen
Aarhus University
steffenh@math.au.dk
Coauthors: Simon Kristensen, Barak Weiss

Mahler defined for $\alpha \in \mathbb{R}$, $n \in \mathbb{N}$ a diophantine exponent

$$\omega_n(\alpha) = \sup\{\omega \in \mathbb{R} : 0 < |P(\alpha)| \leq H(P)^{-\omega}, \\ \text{for infinitely many } P \in \mathbb{Z}[X], \text{ with } \deg P \leq n\},$$

where $H(P)$ is the maximum of the absolute value of the coefficients of P, called the height of P. $\omega_n(\alpha)$ measures how well α can be approximated by algebraic numbers of degree at most n.

In this talk I will present several results on a higher dimensional version of Mahler's approximation, introduced by K. Yu, where we evaluate points $\alpha \in \mathbb{R}^d$ in polynomials $P \in \mathbb{Z}[X_1, \ldots, X_d]$ of total degree at most k.

Quadratic Lagrange spectrum

Tomislav Pejković
University of Zagreb
pejkovic@math.hr

We study the quadratic Lagrange spectrum defined by Parkkonen and Paulin by considering the approximation by quadratic numbers whose regular continued fraction expansion is ultimately periodic with the same period as a fixed quadratic number or its Galois conjugate. We improve the upper bound on the approximation constants involved thereby proving a conjecture stated by Bugeaud.

Reductions of algebraic integers

Antonella Perucca
University of Regensburg
antonella.perucca@mathematik.uni-regensburg.de
Coauthors: Christophe Debry

We consider the reductions of some given number field and in particular of some fixed (non-zero) algebraic number a. Let a prime number ℓ be given. We study the following question: How often is the multiplicative oder of the reduction of a coprime to ℓ? In the sixties Hasse provided a closed-formula for the corresponding natural density. We generalise his result from the rational numbers to any number field and to several algebraic numbers.

On the diophantine equation $1 + 2^a + x^b = y^n$

István Pink
University of Debrecen, Paris Lodron Universität Salzburg
pinki@science.unideb.hu, istvan.pink@sbg.ac.at
Coauthors: Lajos Hajdu

Recently, mixed polynomial-exponential equations similar to the one in the title have been considered by many authors. In these results a certain non-coprimality condition plays an important role.

In this talk we completely solve the title equation for odd positive integers x with $x < 50$. Since we avoid the mentioned non-coprimality condition, this can be considered as a partial completion of the above mentioned results.

It seems that the deep effective tools (such as Baker's method) alone are not capable to handle the problem. We combine local arguments and Baker's method to prove our results.

On the distribution of consecutive gaps between primes

János Pintz

Alfréd Rényi Institute of Mathematics

pintz@mta.renyi.hu

The method of Maynard-Tao showed that we have for any k infinitely many chains of k consecutive primes in bounded intervals of length $C(k)$, where $C(k)$ depends only on k. The method turned to be applicable for the solution of other problems on consecutive primes. The most famous application is the solution of the 76 year-old conjecture of Erdős-Rankin about large prime gaps by Ford-Green-Konyagin-Maynard-Tao. In the lecture some other applications will be mentioned which give full or partial solutions of other 60-70 year-old conjectures, mostly due to Erdős and his coauthors. A particular example is a positive answer to a conjecture of Erdős, Pólya, and Turán. They conjectured that the necessary and sufficient condition that a fixed linear combination of k consecutive prime gaps should take infinitely often both positive and negative values is that the non zero coefficients should not all be the same sign

On common structure of n_k's for which $n_k\alpha \bmod 1 \to x$

Štefan Porubský

Academy of Sciences of the Czech Republic

sporubsky@hotmail.com

Coauthors: Oto Strauch

A. Dubickas [2,Theorem 1] proved the following result:

Theorem. *Let α be a real quadratic algebraic number, and let*[1] $1 \geq \varepsilon_1 \geq \varepsilon_2 \geq \varepsilon_3 \geq \dots$ *be a sequence of real numbers such that $\varepsilon_n \to 0$ as $n \to \infty$. Then there exists an increasing sequence of positive integers $n_1 < n_2 < \dots$ satisfying $\varepsilon_k \leq \frac{k}{n_k}$ for each $k \geq 1$ such that $\lim_{k\to\infty}\{n_k\alpha\} = 0$.*

Dubickas simultaneously showed that condition $\lim_{k\to\infty} \varepsilon_k = 0$ cannot be weakened [2, Theorem 2]. Bugeaud [1] using tools from the theory of continued fractions proved:

Theorem. *Let α be an irrational number and S a finite subset of $[0,1]$. Let $1 \geq \varepsilon_k \geq 0$, $k = 1, 2, \dots$, be a given decreasing sequence of real numbers such that $\lim_{k\to\infty} \varepsilon_k = 0$. Then there exists an increasing sequence of positive integers $n_1 < n_2 < \dots$ satisfying $\varepsilon_k \leq \frac{k}{n_k}$ for each $k \geq 1$ such that the set of limit points of $\{n_k\alpha\}$ coincides with S.*

Recently L.Mišík [3] proved the following generalization in direction of the set of limit points:

Theorem. *Let $X \subset [0,1]$ be a closed set, α be an irrational number, and $\varepsilon_n \leq 1$ be an arbitrary decreasing sequence such that $\lim_{k\to\infty} \varepsilon_k = 0$. Then there exists a sequence $n_1 < n_2 < \dots$ of positive integers such that the set of limit points of $\{n_k\alpha\}$ coincides with X and $\varepsilon_k + |X| \leq \frac{k}{n_k}$ for each $k \geq 1$, where $|X|$ denotes the Lebesgue's measure of X.*

[1] The decreasing property of the sequence ε_n is clearly not a limitation for one can redefine the sequence without loss of generality by taking $\varepsilon_k = \sup_{j\geq k} \varepsilon_j$.

In our talk we show that Dubickas result holds for every irrational α and every $x \in [0,1]$ while the sequence $n_k(x)$ can be subject to additional conditions. One of this conditions extends properties of the set $A = \{n \in \mathbb{N} : \{n\alpha\} \in I\}$ investigated in [4].

We show a construction of sequences n_k, $k = 1, 2, \ldots$, for which the fractional parts $\{n_k\alpha\}$ converges to a fixed but arbitrary $x \in [0,1]$ and $k/n_k \geq \varepsilon_k$ for $k = 1, 2, \ldots$. Here $\{n_k\alpha\} \in I_j$ for $k_{j-1} < k \leq k_j$ and the length $|I_j| = \{h_j\alpha\}$, where h_j is a positive integer for $j = 1, 2, \ldots$ and where the increasing sequence k_j is independent of x. Moreover, the differences $n_{k+1} - n_k$ satisfy the three gaps property with parameters a_j, b_j and $a_j + b_j$ not depending on x for every $k_{j-1} < k < k_j$ and $j = 2, 3, \ldots$. More precisely, we have

Theorem. *Let α be an irrational number and $\varepsilon_j \leq 1$, $j = 1, 2, \ldots$, be a decreasing sequence of positive numbers tending to 0. Then for every $x \in [0,1]$ there exist*

- *an increasing sequence $n_k(x)$, $k = 1, 2, \ldots$, of positive integers,*
- *an increasing sequence k_j, $j = 1, 2, \ldots$, of positive integers independent of x,*
- *a sequence of pairs a_j, b_j, $j = 1, 2, \ldots$, also independent of x, such that*

  (I) $\{n_k(x)\alpha\} \to x$,

  (II) $\varepsilon_k \leq \frac{k}{n_k(x)}$ *for* $k = 1, 2, \ldots$, *and*

  (III) *for every k, $k_{j-1} < k \leq k_j$, $j = 2, 3, \ldots$, we have*

$$n_{k+1}(x) - n_k(x) = \begin{cases} a_j, & \text{or} \\ b_j, & \text{or} \\ a_j + b_j, & \end{cases}$$

where a_j and b_j are coprime for every $j = 1, 2, \ldots$.

We also show using Slater's Theorem that the differences $n_{k+1}(x) - n_k(x)$ can be characterized in the spirit of this Theorem (and independently of x).

References

[1] Bugeaud, Y., On sequences $(a_n\xi)_{n\geq 1}$ converging modulo 1, Proc. Amer. Math. Soc. 137 (2009), 8, 2609-2612.

[2] Dubickas, A., On the limit points of $(a_n\xi)_{n=1}^{\infty}$ mod 1 for slowly increasing integer sequences $(a_n)_{n=1}^{\infty}$, Proc. Amer. Math. Soc. 137 (2009), 8, 449-456.

[3] Mišík, L., On limit points of subsequences of uniformly distributed sequences, Acta Arith. Acta Arith. 165 (2014), 4, 333-338.

[4] Porubský, Š. and Strauch, O., Binary sequences generated by sequences $n\alpha$, n=1,2,..., Publ. Math. Debrecen 77 (2010), 1-2, 139-170.

[5] Porubský, Š. and Strauch, O., On common structure of n_k's for which $n_k\alpha \bmod 1 \to x$, Publ. Math. Debrecen (2015), to appear.

[6] Strauch, O. and Porubský, Š., *Distribution of Sequences: A Sampler*, Schriftenreihe der Slowakischen Akademie der Wissenschaften 1, Peter Lang, Bern, 2005 (revised and extended electronic edition `https://math.boku.ac.at/udt/`)

A note on the shuffle variant of Jeśmanowicz' conjecture

Zsolt Rábai

University of Debrecen

zsrabai@science.unideb.hu

Let (a, b, c) be a primitive Pythagorean triple. In 1956, Jeśmanowicz conjectured that the equation $a^x + b^y = c^z$ has the unique solution $(x, y, z) = (2, 2, 2)$ in positive integers. In 2010 Miyazaki proposed a similar problem. He conjectured that if (a, b, c) is again a primitive Pythagorean triple with b even, then the equation $c^x + b^y = a^z$ with x, y and z positive integers has the unique solution $(x, y, z) = (1, 1, 2)$ if $c = b + 1$ and no solutions if $c > b + 1$. He also proved that his conjecture is true if $c \equiv 1 \pmod{b}$. In our talk, we extend Miyazaki's result to the case $c \equiv 1 \pmod{b/2^{\mathrm{ord}_2(b)}}$.

Recent results on r-Lah polynomials

Gabriella Rácz

University of Debrecen

racz.gabriella@gmail.hu

Coauthors: Gábor Nyul

In enumerative combinatorics, Bell polynomials $B_n(x) = \sum_{k=0}^{n} \left\{ {n \atop k} \right\} x^k$ play an important role, where $\left\{ {n \atop k} \right\}$ denotes a Stirling number of the second kind. In our talk, we will investigate a relative of these polynomials. Namely, we substitute Stirling numbers with r-Lah numbers, generalizations of Lah numbers.

Before studying these polynomials, we give a detailed overview of properties of r-Lah numbers. Based on these results, we present a combinatorial interpretation of r-Lah polynomials, further we give their recurrence, connection between r-Lah and $(r - s)$-Lah polynomials, Spivey and Dobiński type identities, exponential generating function, and we prove that the roots are real.

Upper and lower bounds for $\frac{L_d(1)}{L_d(2)}$ and related results

G Sudhaamsh Mohan Reddy

Icfai Foundation for Higher Education

sudhamsh@ifheindia.org

Coauthors: S Srinivas Rau, B Uma

Let d be the discriminant of a quadratic field $K = Q(\sqrt{d})$.(a) We estimate the ratio of L-function values $\frac{L_d(1)}{L_d(2)} \leq \frac{\zeta(2)}{\zeta(3)} \prod_{p|d}(1 + \frac{1}{p})$. (b) We deduce that the asymptotic density of squarefree ideals in the integer ring $\bigcirc_{\mathbf{K}}$ is less than $\frac{5}{6}$. (c) We obtain a bound for $\frac{L_d(1)}{L_d(2)}$ by using $\prod_{p|d}(1+\frac{1}{p}) = \frac{\sigma(d)}{d} \approx loglogd$ for almost all d. For this we give a direct proof that $\prod_{p \leq x}(1 + \frac{1}{p}) = clogx + \bigcirc(1)$. (d) We obtain a bound $\mathrm{Mean}\{\frac{L_d(1)}{L_d(2)}\} \leq \frac{25}{12}$. (e) It is shown that $L_d(1) = \bigcirc_{\omega(d)}(L_d(2))$ and the unboundedness of $\{L_d(1)\}$ and $\{\frac{L_d(1)}{L_d(2)}\}$ is discussed.

On Selbergs mollification method in the theory of L-functions.

Irina Rezvyakova

Steklov Mathematical Institute

irezvyakova@gmail.com, rezvyakova@mi.ras.ru

Selberg's mollification method plays a crucial role in the theory of L-functions. We shall discuss a certain choice of the mollifier for a given L-function from Selberg class, which gives a chance to prove simultaneously Selberg's positive proportion theorem for the zeros of L-function lying on the critical line and Selberg's density theorem. Also, some results connected with these two theorems will be mentioned.

Some new necessary conditions for the existence of an odd perfect number

Neville Robbins

San Francisco State University

nrobbins@sfsu.edu

Let m denote the least odd perfect number. Using the theory of integer compositions, we prove that (1) 3 does not divide m; (2) there is another odd perfect number, M , such that M is between m and $6m$.

An asymptotic distribution for $|L'/L(1,\chi)|$

Sumaia Saad Eddin

University of Linz

sumaia.saad_eddin@jku.at

Let χ be a Dirichlet character modulo q, let $L(s,\chi)$ be the attached Dirichlet L-function, and let $L'(s,\chi)$ denotes its derivative with respect to the complex variable s. The values at 1 of Dirichlet L-series has received considerable attention, due to their algebraical or geometrical interpretation. Let us mention, in particular, the Birch and Swinnerton-Dyer conjectures, the Kolyvagin Theorem and the Gross-Stark conjecture. Less is known about L'/L evaluated also at the point $s = 1$, through these values are known to be fundamental in studying the distribution of primes since Dirichlet in 1837. In this talk, we show that the values $|L'/L(1,\chi)|$ behave according to a distribution law. The key to this result is to give an asymptotic formula of the $2k$-th power mean value of $|L'/L(1,\chi)|$ when χ ranges a primitive Dirichlet character modulo q for q prime.

About division quaternion algebras and division symbol algebras

Diana Savin

Ovidius University

dianet72@yahoo.com

In this paper, we find a class of division quaternion algebras over the field $\mathbb{Q}(i)$ and a class of division symbol algebras over a cyclotomic field.

Normality in Pisot numeration systems

Adrian Scheerer

Technische Universität Graz

scheerer@math.tugraz.at

Copeland and Erdős showed that the concatenation of primes when written in base 10 yields a real number that is normal to base 10. We give a polynomial generalization of this result to bases that are no longer integers.

More precisely, let the underlying base β be a Pisot number in which all integers have finite expansion. Then the concatenation of the values at the primes of a polynomial when written in

base β gives the expansion of a real number normal to that base.

In this talk we will give a very quick overview over normal numbers (both in integer and real bases) and demonstrate the two main ingredients of the proof: A theorem of Bertrand-Mathis and Volkmann; and logarithmic growth behaviour of the expansions of integers in base β.

Del Pezzo surfaces of degree four violating the Hasse principle

Damaris Schindler

Hausdorff Center for Mathematics

Damaris.Schindler@hcm.uni-bonn.de

Coauthors: J. Jahnel

We show that, over every number field, the degree four del Pezzo surfaces that violate the Hasse principle are Zariski dense in the moduli scheme.

Diophantine approximation on manifolds

Johannes Schleischitz

University of Natural Resources and Life Sciences

johannes.schleischitz@boku.ac.at

The talk deals with the rational approximation properties of smooth manifolds M in Euclidean space $\mathbb{R}^k$. More precisely, for a parameter $\nu > 0$ we investigate the set of points $a = (a_1, ldots, a_k)$ on M that are approximable to degree ν, which means that the system $\max_{1\leq j\leq k} |p_j/q - a_j| \leq q^{-\nu-1}$ has an integral solution vector $(q, p_1, \ldots, p_k) \in \mathbb{Z}^{k+1}$ for arbitrarily large q. By Dirichlet's Theorem any point in $\mathbb{R}^k$ is approximable to degree $1/k$, and almost all to no higher degree. Restricting to $a \in M$ for a sufficiently smooth manifold $M \subset \mathbb{R}^k$ that satisfies some natural regularity conditions, again only a small subset of M is approximable to a degree higher than $1/k$. The question of the Hausdorff dimensions of sets of points on M approximable to a given degree $\nu > 1/k$ arises. The talk aims to sketch selected results for special choices of M, without proofs.

Koecher-Maaß series and representation of quadratic forms

Rainer Schulze-Pillot

Universität des Saarlandes

schulzep@math.uni-sb.de

The Kocher-Maaß series of a Siegel modular form is a Dirichlet series whose coefficient $a(F, d)$ at d^{-s} is the average of the Fourier coefficients of F at symmetric matrices T of determinant d.

If F is a theta series of degree 2 of a positive definite integral quadratic form in 4 variables we can use the special shape of the Clifford algebra in this situation to prove an asymptotic formula for the coefficients $a(F, d)$ of the associated Koecher-Maaß series. This allows to draw new conclusions about representations of binary quadratic forms by quaternary quadratic forms, a case which can not be treated by the available asymptotic formulas for individual Fourier coefficients. It is an open question whether this can be generalized to other dimensions and degrees.

On a connection between pseudorandom measures

Richárd Sebők
Eötvös Loránd University
sebokr@cs.elte.hu

Mauduit and Sárközy proved the following connection between the well-distribution measure and the correlation measure of order 2: $W(E_N) \leq 3\sqrt{NC_2(E_N)}$. In my talk I will speak on the generalization of this result to get similar connection between the combined PR-measure and the correlations of even order.

Number of solutions of Thue inequalities

Divyum Sharma
Tata Institute of Fundamental Research, Mumbai
divyum@math.tifr.res.in
Coauthors: N. Saradha

Let $F(X,Y) \in \mathbb{Z}[X,Y]$ be a form of degree $r \geq 3$, irreducible over $\mathbb{Q}$ and having at most $s+1$ non-zero coefficients. Let h be a non-zero integer. Siegel proposed that the number $N_F(h)$ of integer solutions of the Thue inequality

$$|F(X,Y)| \leq h$$

may be bounded only in terms of s and h. Mueller and Schmidt showed that

$$N_F(h) \ll s^2 h^{2/r}(1 + \log h^{1/r}).$$

Further, they conjectured that s^2 may be replaced by s. In this talk, I present some recent contributions in this direction.
Also, when $r = 3$ and the discriminant D of F is positive, we present improved upper bounds for the number of primitive solutions of the Thue inequality

$$|F(X,Y)| \leq h,$$

where h is a positive integer satisfying

$$h < \frac{(3D)^{1/4}}{2\pi}.$$

On the quadratic forms of five variables

Ketevan Shavgulidze
Tbilisi State University
ketevan.shavgulidze@tsu.ge

A homogeneous polynomial $P(X) = P(x_1, \cdots, x_r)$ of degree ν with complex coefficients, satisfying the condition

$$\sum_{1 \leq i,j \leq r} a_{ij}^* \Big(\frac{\partial^2 P}{\partial x_i \partial x_j} \Big) = 0$$

is called a spherical polynomial of order ν with respect to $Q(X)$, and

$$\vartheta(\tau, P, Q) = \sum_{n \in \mathbb{Z}^r} P(n) z^{Q(n)}, \qquad z = e^{2\pi i \tau}, \qquad \tau \in \mathbb{C}, \qquad \operatorname{Im} \tau > 0$$

is the corresponding generalized r-fold theta-series, where

$$Q(X) = Q(x_1, \cdots, x_r) = \sum_{1 \le i \le j \le r} b_{ij} x_i x_j.$$

In this paper the spherical polynomials with quadratic form of five variables are constructed and the basis of the space of these spherical polynomials is established.The upper bound of dimension of vector spaces of generalized theta-series corresponding to some quadratic form of five variables is considered.

One class field via hypergeometric modular function

Hironori Shiga

Chiba University

shiga@math.s.chiba-u.ac.jp

Starting from the hypergeometric functions of 2-variables, we can construct explicit modular functions on $\mathbf{B}^2$ (the 2-dimensional complex hyper-ball). They are called Picard modular functions. As their application, we show

(1) a modular function for an arithmetic triangle group $\Delta(3, 3, 5)$ together with its theta constant representation, (2) an explicit defining equation of a Hilbert class field of a quartic CM field.

Main ideas are coming from the thesis of J. Voight and the theory of complex multiplication by G. Shimura together with speaker's old works.

A note on Stirling type numbers and Array type polynomials

Yilmaz Simsek

University of Akdeniz

ysimsek@akdeniz.edu.tr

In this paper, we construct new generating functions for the Stirling type numbers and Array type polynomials. By using these generating functions, we derive many properties and identities related to these numbers and polynomials. We also give some combinatorics identities and combinatorics sums for these numbers and polynomials.

Transcendence of generalized Euler-Lehmer constants

Sneh Bala Sinha

Harish Chandra Research Institute

snehbala@hri.res.in

Coauthors: Sanoli Gun, Ekata Saha

In this article, we study the arithmetic properties of generalized Euler-Lehmer constants. We show that these infinite family of numbers are transcendental with at most one exception. This result generalizes a recent result of Murty and Zaytseva.

Problems in additive combinatorics

József Solymosi

University of British Columbia

solymosi@math.ubc.ca

Some questions in number theory can be transformed to a problem of bounding point-line incidences or point-curve incidences over some field. I will talk about the history of incidence bounds, applications, and I will mention some recent results.

Quadratic residues and difference sets mod p

Jack Sonn

Technion Israel Institute of Technology

sonn.jack@gmail.com

Coauthors: Vsevolod F. Lev

It has been conjectured by Sárközy that with finitely many exceptions, the set of quadratic residues modulo a prime p cannot be represented as a sumset $\{a+b\colon a\in A, b\in B\}$ with non-singleton $A, B\subseteq \mathbb{F}_p$. The case $A=B$ of this conjecture has been recently established by Shkredov. The analogous problem for differences remains open: is it true that for all sufficiently large primes p, the set of quadratic residues modulo p is not of the form $\{a'-a''\colon a', a''\in A,\ a'\neq a''\}$ with $A\subseteq \mathbb{F}_p$?

We have attacked a presumably more tractable variant of this problem, which is to show that (with finitely many exceptions) there is no p for which there is an $A\subseteq \mathbb{F}_p$ such that every quadratic residue has a *unique* representation as $a'-a''$ with $a', a''\in A$, and no non-residue is represented in this form. We have found a number of necessary conditions for the existence of such p, involving for the most part the behavior of primes dividing $p-1$. These conditions enable us to rule out all primes p in the range $13<p<10^{18}$ (the primes $p=5$ and $p=13$ being conjecturally the only exceptions).

The talk will focus on an algebraic number theory aspect of this joint work with Seva Lev.

On the Diophantine equation $(x+1)^k+(x+2)^k+...+(lx)^k=y^n$

Gökhan Soydan

Uludağ University

gsoydan@uludag.edu.tr

Let $k\geq 2$ fixed integers. In this work, firstly, we prove that all solution of the equation $(x+1)^k+(x+2)^k+...+(lx)^k=G(x)=y^n$ in integers x, y, n with $x, y\geq 1, n\geq 2$ satisfy $n<C_1$ where $C_1=C_1(G,k)$ is an effectively computable constant. Secondly we prove that all solution of this equation in integers x, y, n with $x, y\geq 1, n\geq 2, k\neq 3$ and $l\equiv 0 \pmod 2$ satisfy $\max\{x, y, n\}<C_2$ where C_2 is an effectively computable constant depending only on G and k.

References

[1] B. Brindza, *On some generalizations of the Diophantine equation* $1^k+2^k+...+x^k=y^z$, Acta Arith. **44** (1984), 99-107.

[2] B. Brindza, *On S-integral solutions of the equation* $y^m=f(x)$, Acta Math. Hung. **44** (1984), 133-139.

[3] K. Győry, R. Tijdeman and M. Voorhoeve, *On the equation* $1^k+2^k+...+x^k=y^z$ Acta Arith. **37** (1980), 234-240.

[4] K. Győry and Á. Pintér, *On the equation* $1^k+2^k+...+x^k=y^z$, Publ. Math. Debrecen **62** (2003), 403-414.

[5] C. Rakaczki, *On some generalizations of the Diophantine equation* $s(1^k+2^k+...+x^k)+r=dy^n$, Acta Arith. **151** (2012), 201-216.

[6] H. Rademacher, *Topics in Analytic Number Theory,* Springer, Berlin, 1973, ISBN 978-3-642-80617-9.
[7] J. J. Schäffer, *The equation* $1^p + 2^p + ... + n^p = m^q$*,* Acta Math. **95** (1956), 155-189.
[8] A. Schinzel and R. Tijdeman, *On the equation* $y^m = P(x)$*,* Acta Arith **31** (1976), 199-204.
[9] M. Voorhoeve, K. Győry and R. Tijdeman, *On the equation* $1^k + 2^k + ... + x^k + R(x) = y^z$*,* Acta Math. **143** (1979), 1-8; Corrigendum Acta Math. **159** (1987), 151-152.
[10] Z. Zhang, *On the Diophantine equation* $(x-1)^k + x^k + (x+1)^k = y^n$*,* Publ. Math. Debrecen **85** (2014), 93-100.

Universality of the Epstein zeta function

Anders Södergren
University of Copenhagen
sodergren@math.ku.dk
Coauthors: Johan Andersson

Voronin's remarkable universality theorem states that any non-vanishing holomorphic function in $\{s \in \mathbb{C} : |s - 3/4| \leq r\}$ $(r < 1/4)$ can be approximated arbitrarily well by vertical shifts of the Riemann zeta-function. Similar universality properties has been proved for large classes of zeta and L-functions. In this talk we discuss several results regarding the universality of the Epstein zeta function in the lattice variable (in the limit of large lattice dimension). In particular we describe a universality theorem that is valid also in the half-plane where the Epstein zeta function is absolutely convergent.

Brauer relations in positive characteristic

Matthew Spencer
University of Warwick
m.j.spencer@warwick.ac.uk
Coauthors: Alex Bartel

Given a finite group G and a finite G-set we may constructs its associated permutation representation over a field k, this extends to a ring homomorphism from the Burnside ring $b(G)$ to the k-representation ring $\mathcal{R}_k(G)$. In this talk we will describe the kernel of this map, particularly when k has positive characteristic. Then we will see how Brauer relations may applied in a number theoretic setting, for example via the use of regulator constants.

Powers of Salem numbers and distribution modulo 1

Dragan Stankov
University of Belgrade
dstankov@rgf.bg.ac.rs

Let θ be a Salem number and $P(x)$ a polynomial. It is well-known that the sequence (θ^n) modulo 1 is dense but not equidistributed. In this article we discuss sequence $(P(\theta^n))$ modulo 1. Our first approach is computational and consists in estimating the number of n so that the fractional part of $(P(\theta^n))$ falls into a subinterval of a partition of $[0, 1]$. If Salem number is of degree 4 we can obtain explicit density function of the sequence, using an algorithm which is also given. Some examples confirm that these two approaches give the same result.

Supnorms of half-integral weight Modular Forms

Raphael S. Steiner
University of Bristol
raphael.steiner@bristol.ac.uk

We give subconvex upper bounds on the supnorm of half-integral weight Hecke-eigenforms in the Kohnen plus space of level 4 in the weight aspect. This is achieved by combining bounds for both the Fourier expansion and for an amplified Bergman Kernel. The methods further generalise to arbitrary real weight.

Elliptic divisibility sequences and modular units

Marco Streng
Universiteit Leiden
streng@math.leidenuniv.nl

The modular curve $Y^1(N)$ parametrises pairs (E, P), where E is an elliptic curve and P is a point of order N on E, up to isomorphism. A *unit* on the affine curve $Y^1(N)$ is a holomorphic function that is nowhere zero. These functions have applications to number theory and cryptography, which I will give in the talk.

The main result is a way of generating generators (sic) of this group using a recurrence relation. The generators are essentially the defining equations of $Y^1(n)$ for $n < (N+3)/2$, and they form an elliptic divisibility sequence. This result proves a conjecture of Maarten Derickx and Mark van Hoeij.

Some results on the zeros of the derivatives of the Riemann zeta function and Dirichlet L-functions

Ade Irma Suriajaya
Nagoya University
m12026a@math.nagoya-u.ac.jp

The number of zeros and the distribution of the real part of non-real zeros of the derivatives of the Riemann zeta function have been investigated by Berndt, Levinson, Montgomery, and Akatsuka. Berndt, Levinson, and Montgomery investigated the general case, meanwhile Akatsuka gave sharper estimates for the first derivative of the Riemann zeta function under the truth of the Riemann hypothesis.

Many properties of the zeros of the derivatives of the Dirichlet L-functions associated with primitive Dirichlet characters were studied by Yildirim. Among, Yildirim also studied the number of zeros.

In this talk, we introduce a generalization of the results of Akatsuka to the k-th derivative (for positive integer k) of the Riemann zeta function. We also give a sharper estimate to the result of Yildirim on the number of zeros for the first derivative of the Dirichlet L-functions associated with primitive Dirichlet characters under the assumption of the generalized Riemann hypothesis.

Power integral bases in quartic fields and quartic extensions

Tímea Szabó

University of Debrecen

szabo.timea@science.unideb.hu

Coauthors: István Gaál

The number field K of degree n is called monogene if it admits a power integral basis of type $(1, \alpha, \ldots, \alpha^{n-1})$. We consider the problem of monogenity in infinite parametric families of quartic number fields. We also consider the relative case, we study relative monogenity in infinite parametric families of quartic relative extensions.

Sum of certain elements in Pascal-type triangles

László Szalay

University of West Hungary

szalay.laszlo@emk.nyme.hu

There exist several variations of Pascal's arithmetic triangle. Besides the well known types, we introduce an unprecedenten generalization, based on some specific graphs. Moreover, a survey on different sums linked the triangles will be presented.

Bounds and formulas for a Jacobsthal-type function in sequences

Márton Szikszai

University of Debrecen

szikszai.marton@science.unideb.hu

Let $j(n)$ be the ordinary Jacobsthal function, that is, the smallest k such that among every k consecutive integers there is one which is coprime to n. In this talk I am going to introduce a Jacobsthal-like function for sequences, replacing consecutive integers with consecutive terms of an integer sequence in the above definition. Beside theoretical upper bounds and formulas for certain well-known families of sequences computational experience on the goodness of these results will be presented. I will also speak about a problematic general situation.

Symmetries for heights on split tori

Valerio Talamanca

Università degli studi "Roma Tre"

valerio@mat.uniroma3.it

Let T_d denote the d-dimensional split torus defined over a number field k. Given a rational representation $\rho : T_d \to GL_n$ we define an height function H_ρ on $T_d(\overline{k})$ by setting $H_\rho(g) = H_s(\rho(g))$ where H_s denotes the spectral height on GL_n. We study the group of symmetries of this height function, namely:

$$\mathcal{H}_\rho = \left\{\varphi \in \mathrm{Aut}(T_d) \;\middle|\; H_\rho(\varphi(g)) = H_\rho(g)\ \forall g \in T_d(\overline{k})\right\}$$

Clearly $\mathcal{H}_\rho$ contains the pull back via ρ of the relative Weyl group of $\rho(T_d)$. One of our main results is the following:

Theorem. *If ρ is a standard realization of T_d as the maximal torus of a classical group, then $\mathcal{H}_\rho$ coincide with the pull back via ρ of the Weyl group of $\rho(T_d)$.*

We also provide several examples in which $\mathcal{H}_\rho$ contains strictly the pull back via ρ of the Weyl group of $\rho(T_d)$.

Rational functions and arithmetic progressions

Szabolcs Tengely
University of Debrecen
tengely@science.unideb.hu

Pethő and Tengely proved the following theorem related to composite rational functions.

Theorem. *Let k be an algebraically closed field of characteristic zero. If $f, g, h \in k(x)$ with*

$$f(x) = g(h(x))$$

and with $\deg g, \deg h \geq 2$, g not of the shape $(\lambda(x))^m, m \in \mathbb{N}, \lambda \in PGL_2(k)$, and f has 3 zeros and poles altogether, then f is equivalent to one of the following rational functions

(a)

$$\frac{(x-\alpha_1)^{k_1}(x+1/4-\alpha_1)^{2k_2}}{(x-1/4-\alpha_1)^{2k_1+2k_2}}$$

for some $\alpha_1 \in k$ and $k_1, k_2 \in \mathbb{Z}, k_1 + k_2 \neq 0$,

(b)

$$\frac{(x-\alpha_1)^{2k_1}(x+\alpha_1-2\alpha_2)^{2k_2}}{(x-\alpha_2)^{2k_1+2k_2}}$$

for some $\alpha_1, \alpha_2 \in k$ and $k_1, k_2 \in \mathbb{Z}, k_1 + k_2 \neq 0$.

We note that in both cases the zeros and poles form an arithmetic progression:

$$\alpha_1 - \frac{1}{4}, \alpha_1, \alpha_1 + \frac{1}{4}, \quad \text{difference} = \frac{1}{4}$$

and

$$\alpha_1, \alpha_2, 2\alpha_2 - \alpha_1, \quad \text{difference} = \alpha_2 - \alpha_1.$$

In this talk we show how to determine possible values of the differences if f has more than 3 zeros and poles altogether.

Towards the modularity of elliptic curves over totally real fields

Jack Thorne
University of Cambridge
thorne.@dpmms.cam.ac.uk

Since 2001 we have known, thanks to the works of Wiles and Breuil, Conrad, Diamond, and Taylor, that all elliptic curves over $\mathbb{Q}$ are modular, i.e. arise from modular forms. Advances in the theory of modularity of Galois representations since that time (especially thanks to Kisin) have made the modularity of elliptic curves over all totally real fields a realistic goal. I will discuss recent progress towards this problem.

S-adic words, Rauzy fractals, and torus rotations

Joerg Thuswaldner
University of Leoben
joerg.thuswaldner@unileoben.ac.at
Coauthors: V. Berthé, W. Steiner

In the 1970ies G.Rauzy devised a proof of the fact that Sturmian words are natural codings of rotations on the 1-dimensional torus using classical continued fraction expansions. In an attempt to generalize this to higher dimensions, Arnoux and Rauzy (1991) invented sequences over three letters, now called Arnoux-Rauzy words. They conjectured that each of these words codes a rotation on the 2-torus. In the meantime, this conjecture only could be confirmed on some "periodic" examples. Moreover, pathological counterexamples have been given by Cassaigne, Ferenczi, and Zamboni (2000).

We set up a general theory for the geometry of S-adic sequences that leads to a proof of the conjecture of Arnoux and Rauzy for almost all Arnoux-Rauzy words (w.r.t. a natural measure). Besides that we give non-periodic Arnoux-Rauzy words fulfilling the conjecture. Moreover, we give examples for our new theory that correspond to S-adic words defined in terms of Brun's continued fraction algorithm.

Arithmetic dynamical systems

Robert Tichy
Technische Universität Graz
tichy@tugraz.at

We start from the concept of dynamical systems and show some applications to number theoretic problems, including normal numbers and computability. Normality is investigated also from a probabilistic and quantitative point of you. This includes sharp bounds for related discrepancies. Furthermore, we present characterizations of bounded remainder sets of some multidimensional sequences. This explains distribution properties of the classical Halton sequences and various analogues for linear-recurring base sequences. The second part of the lecture is devoted to van der Corput sets and sets of recurrence. We give new constructions involving equidistribution of sequences of prime powers. This refines and unifies earlier results obtained by Sárközy, Furstenberg, Kamae and Mendés France and Bergelson and Lesigne. The proofs heavily depend on analytic machinery involving bounds for exponential sums. We conclude with applications to diophantine inequalities.

On P-integers

Alain Togbé
Purdue University North Central
atogbe@pnc.edu
Coauthors: Shichun Yang

Let $k > 1$ be an integer, $\varphi(k)$ be Euler's totient function and $\omega(k)$ the number of distinct prime divisors of k. We say that k is a P-integer if the first $\varphi(k)$ primes coprime to k form a reduced residue system modulo k.

During this talk, we will discuss the progress made to prove that if k is a P-integer, then $k \in \{2, 4, 6, 12, 18, 30\}$.

On certain pairs of q-series identities

Pee Choon Toh

Nanyang Technological University

peechoon.toh@nie.edu.sg

Hirschhorn recently proved a pair of interesting q-series identities that interlinked the coefficients of two infinite products. Using the theory of modular forms, we extend his results from $p = 5$ to other primes and provide another two pairs of infinite products sharing similar properties.

A new bound on Diophantine quintuples

Tim Trudgian

The Australian National University

timothy.trudgian@anu.edu.au

Consider the set $\{1, 3, 8, 120\}$. This has the property that the product of any two of its elements is one less than a square. A Diophantine quintuple is a set of five distinct elements with this property. It is known that there are only finitely many Diophantine quintuples; it is conjectured that there are none.

I shall give a brief overview of my recent work that has led to what is currently the best upper bound on the number of Diophantine quintuples.

Relative genus theory and Iwasawa μ-invariants for rational homology 3-spheres

Jun Ueki

Kyushu University

uekijun46@gmail.com

Following the analogies between knots and primes ([3 [4]), we translate some classical results of number theory into 3-dimensional topology ([7],[8],[9]). We establish an analogue of relative genus theory ([1]) for a branched cover of rational homology 3-spheres, with use of Niibo's idèle theory ([5], [6]). Then we formulate analogues of Iwasawa's theorems on the Iwasawa μ-invariants in $\mathbb{Z}_p$-fields extensions ([2]) for branched $\mathbb{Z}_p$-covers of rational homology 3-spheres.

References

[1] Yoshiomi Furuta, *The genus field and genus number in algebraic number fields*, Nagoya Math. J., 29:281–285, 1967.

[2] Kenkichi Iwasawa, *On the μ-invariants of $\mathbb{Z}_l$-extensions*, In Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki, pages 1–11. Kinokuniya, Tokyo, 1973.

[3] Barry Mazur, *Remark on alexander polynomial*, unpublished note, 1963–64.

[4] Masanori Morishita, *Knots and primes*, Universitext. Springer, London, 2012. An introduction to arithmetic topology.

[5] Hirofumi Niibo, *Idèlic class field theory for 3-manifolds*, Kyushu J. Math, 68(2):421–436, 2014.

[6] Hirofumi Niibo and Jun Ueki, *Idelic class field theory for 3-manifolds and very admissible links*, submitted.

[7] Jun Ueki, *On the homology of branched coverings of 3-manifolds*, Nagoya Math. J., 213:21–39, 2014.
[8] Jun Ueki, *On the Iwasawa invariants for links and Kida's formula*, submitted.
[9] Jun Ueki, *On the Iwasawa μ-invariants of branched $\mathbb{Z}_p$-covers*, submitted.

Primitive integer solutions of certain Diophantine equations

Maciej Ulas
Institute of Mathematics of the Jagiellonian University
maciej.ulas@uj.edu.pl
Coauthors: Maciej Gawron

We present some results concerning Diophantine equations of the form $T^2 = G(\overline{X})$, $\overline{X} = (X_1, \ldots, X_m)$, where mainly $m = 3$ or $m = 4$ and G specific homogenous quintic form. First, we prove that if $F(x, y, z) = x^2+y^2+az^2+bxy+cyz+dxz \in \mathbb{Z}[x, y, z]$ and $(b-2, 4a-d^2, d) \neq (0, 0, 0)$, then the Diophantine equation $t^2 = nxyzF(x, y, z)$ has solution in polynomials x, y, z, t with integer coefficients, without polynomial common factor of positive degree. In case $a = d = 0, b = 2$ we prove that there are infinitely many primitive integer solutions of the Diophantine equation under consideration. As an application of our result we prove that for each $n \in \mathbb{Q} \setminus \{0\}$ the Diophantine equation

$$T^2 = n(X_1^5 + X_2^5 + X_3^5 + X_4^5)$$

has a solution in co-prime (non-homogenous) polynomials in two variables with integer coefficients. We also present a method which sometimes allow us to prove the existence of primitive integers solutions of more general quintic Diophantine equations of the form $T^2 = aX_1^5 + bX_2^5 + cX_3^5 + dX_4^5$, where $a, b, c, d \in \mathbb{Z}$. In particular, we prove that for each $m, n \in \mathbb{Z} \setminus \{0\}$, the Diophantine equation

$$T^2 = m(X_1^5 - X_2^5) + n^2(X_3^5 - X_4^5)$$

has a solution in polynomials which are co-prime over $\mathbb{Z}[t]$. Moreover, we show how modification of the presented method can be used in order to prove that for each $n \in \mathbb{Q} \setminus \{0\}$, the Diophantine equation

$$t^2 = n(X_1^5 + X_2^5 - 2X_3^5)$$

has a solution in polynomials which are co-prime over $\mathbb{Z}[t]$.

Double Somos-4

Alexey Ustinov
Institute of Applied Mathematics, Khabarovsk Division, Russia
vab@iam.khv.ru
Coauthors: Victor Bykovskii

Let $\{A(n)\}$ and $\{B(n)\}$ be a pair of sequences defined by initial values

$$A(\pm 1), A(0), A(2), \quad B(\pm 1), B(0), B(2),$$

and recurrence relations

$$A(n+2)B(n-2) + \alpha A(n+1)B(n-1) + \beta A(n)B(n) = 0,$$

$$A(n-2)B(n+2) + \gamma A(n-1)B(n+1) + \delta A(n)B(n) = 0.$$

Theorem. The general pair of such sequences (subject to some natural restrictions on initial data) has the form

$$A(n) = e^{an^2+b_1n+c_1}\sigma_\Gamma(nz+z_1), \quad B(n) = e^{an^2+b_2n+c_2}\sigma_\Gamma(nz+z_2),$$

where a, $b_{1,2}$, $c_{1,2}$, z, $z_{1,2} \in \mathbb{C}$ and σ_Γ is Weierstrass σ–function associated with lattice Γ.

The case $A = B$ was previously studied by A. Hone [1] and C. Swart [2].

This work was supported by the RFBR (project no. 14-01-00203)

References

[1] H A. Hone, *Elliptic Curves and Quadratic Recurrence Sequences* Bull. Lon, Math. Soc. 37 2 (2005) 161–171.

[2] S C. Swart *Elliptic curves and related sequences*, PhD thesis, Royal Holloway, University of London (2003).

About two-dimensional sumsets and difference sets

Artem Uvakin

Moscow State University

artemuvakin@gmail.com

The paper is about a generalization of the well-known theorem that if A is an additive set in an ambient abelian group $G = (G, +)$ and $|A + A| \leq \frac{3}{2}|A|$ or $|A - A| \leq \frac{3}{2}|A|$, then $A \subseteq x + H$ for some $x \in G$ and subgroup H of G with $|H| \leq 3/2|A|$.

We established a similar result for higher-dimensional sumset $A^2 + \Delta(A) \subseteq G^2$ and difference set $A^2 - \Delta(A) \subseteq G^2$. Here $A^2 = A \times A$ is a set of pairs of elements of A and $\Delta(A)$ is diagonal set $\Delta(A) = \{(a, a) \in G \times G | a \in A\}$.

Theorem. *If $|A^2 \pm \Delta(A)| < 7/4|A|^2$, then $A \subseteq H + x$ for some $x \in G$ and subgroup H of G with $|H| < 3/2|A|$.*

Representation theory of Drinfeld modular forms

Enrico Varela Roldán

Saarland University

varela@math.uni-sb.de

In the theory of Drinfeld modular forms for the principal congruence subgroup $\Gamma(T)$ we study the natural action of the group $G = \mathrm{GL}(2, \mathbb{F}_q)$. We provide an identification of G-modules occurring in the Drinfeld setting with classical G-modules and describe their structure.

One important tool that is used in these studies is a new type of Eisenstein series for $\Gamma(T)$. These *modified Eisenstein series* show remarkable arithmetical properties and may be of interest in future research.

Number fields generated by Pisot units

Tomáš Vávra

Czech Technical University in Prague

t.vavra@seznam.cz

Coauthors: Francesco Veneziano

It is known due to R. Salem that every real number field can be generated by a Pisot number, i.e. a real algebraic integer $\alpha > 1$ whose conjugates lie inside the unit circle. We show that every real number field can also be generated by a Pisot unit. We provide an algorithm for determining such a generator of the smallest absolute value. We also generalize these results to the case of complex fields and the so-called complex Pisot numbers. In particular, we show that any complex number field that is not CM can be generated by a complex Pisot unit.

On the number of representations of numbers by the binary quadratic forms with discriminants -80, -128 and -140

Teimuraz Vepkhvadze

I.Javakhishvili Tbilisi State University

t-vepkhvadze@hotmail.com

The modular properties of generalized theta-functions with characteristics are used to build cusp forms corresponding to the binary quadratic forms. It gives the opportunity of obtaining formulas for the number of representations of positive integers by all primitive Gaussian binary quadratic forms with discriminants -80,-128 and -140.

A Dobrowolski type minoration of the Mahler measure of height 1 trinomials

Jean-Louis Verger-Gaugry

CNRS, Université de Savoie Mont Blanc

Jean-Louis.Verger-Gaugry@univ-smb.fr

The method of asymptotic expansions is introduced for formulating the roots of the trinomials $G_n(X) = -1+X+X^n, n \geq 2$. This method (divergent formal sums of functions of one or several variables) was originally developped by Poincaré in celestial mechanics (1895), for N- body problems. Denote by θ_n the unique zero of G_n in the interval $(0, 1)$. As a consequence we deduce the asymptotic expansion of the Mahler measure of G_n as a function of n and an improvment of the minoration of Dobrowolski (1979) for the family $(\mathrm{M}(\theta_n^{-1}))$. For the collection of Perron numbers (θ_n^{-1}), which tends to 1, Lehmer's conjecture and Schinzel-Zassenhaus's conjecture are directly solved by this method, without invoking Smyth's Theorem (1971) related to Mahler measures of nonreciprocal polynomials, greater than or equal to the smallest Pisot number. Comparison with previous results of Boyd, Dubickas, Schinzel, Smyth and a recent theorem (2014) of Flammang is proposed.

Periodic Jacobi-Perron algorithm expansions

Paul Voutier

paul.voutier@gmail.com

The Jacobi-Perron Algorithm (JPA) is one of the multi-dimensional generalisations of the continued fraction algorithm. Questions about the periodicity of JPA expansions are a central part of this subject, including the following analogue of Lagrange's result for ordinary continued-fractions.

Question. When $1, \alpha_1, \ldots, \alpha_{n-1} \in \mathbb{R}$ form a $\mathbb{Q}$-basis of a number field of degree n, is the JPA expansion of $(\alpha_1, \ldots, \alpha_{n-1})$ periodic?

In 1991, Levesque and Rhin exhibited infinite families of purely periodic JPA expansions of dimension 3 for all periods of the form $3m + 1$ and $4m + 1$.

In this talk, we generalise the work of Levesque and Rhin to all periods of length $m \geq n \geq 3$ for the JPA of dimension n, producing infinite families of examples, arising from linear recurrence sequences, for each such m and n.

We also discuss the Hasse-Bernstein units that arise from these JPA expansions (analogous to the units from the continued-fraction algorithm), in particular, when $n = 3$ and the unit group is of rank 1.

We conclude with a discussion of some computations and resulting observations on when the JPA expansion of $\left(m^{1/3}, m^{2/3}\right)$ is periodic.

References

[1] C. Levesque, G. Rhin, *Two Families of Periodic Jacobi Algorithms with Period Lengths Going to Infinity*, J. Number Theory 37 (1991), 173–180.

Moduli of p-divisible groups

Jared Weinstein

jaredsweinstein@gmail.com

Coauthors: Peter Scholze

Complex abelian varieties are classified by pairs (V, L), where V is a finite-dimensional complex vector space and L is a lattice in V equipped with a Riemann form. In this talk we discuss a p-adic analogue of this classical result. Let C be a complete and algebraically closed extension of $\mathbb{Q}_p$. We present a classification of p-divisible groups over the ring of integers of C in terms of linear algebra data.

Factorisation of finite graphs and polynomials with nonnegative coefficients

Christiaan van de Woestijne

Montanuniversität Leoben

c.vandewoestijne@unileoben.ac.at

We consider product-like binary operators on classes of finite graphs (with or without loops). Even if we want these operators to be associative and commutative and to distribute over the disjoint union operator, we still have the choice between the Cartesian, direct, and strong products. Obviously, this provides us with many new examples of commutative monoids, for which it would be interesting to determine the cancellation and factorisation properties. I will start by introducing the above-mentioned products, and also present the strong results that are already known this area. Most results, however, are restricted to connected graphs. If we consider the factorisation properties of possibly disconnected graphs, it turns out that the structure is isomorphic to the monoid of polynomials with nonnegative integer coefficients. I will show how the isomorphism works, and also present some new results which completely characterise the nonunique factorisation phenomena in this monoid for polynomials with at most 12 terms.

Ramsey multiplicity of patterns in finite abelian groups

Julia Wolf

University of Bristol

julia.wolf@bristol.ac.uk

It is well known (and a result of Goodman) that a random 2-colouring of the edges of the complete graph K_n contains asymptotically the minimum number of monochromatic triangles (K_3s). Erdős conjectured that this was also true of monochromatic copies of K_4, but his conjecture was disproved by Thomason in 1989. The question of determining for which small graphs GoodmanâĂŹs result holds true remains wide open.

We explore an arithmetic analogue of this question: what can be said about the number of monochromatic additive configurations in 2-colourings of finite abelian groups? The techniques used to address this question, which include additive combinatorics and quadratic Fourier analysis, originate in quantitative approaches to SzemerediâĂŹs theorem. Perhaps surprisingly, some of our results in the arithmetic setting have implications for the original graph-theoretic problem.

Carmichael numbers and variants of Korselt's criterion

Thoms Wright

Wofford College

tjw980@yahoo.com

A Carmichael number is a natural number n for which $a^n \equiv a \pmod{n}$ for every $a \in \mathbb{Z}$ but n is not prime. Korselt showed in 1899 that n being a Carmichael number is equivalent to the statement that n is a square-free positive integer such that for every prime $p|n$, $p-1|n-1$. In this talk, we ask and answer the question of whether there exist n for which $p-b|n-b$ for $b \neq 1$. Our work partially resolves questions that Alford, Granville, and Pomerance posed in 1994.

Certain Combinatoric convolution sums arising from Bernoulli and Euler Polynomials

Nazli Yildiz Ikikardes

Balikesir University

nyildiz@balikesir.edu.tr

Coauthors: Daeyeoul Kim, Abdelmejid Bayad

In this talk, we give relationship between Bernoulli-Euler polynomials and convolution sums of divisor functions. And, we establish three explicit formulas for certain combinatoric convolution sums of divisor functions derived from Bernoulli and Euler polynomials.

First author was supported by The Research Fund of Balikesir University, Project No: 2015/20

References

[1] B. C. Berndt, *Ramanujan's Notebooks, Part II*, Springer-Verlag, New York, 1989.

[2] M. Besge, *Extrait d'une lettre de M. Besge à M. Liouville*, J. Math. Pures Appl., **7**, 1862, 256.

[3] B. Cho, D. Kim, H. Park, *Evaluation of a certain combinatorial convolution sum in higher level cases*, J. Math. Anal. Appl., 406, 2013, no.1 203-210.

[4] W. Chu and R. R. Zhou, *Convolutions of Bernoulli and Euler polynomials*, Sarajevo Journal of Mathematics, Vol. 6 (18), 2010, 147-163.

[5] J. G. Huard, Z. M. Ou, B. K. Spearman, and K. S. Williams, *Elementary evaluation of certain convolution sums involving divisor functions*, Number theory for the millennium, II, 2002, 229-274.
[6] D. Kim and A. Bayad, *Convolution identities for twisted Eisenstein series and twisted divisor functions*, Fixed Point Theory and Applications, 2013, 81.
[7] D. Kim and N.Y. Ikikardes, *Certain combinatoric Bernoulli polynomials and convolution sums of divisor functions*, Advance Difference Equations, 2013, 2013:310, 11pp.
[8] D. Kim and Y.K. Park, *Bernoulli identities and combinatoric convolution sums with odd divisor functions*, Accepted to (http://www.hindawi.com/journals/aaa/aip/890973/).
[9] S. Ramanujan, *On certain arithmetical functions*, Trans. Cambridge Philos. Soc. **22**, 1916, 159-184.
[10] Y. Simsek, *Elliptic analogue of the Hardy sums related to elliptic Bernoulli functions*, Gen. Math. **15**, no.3, 3-23, 2007.
[11] H. M. Srivastava and A. Pinter, *Remarks on some relationships between the Bernoulli and Euler polynomials*, Appl. Math. Lett., **17**, (2004), 375-380.
[12] K. S. Williams, *Number Theory in the Spirit of Liouville*, London Mathematical Society, Student Texts 76, Cambridge, 2011.

Siegel invariants and its applications

Dong Sung Yoon
National Institute for Mathematical Sciences
dsyoon@nims.re.kr
Coauthors: Koo, Shin

The Siegel-Ramachandra invariants, as special values of Siegel functions of one variable, generate ray class fields over imaginary quadratic fields. Generalizing these invariants we shall introduce ray class invariants of certain CM-fields obtained from classical theta constants of multi-variables. And we will determine the action of the Galois group on these invariants in a concrete way by making use of Shimura's reciprocity law.

Bernoulli polynomial convolutions and p-adic Arakawa-Kaneko zeta functions

Paul Thomas Young
College of Charleston
paul@math.cofc.edu

The Arakawa-Kaneko zeta functions interpolate the poly-Bernoulli polynomials at the negative integers, while their values at positive integers are connected to multiple zeta values and harmonic number sums. We first present p-adic analogues of these zeta functions using a p-adic adaptation of Hasse's everywhere-convergent series for the Hurwitz zeta function. We then evaluate the ordinary convolution of Bernoulli polynomials in closed form in terms of poly-Bernoulli polynomials, and interpret these convolution identities in terms of p-adic Arakawa-Kaneko zeta functions, including a p-adic analogue of Ohno's sum formula. Series of generalized harmonic numbers which converge to zeta values in both complex and p-adic senses are a prominent feature of this approach.

Number of solutions in a box of a linear equation in an Abelian group

Maciej Zakarczemny

Cracow University of Technology, Cracow, Poland

mzakarczemny@pk.edu.pl

Karol Cwalina and Tomasz Schoen [1] have recently proved the following conjecture of Andrzej Schinzel [2]: the number of solutions of the congruence

$$a_1x_1 + \ldots + a_kx_k \equiv 0 \,(\mathrm{mod}\, n)$$

in the box $0 \leq x_i \leq b_i$, where b_i are positive integers, is at least

$$2^{1-n}\prod_{i=1}^{k}(b_i+1).$$

Using a completely different method we shall prove the following more general statement (Theorem 1), also conjectured by Schinzel [2, pp. 364].
The aim of the talk is to present results of [3] and [4], respectively:

Theorem. 1. *For every finite Abelian group* Γ *and for all* $a_1, \ldots, a_k \in \Gamma$, *the number of solutions of the equation* $\sum_{i=1}^{k} a_ix_i = 0$ *in nonnegative integers* $x_i \leq b_i$, *where* b_i *are positive integers, is at least*

$$2^{1-D(\Gamma)}\prod_{i=1}^{k}(b_i+1),$$

where $D(\Gamma)$ *is the Davenport constant of the group* Γ.
The coefficient $2^{1-D(\Gamma)}$ *is the best possible coefficient independent of* a_i, b_i *and dependent only on* Γ.

Theorem. 2. *For every finite Abelian group* Γ, *for all* $g, a_1, \ldots, a_k \in \Gamma$,
if there exists a solution of the equation $\sum_{i=1}^{k} a_ix_i = g$ *in nonnegative integers* $x_i \leq b_i$, *where* b_i *are positive integers, then the number of such solutions is at least*

$$3^{1-D(\Gamma)}\prod_{i=1}^{k}(b_i+1).$$

The coefficient $3^{1-D(\Gamma)}$ *is the best possible coefficient independent of* a_i, b_i *and dependent only on* Γ.

References

[1] K. Cwalina and T. Schoen, *The number of solutions of a homogeneous linear congruence*, Acta Arith. 153 (2012), pp. 271-279.

[2] A. Schinzel, *The number of solutions of a linear homogeneous congruence, in: Diophantine Approximation: Festschrift for Wolfgang Schmidt (H.-P. Schlickewei et al., eds.)*, Developments Math. 16, Springer, 2008, pp. 363-370.

[3] M. Zakarczemny, *Number of solutions in a box of a linear homogeneous equation in an Abelian group*, Acta Arith. 155 (2012), pp. 227-231.
[4] M. Zakarczemny, *Number of solutions in a box of a linear equation in an Abelian group*, (to appear).

Four dimensional Galois representations with large image

Adrián Zenteno
Universidad Nacional Autónoma de México.
matematicazg@ciencias.unam.mx

Given a normalised eigenform f of level N, weight $k \geq 2$ and Dirichlet character χ, there exist a number field E, such that for all maximal ideal λ of $\mathcal{O}_E$ (the ring of integers of E), we can attach to f a Galois representation

$$\rho_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{E}_\lambda).$$

A well known result of Ribet, says that if f does not have complex multiplication, then the projective image of the residual representation of $\rho_{f,\lambda}$ is $\mathrm{PGL}_2(\mathbb{F}_{\ell^s})$ or $\mathrm{PSL}_2(\mathbb{F}_{\ell^s})$ for almost all maximal ideal λ (i.e. all but finitely many). More generally, given a RAESDC (regular, algebraic, essentially self-dual, cuspidal) automorphic representation (π, μ) of $\mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}})$, there exist a number field E, such that for all maximal ideal λ of $\mathcal{O}_E$, we can attach to (π, μ) a Galois representation

$$\rho_{\pi,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_n(\overline{E}_\lambda).$$

In this talk, we will explain how to construct RAESDC automorphic representations (π, μ) of $\mathrm{GL}_4(\mathbb{A}_{\mathbb{Q}})$, such that the projective image of the residual representation of $\rho_{\pi,\lambda}$ is $\mathrm{PGSp}_4(\mathbb{F}_{\ell^s})$ or $\mathrm{PSp}_4(\mathbb{F}_{\ell^s})$ for (almost) all maximal ideal λ, by using the idea of (n, p)-groups of Khare-Larsen-Savin and the known cases of functoriality between SO_5 and GL_4.

The set of minimal distances in Krull monoids

Qinghai Zhong
University of Graz
qinghai.zhong@uni-graz.at
Coauthors: Alfred Geroldinger

Let H be a Krull monoid with finite class group G. Then every non-unit $a \in H$ can be written as a finite product of atoms, say $a = u_1 \cdot \ldots \cdot u_k$. The set $\mathsf{L}(a)$ of all possible factorization lengths k is called the set of lengths of a. If G is finite, then there is a constant $M \in \mathbb{N}$ such that all sets of lengths are almost arithmetical multiprogressions with bound M and with difference $d \in \Delta^*(H)$, where $\Delta^*(H)$ denotes the set of minimal distances of H. Using methods from Additive Combinatorics we show that $\max \Delta^*(H) \leq \max\{\exp(G) - 2, \mathsf{r}(G) - 1\}$ and that equality holds if every class of G contains a prime divisor, which holds true for holomorphy rings in global fields.

References

[1] A. Geroldinger and Qinghai Zhong, *The set of minimal distances in Krull monoids*, http://arxiv.org/abs/1404.2873.

Diophantine approximation with Pisot numbers

Victoria Zhuravleva
victorai.zhuravleva@me.com

On the number of integers that are the sum of exactly k units

Volker Ziegler
University of Salzburg
volker.ziegler@sbg.ac.at

Let us fix a number field L and let $\mathfrak{o}$ be the maximal order of L and $U = \mathfrak{o}^*$ its group of units. Furthermore, we fix a rational integer $k > 1$. Then we denote by $N_{L,k}(x)$ the number of rational integers $0 < n \leq x$ that can be written as the sum of at most k units $\in U$. In case that L is a real quadratic number field we give asymptotic formulas for $N_{L,k}(x)$. We will also discuss the case that $L/\mathbb{Q}$ is a Galois extension.

Rational points and linear forms near manifolds

Evgeniy Zorin
University of York
evgeniy.zorin@york.ac.uk

I will discuss some classical results on Diophantine approximations on manifolds, as well as recent developments of this topic. If time allows, I will present emerging applications.