Conference on Elementary and analytic number theory (ELAZ 2016)

Strobl, Austria
September 5–9, 2016

Sponsors

The conference organizers thank the following sponsors:

Graz University of Technology

Austrian Science Foundation (FWF)

Sonderforschungsbereich Quasi-Monte-Carlo-Methods

Land Oberösterreich

ELAZ2016 – Conference information

Date

September, 5-9, 2016

Venue

Bundesinstitut für Erwachsenenbildung (bifeb)
Strobl, Austria

Organizers

Christian Elsholtz, Georg Nowak, Robert Tichy

Invited speakers:
Tim Browning
Jörg Brüdern
Rainer Dietmann
Roger Heath-Brown
Igor Shparlinski
Trevor Wooley

List of participants

1. Nikola Adzaga, University of Zagreb
2. Christoph Aistleitner, Graz University of Technology
3. Antal Balog, MTA, Budapest
4. Attila Bérczes, University of Debrecen
5. Alexander Bors, Paris Lodron Universität Salzburg
6. Julia Brandes, Chalmers University of Technology
7. Tim Browning, University of Bristol
8. Jörg Brüdern, Georg-August-Universität Göttingen
9. Jan Büthe, Fraunhofer IIS, Erlangen
10. Yann Bugeaud, Université de Strasbourg
11. Kwok Chi (Gigi) Chim, Graz University of Technology
12. Alexandru Ciolan, Universität Bonn
13. Korneel Debaene, Georg-August-Universität Göttingen
14. Rainer Dietmann, Royal Holloway University of London
15. Sary Drappeau, Université Aix-Marseille
16. Michael Drmota, TU Wien
17. Christian Elsholtz, Graz University of Technology
18. Alan Filipin, University of Zagreb
19. Christopher Frei, LMU München/TU Graz

20. Clemens Fuchs, Paris Lodron Universität Salzburg
21. Peter Grabner, Graz University of Technology
22. Katalin Gyarmati, ELTE, Budapest
23. Hajdu Lajos, University of Debrecen
24. Karin Halupczok, WWU Münster
25. Roger Heath-Brown, University of Oxford
26. Norbert Hegyvári, MTA, Budapest
27. Titus Hilberdink, University of Reading
28. Christoph Hutle, Paris Lodron Universität Salzburg
29. Martin Huxley, University of Cardiff
30. Aleksandar Ivić, Serbian Academy of Sciences and Arts, Belgrade
31. Arne Juhas, WWU Münster
32. Norbert Kaiblinger, BOKU Wien
33. Christina Karolus, Paris Lodron Universität Salzburg
34. Matija Kazalicki, University of Zagreb
35. Daniel Krenn, Alpen-Adria-Universität Klagenfurt
36. Vinay Kumaraswamy, University of Bristol
37. Thomas Lachmann, Graz University of Technololgy
38. Kostadinka Lapkova, MTA, Budapest/TU Graz
39. Gerhard Larcher, Johannes Kepler Universität Linz
40. Daniel Loughran, University of Manchester

41. Manfred Madritsch, Université de Lorraine, Nancy
42. Helmut Maier, Universität Ulm
43. Antoine Marnat, Graz University of Technology
44. László Mérai, RICAM, Linz
45. Pieter Moree, Max-Planck-Institut für Mathematik, Bonn
46. Clemens Müllner, TU Wien
47. Marc Munsch, Graz University of Technology
48. Simon Myerson, University of Oxford
49. Georg Nowak, BOKU Wien
50. Radhakrishnan Nair, University of Liverpool
51. Alina Ostafe, UNSW, Sydney
52. Selin Selen Özbek, Universität Würburg
53. Péter Pal Pach, Budapest University of Technology and Economics
54. Friedrich Pillichshammer, Johannes Kepler Universität Linz
55. János Pintz, MTA, Budapest
56. Stefan Planitzer, Graz University of Technology
57. Maciej Radziejewski, Adam Mickiewicz University, Poznan
58. Oliver Roche-Newton, Johannes Kepler Universität Linz
59. Jürgen Sander, University of Hildesheim
60. Adrian Scheerer, Graz University of Technology

61. Klaus Scheicher, BOKU Wien
62. Jan-Christoph Schlage-Puchta, Universität Rostock
63. Johannes Schleischitz, BOKU Wien
64. Igor Shparlinski, UNSW, Sydney
65. Lukas Spiegelhofer, TU Wien
66. Raphael Steiner, University of Bristol
67. Jörn Steuding, Universität Würzburg
68. Rasa Steuding, Hochschule RheinMain, Wiesbaden
69. Pascal Stumpf, Universität Würzburg
70. Paul Surer, BOKU Wien
71. Ade Irma Suriajaya, Nagoya University
72. Marc Technau, Universität Würzburg
73. Niclas Technau, Graz University of Technology
74. Nicola Thorn, University of Reading
75. Robert Tichy, Graz University of Technology
76. Aled Walker, University of Oxford
77. Martin Widmer, Royal Holloway University of London
78. Florian Wilsch, Leibniz Universität Hannover
79. Arne Winterhof, Austrian Academy of Sciences, Linz
80. Trevor Wooley, University of Bristol
81. Volker Ziegler, Paris Lodron Universität Salzburg

Breakfast 8.00-9.00
Lunch 12.30
Dinner 18.00

As the programme is full, sessions will start on time, and speakers and chairs are asked to keep the times!

The Wednesday afternoon is free.
Prof. Tichy intends to give some details on possible excursions during Monday. Possibilities for excursions include,
(no legal responsibility for any of these is taken...):

- Salzburg, (e.g. by bus)
- Swimming in the Wolfgangsee, which in September is often warm enough.
- Walk along the lake. Also walk to St. Wolfgang.
- Easy hike to Bürglstein, behind the bifeb. wolfgangsee.salzkammergut.at/touren/oesterreich/tour/430002709/buerglstein-runde.html
- Hike to Schafberg, (start a few km away from bifeb, it's possible to go up and down by rack railway, but check the details including time table here:)
  http://www.schafbergbahn.at/content/website_schafbergbahn/de_at.html

  http://www.salzburg.com/wiki/index.php/Schafberg

  It's possible to hike, difference in altitude about 1000m. Decent shoes recommended. Check out the weather!

On the extension of $D(-8k^2)$-triple $\{1, 8k^2, 8k^2+1\}$

Nikola Adžaga

By elementary means, we show that the $D(-8k^2)$-triple $\{1, 8k^2, 8k^2+1\}$ can be extended to at most a quadruple (the fourth element can be only $32k^2+1$). A set of m positive integers $\{a_1, a_2, \ldots, a_m\}$ is called $D(n)$-m-tuple if $a_i a_j + n$ is a perfect square for all $1 \leqslant i < j \leqslant m$.

Extending the initial triple with d and then eliminating d leads to a system consisting of a Pell ($z^2 - (16k^2+2)y^2 = 1$) and a pellian equation ($x^2 - 2y^2 = -8k^2 + 1$). By solving Pell equation, we get two recurrent sequences y_n and z_n. Due to the second equation, the problem reduces to examining when can an element of the new sequence $X_n = 2y_n^2 - 8k^2 + 1$ be a complete square. Using the relations between y_n and z_n, e.g. $y_{2n+1} = 2y_n z_n$, we write X_n as a product of two factors, one of which is obviously not a square. We finish the proof by showing that these factors are relatively prime via principle of descent.

Faculty of Civil Engineering, University of Zagreb
Fra Andrije Kačića Miošića 26
10000 Zagreb
Croatia

Large values of the Riemann zeta function

Christoph Aistleitner

We present an improved version of Soundararajan's *resonance method*, which uses sparse Dirichlet polynomials to establish the existence of large values of the Riemann zeta function in the critical strip. We compare this approach to Montgomery's method, which is based on Diophantine approximation, and discuss a generalization to the case of Selberg L-functions.

TU Graz
Institute of Analysis and Number Theory
Steyrergasse 30
8010 Graz
Austria

Some diophantine properties of the sequence of S-units

Attila Bérczes

Let S be a finite set of rational primes, and let s_n denote the increasing sequence of the positive integers having all their prime factors in S. In the talk a method will be presented to explicitly give the gaps in the sequence s_n. In other words, for any term s_n we can find both s_{n-1} and s_{n+1}, at least in principle, without enumerating all terms of the sequence. In the case when S contains two fixed primes, an efficient algorithm will be presented to find these terms explicitly. Some further interesting properties of the sequence s_n will be presented along with an application of our results to prove some diophantine properties of the sequence s_n.

Coauthors: Andrej Dujella and Lajos Hajdu

University of Debrecen
Egyetem tér 1
H-4032 Debrecen
Hungary

A smoothness criterion for linear spaces on hypersurfaces

Julia Brandes

Let $X \subset \mathbb{P}^n$ be a smooth hypersurface and $F_m(X)$ the Fano scheme of m-dimensional linear spaces contained in X. I will present a criterion to decide whether or not $F_m(X)$ is smooth for a given hypersurface X. This has consequences for the study of linear spaces on hypersurfaces by the circle method.

Coauthor: Per Salberger

Matematiska Vetenskaper
Göteborgs Universitet / Chalmers TH
412 96 Göteborg
Sweden

Strong approximation on S^3 via a twisted Linnik conjecture

Tim Browning

Let S^3 denote the unit sphere $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1$. In a letter about the efficiency of a universal set of quantum gates, Sarnak has raised the question of how well points on S^3 can be approximated by rational points of small height. Specifically, given $r \in \mathbb{N}$, how large do we need to take $\varepsilon > 0$ in order to ensure that the intersection of S_3 with any ε-ball centred on a point of S^3, contains a point of the form $\mathbf{x}/r$, for $\mathbf{x} \in \mathbb{Z}^4$? Recent work of Sardari uses Heath-Brown's smooth δ-function variant of the circle method to show that it suffices to take $\varepsilon \gg r^{-1/3+\frac{1}{2016}}$. By exploiting extra averaging, we show that a twisted variant of the Linnik conjecture (concerning sums of Kloosterman sums) leads to a better exponent of approximation for S^3.

Coauthors: V. Vinay Kumaraswamy and R. Steiner.

References: N.T. Sardari, Optimal strong approximation for quadratic forms, *Preprint*, 2015.

University of Bristol
Bristol
BS8 1TW
United Kingdom

Expander estimates for cubes

Jörg Brüdern

Given a set A, we investigate the question what can be said about

$$N(X) = |\{z^3 + a \le B : a \in A\}|.$$

There is a classical dimishing ranges method due to Hardy and Littlewood that was significantly improved by Davenport in 1942. We describe an approach based on differencing cubic exponential sums, rather than differencing a certain symmetric diophantine equation. Some applications will also be discussed.

Analytic computation of the prime counting function

Jan Büthe

The most frequently used method for calculating $\pi(x)$, the number of prime numbers not exceeding x, at larger values is the combinatorial Meissel-Lehmer method, which requires $O(x^{2/3+\varepsilon})$ arithmetic operations in order to evaluate $\pi(x)$.

In the late 1980s Lagarias and Odlyzko proposed an analytic method which was capable of calculating $\pi(x)$ using only $O(x^{1/2+\varepsilon})$ arithmetic operations. Although the new method would eventually outperform the combinatorial method, the latter remained the method of choice for another two decades, since the implied constant was expected to be large.

Recently, new variants of the analytic method have been developed and implemented and for the first time record computation of $\pi(x)$ have been carried out this way. In this talk, a brief overview of these recent improvements and applications will be given.

Fraunhofer Institute for Integrated Circuits
Am Wolfsmantel 33
91058 Erlangen
Germany

On the b-ary expansions of $\log(1+\frac{1}{a})$ and e

Yann Bugeaud

Let $b \geq 2$ be an integer and ξ an irrational real number. We prove that, if the irrationality exponent of ξ is equal to 2 or slightly greater than 2, then the b-ary expansion of ξ cannot be 'too simple', in a suitable sense. Our result applies, among other classical numbers, to badly approximable numbers, non-zero rational powers of e, and $\log(1+\frac{1}{a})$, provided that the integer a is sufficiently large. It establishes an unexpected connection between the irrationality exponent of a real number and its b-ary expansion.

Coauthor: Dong Han Kim (Seoul).

Y. Bugeaud and D. H. Kim, On the b-ary expansions of $\log(1+\frac{1}{a})$ and e, Ann. Scuola Normale Sup. di Pisa. To appear.

Université de Strasbourg
7 rue René Descartes
67084 Strasbourg
France

Gaps and jumps in cyclotomic coefficients

Alexandru Ciolan

We improve several recent results by Hong, Lee, Lee and Park (2012) on gaps and Bzdęga (2014) on jumps amongst the coefficients of cyclotomic polynomials. Besides direct improvements, we also introduce several new techniques that have never been used in this area.

Joint work with O.-M. Camburu, F. Luca, P. Moree and I. Shparlinski.

University Bonn
Germany

A Brun-Titchmarsh inequality for Chebotarev's density theorem

Korneel Debaene

The well-known Brun-Titchmarsh inequality gives an upper bound for the number of primes in an arithmetic progression. In the context of Chebotarev's Density Theorem, one can ask for a similar result, giving a bound for the number of primes with some given splitting behaviour in a given number field K. We develop a method to use the Selberg Sieve to obtain such a result. As in the Brun-Titchmarsh inequality, the bound is off by a factor 2 asymptotically, but its merit is its effectiveness.

The main new ingredient is a lemma that allows one to count integral elements in K of bounded norm, up to multiplication by unit elements.

Mathematisches Institut,
Georg-August-Universität Göttingen
Bunsenstrasse 3-5
37073 Göttingen
Germany

On the ℓ-invariant of forms

Rainer Dietmann

In this talk we want to introduce the ℓ-invariant, a generalization of the well known h-invariant of cubic forms to systems of homogeneous forms of the same degree. We discuss some of its properties under field extensions and in the case of systems of cubic forms how it relates to the h-invariant of certain individual forms in the pencil. This allows us to say something new about positive density of local solutions for some Diophantine problems. In particular, we can show that any system of r rational cubic forms in more than $800000r^4$ variables has a non-trivial rational zero, improving on a previous result from 1982 by Wolfgang Schmidt, who obtained the bound $(10r)^5$ instead. The proofs amongst other tools involve reduction theory and an application of Schmidt's subspace theorem.

Department of Mathematics, Royal Holloway, University of London, TW20 0EX Egham, United Kingdom

Divisors of friable numbers

Sary Drappeau

The distribution of divisors of an integer n is studied through the distribution of the random variable

$$D_n := (\log d)/\log n$$

where d is chosen uniformly at random from divisors of n. Among many interesting aspects of the sequence (D_n), one may ask about its possible convergence in law, along various sequences of integers. For instance, a classical result of Deshouillers, Dress and Tenenbaum shows the convergence of the Cesaro mean of the distribution functions of D_n.

Coauthors: G. Tenenbaum (Nancy)

Aix-Marseille Université
163 avenue de Luminy
13009 Marseille
France

On the strong version of Diophantine quintuple conjecture

Alan Filipin

A set of m positive integers is called a Diophantine m-tuple if the product of any two of its distinct elements increased by 1 is a prefect square. One of the interesting questions is how large those sets can be. There is a folklore conjecture that there does not exist a Diophantine quintuple. Furthermore, there is a stronger version of that conjecture, that every Diophantine triple can be extended to a quadruple with a larger element in the unique way. In 2004, Dujella proved that there does not exist a Diophantine sextuple and that there only finitely many quintuples. His results were improved in recent years, but the conjecture still remains open.

Let $\{a, b, c, d\}$ such that $a < b < c < d$ be a Diophantine quadruple. In this talk we give an upper bound for minimal c such that d is not unique. It helps us to prove the strong version of the conjecture for various families of Diophantine triples and as corollary it implies the non-extendibitily of some parametric families of Diophantine pairs to a quintuple.

Coauthors: Yasutsugu Fujita, Alain Togbé.

University of Zagreb, Faculty of Civil Engineering
Kačićeva 26
10000 Zagreb
Croatia

Lower bounds for rational points on smooth del Pezzo surfaces

Christopher Frei

We discuss conjecturally sharp asymptotic lower bounds for the number of rational points on del Pezzo surfaces, in particular on smooth cubic surfaces. These bounds are valid for all del Pezzo surfaces over all number fields, after a finite extension of the base field. The proofs are based on a fibration into conics and the analysis of certain divisor sums over the values of binary quadratic forms.

Coauthors: Daniel Loughran, Efthymios Sofos

Technische Universität Graz
Institut für Analysis und Zahlentheorie
Kopernikusgasse 24/II
A-8010 Graz
Austria

On reducible and primitive sets of numbers

Katalin Gyarmati

A set $\mathcal{A}$ is said to be reducible if it can be represented in the form $\mathcal{A} = \mathcal{B} + \mathcal{C}$ with $|\mathcal{B}|, |\mathcal{C}| \geq 2$. If there are no sets $\mathcal{B}, \mathcal{C}$ with these properties then $\mathcal{A}$ is said to be primitive. Here three criteria are presented for primitivity of subsets of $\mathbb{F}_p$. Then the distance between a given set $\mathcal{A} \subset \mathbb{F}_p$ and the closest primitive set is studied. Further related questions and problems are also studied.

Coauthors: Sergei Konyagin, András Sárközy.

K. Gyarmati, S. Konyagin, A. Sárközy, On the reducibility of large sets of residues modulo p, J. of Number Theory 133 (2013), 2374-2397.

K. Gyarmati, A. Sárközy, On reducible and primitive subsets of F_p, I, Integers 15A (2015), A6.

K. Gyarmati, A. Sárközy, On reducible and primitive subsets of F_p, II, Q. J. Math. (2015) (online).

Eötvös Loránd University
Pázmány Péter st. 1/C
1117 Budapest
Hungary

Consecutive primes forming a complete or a reduced residue system

Lajos Hajdu

In the talk we discuss some problems and (partial) solutions concerning consecutive primes and residue classes.

First we present a proof of a conjecture of Recaman from 1978, stating that the only prime p for which the first p primes form a complete residue system modulo p is $p = 2$.

Then we discuss a more general conjecture of Pomerance from 1980, which is an alike statement concerning the first $\varphi(m)$ primes coprime to m, forming a reduced residue system modulo m. In this case the complete solution is due to Togbé and Yang (2014).

Finally, we consider a problem of Balasubramanian from 2015, where the above primes forming a (reduced) residue system, can be arbitrary consecutive ones. We briefly mention recent, more general problems and results of Elsholtz, Technau and Tichy, as well.

Coauthors: N. Saradha and R. Tijdeman

University of Debrecen
Egyetem tér 1
H-4032 Debrecen
Hungary

Polynomial large sieve inequalities and a Bombieri–Vinogradov theorem with products of Gaussian primes

Karin Halupczok

Quite a general multivariate polynomial large sieve inequality was proved in [1]. It has advantages in certain applications compared to standard large sieve approaches. As a further application, we present a multivariate variant of Bombieri–Vinogradov's Theorem with appropriate products of Gaussian primes as moduli, see [2]. This variant incorporates the benefit coming from the polynomial large sieve inequality, and apart from that, only standard methods are used in the proof.

References: [1] K. Halupczok, Large sieve inequalities with general polynomial moduli, Q. J. Math. 66 (2015) no. 2, 529–545; doi: 10.1093/qmath/hav011. [2] K. Halupczok, A Bombieri–Vinogradov Theorem with products of Gaussian primes as moduli, accepted by Functiones et Approximatio. Preprint: arXiv:1607.07265 [math.NT]

Westfälische Wilhelms-Universität Münster
Mathematisches Institut
Einsteinstraße 62
D-48149 Münster
Germany

Gaps Between Smooth Numbers

Roger Heath-Brown

If $g_1, g_2, \dots$ are the successive x^ε-smooth numbers, one may conjecture that

$$\sum_{g_n \le x} (g_{n+1} - g_n)^2 \ll_\varepsilon x^{1+\varepsilon}.$$

The investigation of this leads to a novel question about mean-values of Dirichlet polynomials. The result we shall prove has applications to questions about gaps in other sequences.

Mathematical Institute
Radcliffe Observatory Quarter
Woodstock Road
Oxford OX2 6GG
U.K.

On some properties of Hilbert cubes in prime fields

Norbert Hegyvári

We investigate some arithmetic behavior (sumset; energy) of multiplicative and additive Hilbert cubes in prime fields showing connections with additive and multiplicative character sums.

As a short introduction we discuss some former results of Hilbert, Szemerédi, Elsholtz, Dietmann, Shparlinski, and the author.

Eötvös University, Institute of Mathematics
Pázmány st. 1/c,
H-1117 Budapest
Hungary

The Singular Values of Multiplicative Toeplitz matrices

Titus Hilberdink

Abstract: We investigate the asymptotic behaviour of the singular values of matrices with entries $a_{ij} = f(i/j)$ if $j|i$ and zero otherwise, where f is an arithmetical function. In particular, we consider the case where f is multiplicative and $\sum_{n\leq x} |f(n)|^2$ is regularly varying. We show that under some mild conditions, the (normalised) singular values behave like the eigenvalues values of a certain Hilbert-Schmidt operator. Further, we discuss the nature of these eigenvalues.

University of Reading
Reading
UK

Diophantine triples with values in k-generalized Fibonacci sequences

Christoph Hutle

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.

It was shown by Fuchs, Hutle, Irmak, Luca and Szalay in 2015, that for 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 $n \geq 0$, there exist only finitely many Diophantine triples with values in $\{T_n\}_{n\geq 0}$.

In this talk, we will consider the k-generalized Fibonacci sequence given for some $k \geq 2$ by $F_0^{(k)} = \ldots = F_{k-2}^{(k)} = 0, F_{k-1}^{(k)} = 1$ and

$$F_{n+k}^{(k)} = F_{n+k-1}^{(k)} + \cdots + F_n^{(k)}$$

for all $n \geq 0$. Improving the previous result, we show that there are only finitely many Diophantine triples with values in $\{F_n^{(k)}\}_{n\geq 0}$.

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.

Coauthors: C. Fuchs, F. Luca, L. Szalay

References:

C. Fuchs, C. Hutle, F. Luca, L. Szalay, Diophantine triples with values in k-generalized Fibonacci sequences, bulletin of the malaysian mathematical sciences society, to appear.

C. Fuchs, C. Hutle, N. Irmak, F. Luca, L. Szalay, Only finitely many Tribonacci Diophantine triples exist, Math. Slovaca, to appear.

University of Salzburg
Hellbrunner Straße 34
5020 Salzburg, Austria

The Lattice Points in a Convex Plane Set

M. N. Huxley

A closed convex shape in two dimensions is shown on a computer screen by overlaying a square lattice (the integer lattice), and lighting the picksels corresponding to the lattice points which fall inside the shape. The human eye sees the screen image as a convex polygon.

The set of picksels lit is very sensitive to translation and to change of scale. Classically the shape is a circle radius R. Most of the results known for the circle extend to any oval whose boundary curve is three times differentiable. The number of lattice points is asymptotic to AR^2, and is usually $AR^2 + O\left(R^{1/2}(\log R)^\delta\right)$, for any $\delta > 0$. The number of sides of the polygon of lattice points is usually about $BR^{2/3}$.

The lattice sees the boundary curve as an envelope of tangents, not as a set of points. The points of contact of the tangents with rational gradients are uniformly distributed modulo the integer lattice.

References:

M. N. Huxley, Area, Lattice Points and Exponential Sums, London Math. Soc. Monographs, Oxford U. P.,1996.

M. N. Huxley, The convex hull of the lattice points inside a curve, Periodica Math. Hung., 68, 2014, 100-118.

University of Cardiff
Mathematics Institute
23 Senghenydd Road
Cardiff CF24 4AG
United Kingdom of Great Britain and Northern Ireland
European Common Market (for at least another 6 months)

The distribution of values of Hardy's function $Z(t)$

Aleksandar Ivić

Hardy's classical function $Z(t)$ (see [1]) is

$$Z(t) := \zeta(\tfrac{1}{2}+it)\big(\chi(\tfrac{1}{2}+it)\big)^{-1/2},\ \zeta(s) = \chi(s)\zeta(1-s) \quad (t \in \mathbb{R}).$$

In this talk some results and problems involving Hardy's function are presented. In particular, is it true that there exist constants $A_+ > 0, A_- > 0$ such that ($\mu(\cdot)$ denotes measure)

$$\mathcal{J}_+(T) := \mu\Big\{T < t \le 2T\ :\ Z(t) > 0\Big\} = \big(A_+ + o(1)\big)T \quad (T \to \infty),$$

$$\mathcal{J}_-(T) := \mu\Big\{T < t \le 2T\ :\ Z(t) < 0\Big\} = \big(A_- + o(1)\big)T \quad (T \to \infty)?$$

Obviously $A_+ + A_- = 1$ (if A_+, A_- exist). Perhaps $A_+ = A_- = 1/2$? This statement is supported by numerical evidence. In a forthcoming joint work with S.M. Gonek (arXiv:1604.00517) it is unconditionally proved that, for some $C > 0$ and $T \ge T_0$, we have $\mathcal{J}_+(T) \ge CT$, $\mathcal{J}_-(T) \ge CT$. If the Riemann Hypothesis and H.L. Montgomery's pair correlation conjecture is assumed then, for $T \ge T_0$,

$$\mathcal{J}_+(T) \ge 0.32909\,T, \qquad \mathcal{J}_-(T) \ge 0.32909\,T.$$

References:

[1] A. Ivić, The theory of Hardy's Z-function, Cambridge University Press, Cambridge, 2012, 245pp. ISBN 978-1-107-02883-8.

Serbian Academy of Sciences and Arts
Knez Mihailova 35
11000 Beograd
Serbia

Inequalities of the second moment for prime numbers and the pair correlation function

Arne Juhas

We consider lower bounds of second moments for primes in short intervals. for which the expected asymptotic formula is predicted by Montgomery's Pair Correlation Conjecture. D. Goldston proved supporting lower bounds assuming the Generalized Riemann Hypothesis.
Using a modified approach based upon his method, we examine which additional assumptions beyond GRH lead to improved lower bounds. The proof uses a method of Hooley relying on the Fourier–expansion of the sawtooth curve and the large sieve inequality.
The method is also applicable to derive lower bounds of the pair correlation function.

University of Muenster
Einsteinstr. 62
48149 Muenster
Germany

Composite polynomials in second order linear recurrence sequences

Christina Karolus

Let $(G_n)_{n=0}^{\infty} \in \mathbb{C}[x]$ be a minimal non-degenerate simple binary linear recurrence sequence of polynomials, defined by $A_0, A_1, G_0, G_1 \in \mathbb{C}[x]$ and the relation

$$G_{n+2}(x) = A_1(x)G_{n+1}(x) + A_0(x)G_n(x), \ n \in \mathbb{N}.$$

We show that, under certain assumptions on the sequence, if $G_n(x) = g \circ h(x)$ holds for some $n \in \mathbb{N}$ and h is indecomposable, then either h is of special shape or $\deg g$ is bounded by a constant independent on n. Moreover, we give sufficient conditions on A_0, A_1, G_0, G_1 such that the assumptions in question are satisfied. In the talk an outline of the proof shall be presented.

Coauthors: Clemens Fuchs, Dijana Kreso

University of Salzburg
Hellbrunnerstraße 34
5020 Salzburg
Austria

Rational Diophantine sextuples

Matija Kazalicki

A rational Diophantine m-tuple is a set of m nonzero rationals such that the product of any two distinct elements from the set increased by 1 is a perfect square. The first rational Diophantine quadruple was found by Diophantus, while Euler proved that there are infinitely many rational Diophantine quintuples. In 1999, Gibbs found the first example of a rational Diophantine sextuple. In this talk, we present two constructions of infinite families of rational Diophantine sextuples.

Coauthors: A. Dujella, M. Mikić, M. Szikszai

References: A. Dujella, M. Kazalicki, M.Mikić, M. Szikszai, There are infinitely many rational Diophantine sextuples, IMRN, 2016, doi: 10.1093/imrn/rnv376.
A.Dujella, M. Kazalicki, More on Diophantine sextuples, preprint.

University of Zagreb
Bijenicka cesta 30
10000 Zagreb
Croatia

(Non-)Minimal Redundant Digit Expansions with an Imaginary Quadratic Integer Base

Daniel Krenn

This talk will be about redundant digit expansions with an imaginary quadratic algebraic integer with trace ± 1 as base and a minimal norm representatives digit set. We will consider the width-w non-adjacent form and its (non-)minimizing property of the Hamming-weight among all possible expansions with the same digit set. One main part in the proof of the presented results is to show that a certain inequality does not have any integer solutions. Furthermore, approximation properties of continued fractions are used (by a variant of the Baker–Davenport reduction method).

Coauthors: Volker Ziegler

Alpen-Adria-Universität Klagenfurt
Universitätsstraße 65–67
9020 Klagenfurt am Wörthersee
Austria

On sums of class numbers of imaginary quadratic fields

V Vinay Kumaraswamy

Let $h(-d)$ denote the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$. Moments of class numbers - sums of the form $\sum_{d \leq X} h^k(-d)$ - have been studied in the past, and are well understood. In this talk, I will speak about obtaining an asymptotic formula for the shifted sum $\sum_{d \leq X} h(-d)h(-d-l)$, where l is an integer; the proof makes use of the smooth δ-symbol.

University of Bristol
Howard House
Bristol BS8 1SN
United Kingdom

On estimating divisor sums

Kostadinka Lapkova

Consider the divisor sum $\sum_{n\leq N}\tau(f(n))$, where $f(n)=n^2+2bn+c$ for certain integers b and c. We will discuss asymptotic formulae for this average sum for both irreducible and reducible polynomials $f(n)$ and show explicit upper bounds in both cases, which are close to the optimal. We would then illustrate the application of such explicit bounds in the problem for estimating the maximal possible number of $D(m)$-sets for certain integers m.

Alfréd Rényi Institute of Mathematics
Hungarian Academy of Sciences
Reáltanoda utca 13-15
1053 Budapest
HUNGARY

ADDITIVE ENERGY AND METRIC PAIR CORRELATION OF SEQUENCES

GERHARD LARCHER
(JOINT WORK WITH CHRISTOPH AISTLEITNER, JEAN BOURGAIN AND MARK LEWKO)

ABSTRACT. The concept of *pair correlation* of sequences of real numbers in $[0,1)$ was introduced by Rudnick and Sarnak, and was studied in several papers for example by Rudnick, Sarnak, Zaharescu, Heath-Brown and others. We say that the pair correlation of a sequence $(x_n)_{n\geq 1}$ is *Poissonian* if for every real $s > 0$ we have

$$\frac{1}{N}\#\left\{1 \leq j \neq k \leq N : \|x_j - x_k\| \leq \frac{s}{N}\right\} \underset{N\to\infty}{\longrightarrow} 2s.$$

Randomly chosen sequences in $[0,1)$ satisfy this property. In this talk we consider sequences of the form $(\{a_n\alpha\})_{n\geq 1}$ where α is a given real and $(a_n)_{n\geq 1}$ is a given strictly increasing sequence of integers. We are interested in the question under which conditions these sequences are Poissonian for almost all α. We show that this question on metric pair correlation is strongly connected with the concept of *additive energy* of the sequence $(a_n)_{n\geq 1}$ in the sense of additive combinatorics. Thereby we essentially extend and generalize earlier results of Rudnick, Sarnak and Zaharescu on metric pair correlation.

Number of rational points on cubic surfaces over finite fields

Daniel Loughran

Given a smooth cubic surface S over a finite field $\mathbb{F}_q$, Serre has posed the problem of determining the possibilities for the number of rational points $\#S(\mathbb{F}_q)$. In this talk we shall give a complete answer to this problem, building on special cases treated by Swinnerton-Dyer.

Coauthors: Barinder Banwait and Francesc Fité.

School of Mathematics
The University of Manchester
Manchester
M13 9PL
UK

DIOPHANTINE INEQUALITIES

MANFRED G. MADRITSCH

This is joint work with Robert Tichy.

Dirichlet's approximation theorem states that for any real ξ and any $N > 0$ there exists $1 \leq n \leq N$ such that $\|\xi n\| \leq N^{-1}$, where $\|\cdot\|$ denotes the distance to the nearest integer. This was generalized, among others, by Heilbronn (1948), who proved that for any real ξ and any integer $N > 0$ there exists $1 \leq n \leq N$ such that $\|\xi n^2\| \leq N^{-\frac{1}{2}+\varepsilon}$.

We start the talk by presenting the connection of these questions with uniform distribution and intersective sets. Then we mention recent result involving pseudo polynomials, *i.e.* functions $f(x) = \alpha_1 x^{\theta_1} + \cdots + \alpha_d x^{\theta_d}$ such that $1 < \theta_1 < \cdots < \theta_d$ and at least one $\theta_j \notin \mathbb{Z}$. In particular, we show that for any real ξ and any integer N there exist $\sigma, \eta > 0$ depending only on f such that there exists an integer n with $1 \leq n \leq N$ and a prime p with $1 \leq p \leq N$ such that

$$\|\xi \lfloor f(n) \rfloor\| \leq N^{-\sigma} \quad \text{and} \quad \|\xi \lfloor f(p) \rfloor\| \leq N^{-\eta}.$$

(M. G. Madritsch) Institute Elie Cartan Nancy
Faculté de Sciences et Technologies
Université de Lorraine
54506 Vandoeuvre-lès-Nancy Cedex, France

Moments of Cotangent Sums related to the Estermann Zeta-function

Helmut Maier

Cotangent Sums are associated to the zeros of the Estermann zeta function. They have also proven to be of importance in the Nyman-Beurling criterion for the Riemann Hypothesis. We shall give a short overview on these relations as well as on recent results of Michael Rassias and the speaker on moments of these cotangent sums.

University of Ulm
Germany

On the spectrum of exponents of Diophantine approximation

Antoine Marnat

Using the Parametric Geometry of Numbers introduced recently by W.M. Schmidt and L. Summerer and results by D. Roy, we establish that the spectrum of the $2n$ exponents of Diophantine approximation in dimension $n \geq 3$ is a subset of $\mathbb{R}^{2n}$ with non empty interior.

References:
D. Roy, On Schmidt and Summerer parametric geometry of numbers ,Ann. of Math. (2), 182:739-786, 2015
A. Marnat, About Jarník's-type relation in higher dimension, submitted.

Technische Universität Graz
Steyrergasse 30
8010 GRAZ
Austria

Predicting the elliptic curve congruential generator

László Mérai

Let p be a prime and let $\mathbf{E}$ be an elliptic curve defined over the finite field $\mathbb{F}_p$. For a point $G \in \mathbf{E}$ the *elliptic curve congruential generator* produces a sequence (x_n) by the relation

$$x_n = x(W_n) = x(W_{n-1} \oplus G) = x(nG \oplus W_0), \quad n = 1, 2, \ldots,$$

where $\oplus$ denotes the group operation in $\mathbf{E}$ and $W_0 \in \mathbf{E}$ is an initial point.

Although the sequence (x_n) has many nice pseudorandom properties, e.g. it has large linear complexity and small discrepancy, it also has cryptographically weak properties. Namely, we show that if some consecutive elements of the sequence (x_n) are given as integers, one can compute in polynomial time an elliptic curve congruential generator (where the curve possibly defined over the rationals or over a residue ring) such that the generated sequence is identical to (x_n) in the revealed segment. It turns out that in practice, all the secret parameters, and thus the whole sequence (x_n), can be computed from eight consecutive elements, even if the prime and the elliptic curve are private.

Johann Radon Institute for Computational and Applied Mathematics,
Austrian Academy of Sciences
Altenberger Str. 69
4040 Linz
Austria

Automatic sequences satisfy the Sarnak conjecture

Clemens Müllner

We use analytic tools to prove that the dynamical system corresponding to any automatic sequence fulfils the Sarnak conjecture. In particular, any complex valued automatic sequence is orthogonal to the M obius function. In this talk we outline a method to reduce the treatment of automatic sequences to a structure combining synchronizing and invertible aspects. We use (and adopt) a method developed by Mauduit and Rivat, as well as com- bine ideas for invertible automata by Drmota and Morgenbesser and synchronizing automata by Deshouillers, Drmota and myself. Furthermore, we prove a prime number theorem for many automatic sequences.

TU Wien
Wiedner Hauptstr. 8
1040 Wien
Österreich

MOMENTS OF THETA FUNCTIONS AND SHIFTED MOMENTS OF L- FUNCTIONS

MARC MUNSCH

We will talk about some problems and results concerning moments of theta functions (conjecture, upper and lower bounds). We will explain briefly some techniques involved in the proofs and particularly give a result on shifted moments of Dirichlet L- functions using Soundararajan's method used to bound moments of Riemann zeta function.

References

[1] M. Munsch, 'Shifted moments of L-functions and moments of theta functions', to appear in *Mathematika*.

[2] K. Soundararajan, 'Moments of the Riemann zeta function', *Ann. of Math. (2)*, **170** (2009), 981–993.

5010 Institut fr Analysis und Zahlentheorie 8010 Graz, Steyrergasse 30, Graz
E-mail address: munsch@math.tugraz.at

Real and rational systems of forms

Simon Myerson

Consider a system f of R forms of degree d in f variables. A classic result of Birch estimates the density of integral zeroes of f when $n \gg_{d,R} 1$ is large and the variety $f = 0$ is smooth. We give an improvement when $R \gg_d 1$ is large, and an extension to systems of Diophantine inequalities $|f| < 1$ with real coefficients. Our strategy reduces the problem to an upper bound for the number of solutions to a multilinear auxiliary inequality.

Mathematical Institute
Radcliffe Observatory Quarter
Woodstock Road
Oxford OX2 6GG
U.K.

On sub-sums of partial quotients of real numbers

Radhakrishnan Nair

For $x \in (0,1)$, let $x = [c_1(x), c_2(x), \cdots]$ denote its regular continued fraction expansion. Also let

$$S_n(x) = \sum_{j \le n} c_j(x). \qquad (n = 1, 2, \ldots)$$

A. Ya. Khinchin showed that

$$\lim_{n\to\infty} \frac{S_n(x)}{n} = +\infty,$$

almost everywhere with respect to Lebesgue measure. Later H. G. Diamond and J. D. Vaaler showed that, there exist $\theta \in (0,1)$ and $n_0(x) \in \mathbb{N}$ such that

$$S_n(x) = \frac{1+o(1)}{n} n \log n + \theta \max_{1\le j\le n} c_j(x),$$

if $n > n_0(x)$ almost everywhere with respect to Lebesgue measure. The presence of the term $\max_{1\le j\le n} c_j(x)$, here tells you an almost everywhere estimate for $S_n(x)$ dependent only on n is likely to be problematic. Another option is to preclude the possibility that c_j is too big. In this context Khinchin showed that if we let

$$b_j(x) = \begin{cases} c_j(x), & \text{if } c_j(x) < j(\log j)^{4/3} \\ 0, & \text{otherwise,} \end{cases}$$

then

$$\lim_{n\to\infty} \frac{b_1(x) + \ldots + b_n(x)}{n} \to \frac{1}{\log 2}$$

in measure. The same result is not true almost everywhere as Khinchin also observed. Further refinements were given by W. Philipp.

This talk discusses analogous results for sums of the form

$$T_n(x) = \sum_{1\le j\le n} c_{k_j}(x), \qquad (n = 1, 2, \ldots)$$

for arithmetically interesting sequences of integers $(k_j)_{j\geq 1}$ like the squares or primes.

Coauthor: Liangang Ma, The University of Binzhou

1) R. Nair, On the metrical theory of continued fractions, Proc. Amer. Math. Soc. vol. **120**, (1994), no. 4, 1994, 1041-1046.

2) L. Ma and R. Nair, Limit theorems for sub-sums fo partial quotients of continued fractions, Preprint 17 pages.

The University of Liverpool
1 Peach Street
Liverpool L69 7ZL
Great Britain

Polynomial orbits in structural sets

Alina Ostafe

The underlying motive of the talk is showing various instances of the following principle: Polynomials have no respect for Law and Order.

More precisely, given a polynomial f over a field K and a structural set $M \subseteq K$ defined in terms unrelated to f, it is natural to expect that the orbits of f have a finite intersection with M. In this talk we present results for univariate rational functions defined over fields of characteristic zero and for special sets M such as S-integers, roots of unity or finitely generated groups. If M is an orbit of another polynomial this is known as a problem about orbit intersections, which has recently been studied by Ghioca, Tucker and Zieve.

We are interested in finiteness results or, failing this, in bounding the frequency of such intersections.

The University of New South Wales, Sydney 2052, Australia

Progression-free sets

Péter Pál Pach

We show that if the subset $A \subseteq \mathbb{Z}_4^n$ is free of three-term arithmetic progressions, then $|A| \leq 4^{\gamma n}$ with an absolute constant $\gamma \approx 0.926$. That is, progression-free sets in $\mathbb{Z}_4^n$ are exponentially small.

Coauthors: Ernie Croot, Vsevolod F. Lev

Budapest University of Technology and Economics
Magyar Tudósok krt. 2.
1117 Budapest
Hungary

On some problems on consecutive differences of primes

János Pintz

Many 50-60-70 year old problems on consecutive differences of primes seemed to be unattackable until three years ago. Soon after the sensational results of Zhang, Maynard and Tao proving the existence of infinitely many bounded intervals containing at least two primes (Zhang), respectively at least k primes for any k (Maynard and Tao), this situation changed also. It turned out that the method of Zhang, and especially that of Maynard and Tao coupled with other ideas enabled the answer of many such problems (for example, to improve also the best known bound of Rankin about large gaps between consecutive primes, originating from 1938). In the lecture we give a survey of the recent developments concerning a number of such problems.

Rényi Mathematical Institute of the Hungarian Academy of Sciences
Reáltanoda u. 13–15
Budapest
H-1053 Hungary

Sequences with Property P

Stefan Planitzer

A monotonically increasing sequence $A = \{a_1 < a_2 < \ldots\}$ of positive integers having the property that a_i does not divide the sum $a_j + a_k$ for $i < j < k$ is said to have 'Property P'. This concept was first introduced by Erdős and Sárközy in [1]. They come up with an infinite set with Property P with a lower bound on the counting function of order $\frac{\sqrt{x}}{\log x}$. We will show how to construct a sequence with Property P which improves on this lower bound by roughly a factor of $\sqrt{\log x}$.
Coauthor: Christian Elsholtz

References: [1] P. Erdős, A. Sárközi, On the divisibility properties of sequences of integers, Proc. London Math. Soc. (21), 1970, 97–101.

Graz University of Technology
Institute of Analysis and Number Theory
Steyrergasse 30/II
8010 Graz
Austria

Quantitative results in old and new semigroups

Maciej Radziejewski

We give an account of results on the counting functions (size of the main term and oscillations) of semigroup subsets defined by factorization-related properties. We consider three classes of arithmetical semigroups, i.e., in the order of increasing generality: generalized Hilbert semigroups (F. Halter-Koch, Exposition. Math. 8, 1990), L-semigroups (Acta Arith. 163.2, 2014), and analytic monoids (J. Kaczorowski, Semigroup Forum, 2016). A part of this research is joint work with J. Kaczorowski.

Adam Mickiewicz University
ul. Umultowska 87
PL-61-614 Poznań
Poland

Inverse problems for sum-product and distance problems

Oliver Roche-Newton

A celebrated result of Guth and Katz states that any set $P \subset \mathbb{R}^2$ of N points determines $\Omega(N/\log N)$ distinct distances, and this result is tight up to logarithmic factors. What remains wide open is the inverse problem: what can we say about sets which determine few distinct distances? Erdős conjectured that extremal sets are "lattice like".

This talk discusses some more precise formulations of this conjecture and introduces some results. For the special case when $P = A \times A$, a result of Hanson shows that extremal sets have some additive structure. For this case, the results and techniques resemble those from additive combinatorics, and there is a close relation with recently introduced extremal sum-product problems.

Johannes Kepler Universität
69 Altenburger Straße
Linz
Austria

On a construction of an absolutely normal number by Sierpinski

Adrian Scheerer

A real number is called absolutely normal if for every integer $b \geq 2$ its orbit under the multiplication-by-b map is uniformly distributed modulo one. In 1917, Sierpinski gave the first example of such a number. His construction has recently been made computable by Becher and Figueira. In this talk I explain how to modify this algorithm to give an example of a computable absolutely normal number that is moreover continued fraction normal, meaning that its orbit under the Gauss map is uniformly distributed modulo one with respect to the Gauss measure. The proof is not too difficult and uses explicit estimates for the measure of sets of certain non-normal numbers obtained by an application of a large deviation inequality for mixing random variables. This gives an answer to a question by Bugeaud.

TU Graz
Kopernikusgasse 24
8010 Graz
Austria

Uniform distribution problems involving coprimality conditions

Jan-Christoph Schlage-Puchta

Let $(a_1, \dots, a_k)$ is an integer vector, and consider the set

$$\mathcal{S} = \left\{ \frac{1}{n} \cdot (ta_1 \bmod n, \dots, ta_k \bmod n) \middle| 1 \le t \le n, (t,n) = 1 \right\} \subseteq [0,1]^k.$$

A standard application of the Erdős-Turán-Koksma-inequality implies that for a given $\epsilon > 0$ the set $\mathcal{S}$ meets every ball of radius ϵ, unless either n is too small, or the integers $a_1, \dots, a_k$ satisfy a linear relation with small coefficients. Unfortunately, for applications where one is looking for a classification of all situations, where $\mathcal{S}$ avoids a certain set, the bounds implied by this approach are way too large.

In this talk I describe three quite similar problems coming from different branches of mathematics (dynamical systems, homology of curves, and zero-sums), and two simple tricks which are surprisingly useful for solving such problems.

University of Rostock
Ulemnstraße 69
18057 Rostock
Germany

Wirsing's problem and uniform Diophantine approximation

Johannes Schleischitz

A longstanding big open problem in Diophantine approximation posed by Wirsing in 1961 is to decide whether for any given integer $n \geq 1$, any real number ζ is approximable to degree $n+1$ by algebraic numbers of degree at most n, or not. By approximable to degree η here we mean that

$$|\zeta - \alpha| \leq H(\alpha)^{-\eta}$$

has a solution with arbitrarily large values $H(\alpha)$, which is the height of the algebraic number α. For $n = 1$ this is true by the well-known Dirichlet Theorem, but apart from that only in the case $n = 2$ an affirmative answer was established by Davenport and Schmidt in 1967. For $n \geq 3$ the lower bound $(n+1)/2$ for the largest uniform η as above by Wirsing has been only very slightly improved since 1961. The talk aims to present links of Wirsings problem to certain exponents of Diophantine approximation, and recent results on these exponents, without proofs. The new methods might lead to a better understanding of Wirsing's problem in the future.

References:

Y. Bugeaud, J. Schleischitz, On uniform approximation to real numbers, to appear in Acta Arith., arXiv: 1512.00780.
E. Wirsing, Approximation mit algebraischen Zahlen beschränkten Grades, J. reine angew. Math. 206, (1961).

BOKU Vienna
Gregor-Mendel-Strae 1,
1190 Vienna
AUSTRIA

Groups and Intervals

Igor Shparlinski

In 1983, Erdős & Szemerédi proved a remarkable result, nowadays known as the **sum-product theorem**, which asserts that a set of integers A cannot simultaneously have a small sum-set $\{a_1 + a_2 \ : \ a_1, a_2 \in A\}$ and a small product-set $\{a_1 a_2 \ : \ a_1, a_2 \in A\}$. That is, it cannot behave as an arithmetic progression as well as a geometric progression. Since that time there has been an explosion of work in this direction: Bourgain–Katz–Tao, Solymosi, Garaev, Rudnev, Konyagin–Shkredov and many other. In particular, similar results have been obtained for many other algebraic structures: complex and real numbers, finite fields, polynomials and matrix rings over these fields, etc.. In this talk we mostly discuss the following **dual question**: *How big the intersection of an arithmetic progression of length H and a geometric progression of length T can be?*

We consider this question in the settings of finite fields $\mathbb{F}_p$ of p elements, where p is prime. Thus, arithmetic and geometric progressions are now given by sets of residues of the form ax and $b\vartheta^y$, where x and y run through some intervals consecutive integers of lengths H and T respectively, and $a, b, \vartheta \in \mathbb{F}_p^*$ are fixed. In particular, if T is the multiplicative order of ϑ then we have a question about the size of the intersection of an interval and a coset of a multiplicative subgroup of $\mathbb{F}_p^*$.

We outline various results and techniques which have been used in this area, together with a broad range of applications. These applications span from bounds of exponential and character sums to Fermat quotient to fixed points of the discrete logarithm, to distribution of g-ary digits in reciprocals of primes, to pseudopowers, to algorithms. We also pose several open questions.

School of Mathematics and Statistics
The University of New South Wales
Sydney NSW 2052
Australia

Divisibility of binomial coefficients by powers of two

Lukas Spiegelhofer

We are concerned with the number $\vartheta(j,n)$ of entries in the n-th row of Pascal's triangle that are exactly divisible by 2^j. In order to determine these values, we define digital functions in base 2: for a finite word w in $\{\mathtt{0},\mathtt{1}\}$ let $|n|_w$ be the number of occurrences of the word w in the binary expansion of $n \in \mathbb{N}$. It follows from the work of Barat and Grabner (2001) that $\vartheta(j,n)/\vartheta(0,n)$ is given by a polynomial P_j in the variables X_w, where w are certain finite words in $\{\mathtt{0},\mathtt{1}\}$, and each variable X_w is set to $|n|_w$.

In this short talk, we present a method for obtaining the coefficients of a given monomial in P_j as a generating function. For example, the monomial $X_{\mathtt{10}}$, corresponding to the term $|n|_{\mathtt{10}}$, occurs with coefficients $0, 1/2, -1/8, 1/24, -1/64, \ldots$ in the polynomials $P_0, P_1, \ldots$, which gives the generating function $\log(1+x/2)$. To give another, more generic, example, the coefficients of the monomial $X_{\mathtt{10}}^2 X_{\mathtt{1010}}^3$ are given by the generating function

$$\frac{1}{2!}\big(\log(1+x/2)\big)^2 \frac{1}{3!}\Big(\log\big(1+\tfrac{1}{2}x^3/(1+x/2)^2\big)\Big)^3.$$

In particular, the monomial $X_{\mathtt{10}}^2 X_{\mathtt{1010}}^3$ occurs first in the polynomial P_{11}, corresponding to exact divisibility by 2048. Besides providing insight into the structure of the polynomials P_j, our results allow us to compute the polynomials P_j in a very efficient way.

Coauthors: Michael Wallner

References: L. Spiegelhofer and M. Wallner, Divisibility of binomial coefficients by powers of primes, arXiv:1604.07089, submitted to a journal

Vienna University of Technology
Wiedner Hauptstraße 8–10
1040 Vienna
Austria

On a twisted version of the Linnik-Selberg conjecture

Raphael S. Steiner

We discuss cancellation in sums of Kloosterman sums against a new kind of twist: $\sum_{q\leq Q}\frac{1}{q}S(m,n,q)e_q(2\sqrt{mn}\alpha)$. By making use of Kuznetsov's trace formula we are able to prove bounds as strong as the ones given by Sarnak and Tsimerman for $\alpha = 0$ provided that $|\alpha| \leq 1-\delta$.

References: P. Sarnak and J. Tsimerman, "On Linnik and Selberg's conjecture about sums of Kloosterman sums", Algebra, Arithmetic, and Geometry: in honor of Yu. I. Manin. Vol. II, 2009, 619–635.

University of Bristol
Department of Mathematics
Bristol BS8 1TW
United Kingdom

On the Frobenius Problem for Beatty Sequences

Jörn Steuding

We discuss the Frobenius problem with respect to Beatty sequences, defined by $\mathcal{B}(\alpha) = \{\lfloor n\alpha \rfloor : n \in \mathbb{N}\}$. We show that, *given coprime* $a, b \in \mathbb{N}$ *and* $\alpha, \beta \in \mathbb{R}_{>1}$*, then, for every sufficiently large* $c \in \mathbb{N}$*, the equation* $aX + bY = c$ *is solvable with a solution* $x \in \mathcal{B}(\alpha)$ *and* $y \in \mathcal{B}(\beta)$ *if* $1, \frac{1}{\alpha}$ *and* $\frac{1}{\beta}$ *are linearly independent over* $\mathbb{Q}$*.* Moreover, in the special case $a = b = 1$ we are able to remove the linear independence condition: *for every pair of real numbers* $\alpha, \beta \in [1, 2)$*, the set* $\mathbb{N} \setminus (\mathcal{B}(\alpha) + \mathcal{B}(\beta))$ *is finite.*

This is joint work with Pascal Stumpf (also from Würzburg).

Würzburg University
Emil-Fischer-Str. 40
97 074 Würzburg
Germany

On the distribution of zeros of the first derivative of Dirichlet L-functions

Ade Irma Suriajaya

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, Akatsuka, and myself. Berndt, Levinson, and Montgomery investigated the general case, meanwhile Akatsuka and I gave sharper estimates under the truth of the Riemann hypothesis. Analogous to the case of the Riemann zeta function, the number of zeros and many other properties of zeros of the derivatives of Dirichlet L-functions associated with primitive Dirichlet characters were studied by Yildirim.

In this talk, we improve some results shown by Yildirim for the first derivative and show some new results. We also introduce two improved estimates on the distribution of zeros obtained under the truth of the generalized Riemann hypothesis. Finally, we introduce an equivalence condition for the generalized Riemann hypothesis, stated in terms of the distribution of zeros of the first derivative of Dirichlet L-functions associated with primitive Dirichlet characters.

Nagoya University
Furo-cho, Chikusa-ku, Nagoya
Japan

The Least Prime Number in a Beatty Sequence

Marc Technau

We prove an upper bound for the least prime in an irrational Beatty sequence. This result may be compared with Linnik's theorem on the least prime in an arithmetic progression.

Coauthors: Jörn Steuding

J. Steuding and M. Technau, The Least Prime Number in a Beatty Sequence, 2015, arXiv:1512.08382 [math.NT].

University of Würzburg
Emil-Fischer-Str. 40
97074 Würzburg
Germany

On a Counting Theorem of Skriganov

Niclas Technau

A deep counting theorem of Skriganov [1, Thm. 6.1] provides extraordinarily precise estimates for the number of lattice points in homogeneously expanding boxes - and more general polytopes - for lattices whose dual lattice is "weakly admissible".

In a joint work (in progress) with M. Widmer, the aforementioned counting result is extended for counting lattice points, of lattices whose dual lattice is weakly admissible, in certain inhomogeneously expanding, aligned boxes. Moreover, we give a number theoretic application, and show that certain further improvements are not possible.

Coauthors: M. Widmer

References: [1] M. M. Skriganov, *Ergodic theory on SL (n), Diophantine approximations and anomalies in the lattice point problem*, Inventiones mathematicae, **132**(1), 1998, 1–72

Graz University of Technology
Steyrergasse 30/II
8010 Graz
Austria

The number of prime solutions to (almost-all) linear inequalities

Aled Walker

In this talk we describe a new method, based on the classical work of Green-Tao, which yields asymptotic formulae for the number of prime solutions to a set of simultaneous linear inequalities. The type of inequality considered is that which is usually tackled by the Davenport-Heilbronn method – a Fourier-analytic approach – but the transference method succeeds in dramatically reducing the number of required variables, at least in a generic case. Indeed, provided the coefficients satisfy certain generic diophantine hypotheses – conditions which we hope to remove in future work – we may reduce the number of prime variables required from $2m + 1$ to $m + 2$, answering a question of Wooley.

Mathematical Institute
University of Oxford
Andrew Wiles Building
Radcliffe Observatory Quarter
Woodstock Road
Oxford
OX2 6GG
United Kingdom

Complete Mappings

Arne Winterhof

A permutation polynomial $f(x)$ over the finite field $\mathbb{F}_q$ of q elements is called a *complete mapping* if $f(x)+x$ is also a permutation polynomial.

In the first part of the talk we recall some known applications of these permutations including check digit systems.

The well-known Chowla and Zassenhaus conjecture, proven by Cohen in 1990, states that for any $d \geq 2$ and any prime $p > (d^2-3d+4)^2$ there is no complete mapping polynomial in $\mathbb{F}_p[x]$ of degree d.

In the second part of the talk, for arbitrary finite fields $\mathbb{F}_q$, we give a similar result in terms of the Carlitz rank of a permutation polynomial rather than its degree. We prove that if $n < \lfloor q/2 \rfloor$, then there is no complete mapping in $\mathbb{F}_q[x]$ of Carlitz rank n of small linearity. We also determine how far permutation polynomials $f(x)$ of Carlitz rank $n < \lfloor q/2 \rfloor$ are from being complete, by studying value sets of $f(x)+x$. We provide examples of complete mappings if $n = \lfloor q/2 \rfloor$, which shows that the above bound cannot be improved in general.

Coauthors: L. Isik, A. Topuzoğlu

References:

A. Winterhof, Generalizations of complete mappings of finite fields and some applications, J. Symbolic Comput. 64, 2014, 42–52.

L. Işık, A. Topuzoğlu, A. Winterhof, Complete mappings and Carlitz rank, Preprint 2016.

arne.winterhof@oeaw.ac.at

Johann Radon Institute for Computational and Applied Mathematics
Austrian Academy of Sciences
Altenbergerstr. 69
4040 Linz
Austria

Shorts in brief: exponential sums in short intervals and their applications

Trevor D. Wooley

We consider estimates for exponential sums over polynomials in which the summands lie in a short interval, discussing both pointwise bounds and mean values. These estimates find application in a number of problems of additive number theory, including variants of Waring's problem, super-strong approximation, and strong variants of uniform approximation. As might be expected, there are connections to efficient congruencing and Vinogradov's mean value theorem.

School of Mathematics
University of Bristol
University Walk, Clifton
Bristol BS8 1TW
United Kingdom, EU

Monday	**Monday**	**Tuesday**	**Tuesday**	**Wednesday**	**Wednesday**	**Thursday**	**Thursday**	**Friday**	**Friday**
Chair	**Tichy**	**Chair**	**Dietmann**	**Chair**	**Sander**	**Chair**	**Wooley**	**Chair**	**Shparlinski**
9.05-10.00	Wooley	9.05-10:00	Browning	9.05-9.25	Bugeaud	9.05-10.00	Heath-Brown	9.05-10:00	Dietmann
		10.05-10.25	Steiner	9.30-9.50	Steuding			10.05-10.25	Myerson
				9.55-10.25	Technau-Technau				
	coffee		**coffee**		**break**		**coffee**		**break**
Chair	**Heath-Brown**	**Chair**	**Drmota**	**Chair**	**Nowak**	**Chair**	**Browning**	**Chair**	**Ivic**
10.25-11.20	Brüdern	10.50-11.10	Frei	10.50-11.10	Schlage-Puchta	10.25-11.20	Shparlinski	10.45-11.05	Berczes
11.25-11.45	Pintz	11.15-11.35	Loughran	11.15-11.35	Schleischitz	11.25-11.45	Pach	11.10-11.30	Hajdu
11.50-12.10	Walker	11.40-12.30	eight 5 minutes talks	11.40-12.00	Radziejewski	11.50-12.10	Ostafe	11.35-11.55	Kazalicki
			Adzaga, Brandes, Büthe,	12.05-12.25	Nair			12.00-12.20	Madritsch
			Ciolan, Filipin, Halupczok					12.25-12.35	closing
			Hutle, Huxley						
12.30	lunch	12.30	lunch	12.30	lunch	12.30	lunch	12.30	lunch
Chair	**Schlage-Puchta**	**Chair**	**Larcher**			**Chair**	**Balog**		
14.30-14.50	Lapkova	**14.10**-15.20	nine 5 minutes talks		**free afternoon**	14.30-14.50	Larcher		
14.55-15.15	Müllner		Juhas, Karolus, Krenn,			14.55-15.15	Roche-Newton		
			Marnat, Munsch, Planitzer						
			Scheerer, Spiegelhofer,						
			Suriajaya						
15.20-15.40	Merai	15.20-16.10	poster view			15.20-15.40	Gyarmati		
15.40-16.10	**break**	**16.10-16.40**	**coffee**			**15.40-16.10**	**break**		
Chair	**Brüdern**	**Chair**	**Steuding**			**Chair**	**Elsholtz**		
16.10-16.30	Debaene	16.20-16.40	Aistleitner			16.10-16.30	Hegyvari		
16.35-16.55	Kumaraswamy	16.45-17.05	Ivic			16.35-16.55	Winterhof		
17.00-17.20	Hilberdink	17.10-17.30	Maier			17.00-17.20	Drappeau		
18.00	dinner	18.00	dinner			18.00	dinner		
		Chair	**Widmer**						
19.30		19.30	**problem session**			19.30			