Titles and Abstracts

• Abdullatif Altheyab, University of Melbourne
  **Isogenies of pointed conics and elliptic curves; a comparison**
  It is well-known that group structures on varieties have found applications in cryptography via the difficulty of the discrete logarithm problem in these structures. In this talk, we’ll define isogenies of pointed conics and compare them with the more well-known notion of an isogeny of elliptic curves. We’ll conclude with a brief discussion of the potential uses of conics in cryptography.

• Dmitry Badziahin, University of Sydney
  **Approximational properties of Mahler numbers**
  By Mahler numbers we mean values of Mahler functions at integer points; Mahler functions are the solutions of certain functional equations. They were introduced as a rich source of transcendental numbers. In this talk we ask the following question: how well can Mahler numbers be approximated by rationals? We will see that these numbers can show different approximational behaviour and are closely related to the Pade approximation of the underlying Mahler function. I will mention the latest results in this direction which say that the spectrum of irrationality exponents for a big class of Mahler numbers is contained in the set of rational numbers not smaller than two.

• Ayreena Bakhtawar, La Trobe University
  **Hausdorff dimension of the set of Dirichlet non-improvable numbers**
  An important consequence of Dirichlet’s theorem (1842) is that any irrational number can be approximated by infinitely many rationals with an error one over the denominator squared. Surprisingly, most results improve this corollary instead of Dirichlet’s original theorem. Recently, metric theoretic results for sets of real numbers admitting improvements to Dirichlet’s original theorem have been developed by Hussain, Kleinbock and others (2017, 2018). The classical set of well approximable numbers $K(\Psi)$ is properly contained in the set of Dirichlet non-improvable numbers $G(\Psi)$. In this talk, I will explain how we calculate the Hausdorff dimension for the set $G(\Psi) \setminus K(\Psi)$ and hence we show that the set of real numbers in $G(\Psi) \setminus K(\Psi)$ is uncountable. This is joint work with Philip Bos and Mumtaz Hussain.

• Jim Borger, ANU
  **What is a Witt vector?**
  This will be a introduction to the theory of Witt vectors, assuming nothing more than a familiarity with the concept of commutative ring.
Phil Bos, La Trobe University  
**Hausdorff measure and Dirichlet non-improvable numbers**

Let $\Psi : [1, \infty) \to \mathbb{R}_+$ be a non-decreasing function, $a_n(x)$ the $n$th partial quotient of $x$ and $q_n(x)$ the denominator of the $n$th convergent. The set of $\Psi$-Dirichlet non-improvable numbers

$$G(\Psi) := \left\{ x \in [0, 1) : a_n(x)a_{n+1}(x) > \Psi(q_n(x)) \text{ for infinitely many } n \in \mathbb{N} \right\},$$

is related to the classical set of $1/q^2 \Psi(q)$-approximable numbers $\mathcal{K}(\Psi)$ in the sense that $\mathcal{K}(3\Psi) \subset G(\Psi)$. Both of these sets enjoy the same $s$-dimensional Hausdorff measure criterion for $s \in (0, 1)$. We prove that the set $G(\Psi) \setminus \mathcal{K}(3\Psi)$ is uncountable by proving that its Hausdorff dimension is the same as that for the sets $\mathcal{K}(\Psi)$ and $G(\Psi)$. This answers a question raised by Hussain–Kleinbock–Wadleigh–Wang (2017). This is a joint work with Ayreena Bakhtawar and Mumtaz Hussain. In my talk, I will follow on from Ayreena’s preceding talk which sets the scene and I will sketch the proof.

Richard Brent, ANU and University of Newcastle  
**Asymptotic expansions and conjectures related to the exponential integral**

Let $f_0(z) = \exp(z/(1 - z))$ and $f_1(z) = \exp(1/(1 - z))E_1(1/(1 - z))$, where $E_1(x) = \int_x^\infty e^{-t}t^{-1}dt$ is an exponential integral. $f_0$ and $f_1$ satisfy the same differential equation $(1 - z)^2 f''' + (4z - 5)f'' + 2f' = 0$. In the unit disk $|z| < 1$, $f_0(z)$ and $f_1(z)$ may be represented by convergent power series, $\sum a_n z^n$ and $\sum b_n z^n$, respectively. Here $a_n$ and $b_n$ may be expressed in terms of confluent hypergeometric functions. We consider the asymptotic behaviour of the sequences $(a_n)$ and $(b_n)$ as $n \to \infty$, showing that they are closely related, and proving a conjecture of Bruno Salvy regarding $(b_n)$.

Let $\rho_n = a_n b_n$, so $\sum \rho_n z^n$ is the Hadamard product of $f_0(z)$ and $f_1(z)$. We obtain an asymptotic expansion $2n^{3/2} \rho_n \sim -\sum d_k n^{-k}$ as $n \to \infty$, where the $d_k$ are rational numbers satisfying a certain recurrence relation. Define $r_k = 2^{6k}d_k$. Then $(r_k)_{k \geq 0} = (1, -14, 86, -3660, \ldots)$. We can prove that $k!r_k \in \mathbb{Z}$. On the basis of numerical evidence for $k \leq 1000$, we conjecture that $r_k \in \mathbb{Z}$. An analogous result is known for the modified Bessel functions $I_\nu(z)$ and $K_\nu(z)$. This is joint work with Tony Guttmann (Melbourne) and Larry Glasser (Clarkson, NY).

Florian Breuer, University of Newcastle  
**Periods of Ducci sequences and odd solutions to a Pellian equation**

A Ducci sequence is a sequence of integer $n$-tuples generated by iterating the map

$$D : (a_1, a_2, \ldots, a_n) \mapsto (|a_1 - a_2|, |a_2 - a_3|, \ldots, |a_n - a_1|).$$

Such a sequence is eventually periodic and we denote by $P(n)$ the maximal period of such sequences for given $n$. Upper bounds on $P(n)$ have been known since the late 1980s. In this talk, I present a new upper bound in the case where $n$ is a power of a prime $p \equiv 5 \mod 8$ for which the Pellian equation

$$x^2 - py^2 = -4$$

has no solutions in odd integers $x$ and $y$. 


• Changhao Chen, UNSW Sydney

**A new sum-product estimate in prime fields**

Sum-product phenomena is a fundamental topic in additive combinatorics, and has many deep applications in exponential sums and character sums. Recently we improve the sum-product estimate of Shakan and Shkredov by putting things together in a more economical way. In this talk I will emphasise on applying incidence theorem to sum-product estimates. This is joint work with Bryce Kerr and Ali Mohammadi.

• Brendan Creutz, University of Canterbury

**There are no transcendental Brauer-Manin obstructions on abelian varieties**

Since work of Manin in the 1970s it has been known that the Brauer group of a variety over a number field can be used to obtain information about the rational points on said variety. The Brauer group has a subgroup of “algebraic” elements which are typically much easier to understand, and transcendental elements which are much trickier. For general varieties there can be information encoded in these transcendental elements that is not available from the algebraic subgroup. I will present a result showing that this is not the case for abelian varieties. This had been known since the work of Manin, conditionally on a widely believed conjecture (finiteness of Tate-Shafarevich groups of abelian varieties). My result is unconditional.

• Sasha Fish, University of Sydney

**On infinite discrete approximate subgroups in \( R^d \) and quasi-crystals**

A set \( A \) in \( R^d \) is a Meyer set (or quasi-crystal) if it is a relatively dense discrete subset which is also an approximate group, i.e., there exists a finite set \( F \) in \( R^d \) such that \( A - A \) is a subset of \( A + F \). Yves Meyer is early 70s proved the following result: A set \( A \) is a Meyer set if and only if it is a cut-and-project set. As a consequence of this theorem, we know that every Meyer set is originated from a lattice in an abelian continuous group. In this talk we address the question: what would be if we drop the assumption of the relative density in the definition of a Meyer set.

• Alex Ghitza, University of Melbourne

**Newforms modulo \( p \)**

We explore some of the issues surrounding the concept of being “new” for a modular form mod \( p \).

• Junsoo Ha, Korean Institute for Advanced Study, Korea

**The \( a \)-values of Riemann zeta function near the critical line**

Let \( \zeta(s) \) be the Riemann zeta function. We call the solutions to \( \zeta(s) = a \) the \( a \)-values of Riemann zeta function. Selberg has studied the vertical value distribution of the zeta-function near the critical line and shown that \( \log \zeta(1/2 + it) \) for \( t \in [T, 2T] \) behaves like a Gaussian random variable of the mean 0 and the variance \( \log \log T \). From this, he obtained the number of \( a \)-values on the box \( \sigma \geq 1/2 \) and \( t \in [T, 2T] \). Recently, Lamzouri, Lester and Radziwill obtained the discrepancy between the Riemann zeta function and its randomised model, and achieved the \( a \)-value result for \( \sigma > \sigma_0 > 1/2 \) for some fixed \( \sigma_0 \). In this talk, we survey the ideas behind their works and present the explicit range for which their result is valid. This is a joint work with Yoonbok Lee.
• David Harvey, UNSW Sydney
  **The truncated product problem**
  I will discuss recent progress on the problem of computing a truncated product, i.e., the high $N$ bits or the low $N$ bits of the product of two $N$-bit integers, using fast Fourier transform methods. Last year I proposed an algorithm that yields a 25% speedup for this problem, relative to the cost of computing the full $2N$-bit product. Unfortunately this only seems to work for multiplication algorithms based on transforms over complex numbers. I will explain why I would like to adapt this algorithm to the setting of transforms over finite fields (or rings), and what are the obstructions to doing so.

• Mumtaz Hussain, La Trobe University
  **A general principle for Hausdorff measure**
  We introduce a general principle for studying the Hausdorff measure of limsup sets. A consequence of this principle is the well-known Mass Transference Principle of Beresnevich and Velani (2006). Further, we use this principle in obtaining Hausdorff measure for beta dynamical systems. This is a joint work with David Simmons (York).

• Bryce Kerr, UNSW Sydney
  **On the constant in the Pólya–Vinogradov inequality**
  In this talk we explain how to obtain a new constant in the Pólya–Vinogradov inequality. The argument follows previously established techniques which use the Fourier expansion of an interval to reduce to Gauss sums. The improvement comes from approximating an interval by a function with slower decay on the edges which allows for a better estimate of the $\ell_1$ norm of the Fourier transform. This approximation induces an error for the original sums which is dealt with by combining some ideas of Hildebrand with Garaev and Karatsuba concerning long character sums.

• Simon Macourt, UNSW Sydney
  **A low energy decomposition of subsets in finite fields**
  The sum-product phenomenon has received much recent attention in the setting of finite fields. Furthermore, related problems on bounds on additive and multiplicative energy have found similar interest. In this talk we present an overview of these related questions and outline some recent results. We then present an extension of results of Roche-Newton, Shparlinski and Winterhof, which states that we can decompose a subset in finite fields into two disjoint subsets, $U$ and $V$, such that, for a suitably chosen rational function $f$, both $U$ and $f(V)$ have small energy.

• Thomas Morrill, UNSW Canberra
  **An elementary bound on Siegel zeroes**
  We consider Dirchlet $L$-functions $L(s, \chi)$, where $\chi$ is a real non-principal character modulo $q$. McCurley has shown that for such $L$-functions, there can be at most one real zero $\beta$ with $1 - c/\log q < \beta < 1$ and $c = 0.62$, which Kadiri improved to $c = 0.909$. We offer an improvement to $c$ based on Pintz’s elementary method.
• Uri Onn, ANU

On pro-isomorphic zeta functions
Pro-isomorphic zeta functions are Dirichlet series associated with finitely generated nilpotent groups that enumerate finite index subgroups having the same finite quotients as the parent group. They constitute a natural non-commutative analogue of Dedekind zeta functions. While other analogues, such as (normal) subgroup zeta functions, have been studied intensively, the study of pro-isomorphic zeta functions is in a far less advanced state. A unique feature of the latter is that they are closely related to zeta functions of algebraic groups, studied by Weil, Igusa and others. I will describe the tools used to study pro-isomorphic zeta functions and report on some recent results regarding zeta functions associated with members of a family of class-2 nilpotent groups called $D^*$-groups. This is a joint work with Mark Berman and Benjamin Klopsch.

• Alina Ostafe, UNSW Sydney

Unlikely intersections in arithmetic dynamics
The underlying motif of the talk is showing finiteness of various relations between elements of orbits in arithmetic dynamics with coefficients from structural sets, such as $S$-integers, subgroups and subfields of a number field. I will concentrate on multiplicative dependence between elements in orbits of algebraic dynamical systems over number fields modulo a finitely generated multiplicative subgroup of the field. Many of our results may be viewed as a blend of Northcott’s theorem on boundedness of preperiodic points and Siegel’s theorem on finiteness of solutions to $S$-unit equations. This is joint work with Attila Bérczes, Igor Shparlinski and Joseph Silverman.

• Dave Platt, University of Bristol

Turing’s method for the Selberg zeta-function
One key component in the numerical verification of the Riemann Hypothesis (e.g. for zeta) is Turing’s method for bounding the number of zeros in a piece of the critical strip. I will describe joint work with Andrew Booker that exploits the trace formula to develop a similar tool for the Selberg zeta-function for $\text{PSL}(2, \mathbb{Z}) \setminus \mathbb{H}$. Knowing (or caring) about such zeta-functions is not a pre-requisite.

• Tanja Schindler, ANU

Limit theorems on counting large continued fraction digits
Inspired by a result by Galambos on Lroth series we give a refinement of Galambos of the famous Borel–Bernstein Theorem for continued fractions and — closely related to this — a central limit theorem. As a side result we determine the first phi-mixing coefficient of the Gauss system. This is joint work with Marc Kesseböhmer.

• Min Sha, Macquarie University

On the density of multiplicatively dependent vectors
A vector with non-zero complex coordinates is called multiplicatively dependent if its coordinates are multiplicatively dependent. In this talk, I will present some recent work on the density of multiplicatively dependent vectors. For example, we show that they are everywhere dense both in the real spaces and in the complex spaces. We also
investigate the density in a more detailed manner by considering the covering radius of such vectors. This is joint work with Igor E. Shparlinski and Cameron L. Stewart.

• Igor Shparlinski, UNSW Sydney

On smooth square-free numbers in arithmetic progressions

A. Booker and C. Pomerance (2017) have shown that any residue class modulo a prime \( p \geq 11 \) can be represented by a positive \( p \)-smooth square-free integer \( s = p^{O(\log p)} \) with all prime factors up to \( p \) and conjectured that one can find such \( s \) with \( s = p^{O(1)} \). Using bounds on double Kloosterman sums due to M. Z. Garaev (2010) we prove this conjecture in a stronger form \( s \leq p^{3/2+o(1)} \). Furthermore, using some additional arguments we show that for almost all primes \( p \) one can replace \( 3/2 \) with \( 4/3 \).

We also consider general versions of this question, replacing \( p \)-smoothness of \( s \) by the stronger condition of \( p^\alpha \)-smoothness. Using bounds on multiplicative character sums and a sieve method, we can represent all residue classes by a positive square-free integer \( s \leq p^{2+o(1)} \) which is \( p^{1/(4e^{1/2})+o(1)} \)-smooth. This is joint work with Marc Munsch.

• Ade Irma Suriajaya, RIKEN (Wako, Japan)

Zeros of derivatives of the Riemann zeta function and Dirichlet \( L \)-functions

Speiser in 1935 showed that the Riemann hypothesis is equivalent to the derivative of the Riemann zeta function having no zeros in the left-half of the critical strip. The distribution of zeros of derivatives of the Riemann zeta function has been investigated by Berndt, Levinson, Montgomery, and Akatsuka. Berndt, Levinson, and Montgomery investigated the general case, while Akatsuka gave sharper estimates under the Riemann hypothesis, which were further improved by Ge. We introduce these and generalize the result of Akatsuka to higher-order derivatives of the Riemann zeta function.

Analogous to the Riemann zeta function, many properties of zeros of the derivatives of Dirichlet \( L \)-functions associated with primitive Dirichlet characters were studied by Yıldırım. We improve some results for the first derivative. We also introduce two improved estimates on the distribution of zeros obtained under the truth of the generalized Riemann hypothesis. We also extend the result of Ge to these Dirichlet \( L \)-functions when the associated modulus is not small. Finally, we introduce an equivalence condition analogous to that of Speiser’s for the generalized Riemann hypothesis.

• Daniel Sutherland, University of Newcastle

Investigating higher-dimensional Ducci sequences

A Ducci sequence is a sequence \( u_1, u_2, \ldots \in \mathbb{Z}^n \) of \( n \)-tuples given by \( u_{i+1} = Du_i \), where

\[ D(a_1, a_2, \ldots, a_n) := (|a_1 - a_2|, |a_2 - a_3|, \ldots, |a_{n-1} - a_n|, |a_n - a_1|). \]

These sequences are named in honour of Enrico Ducci who first studied them in the 1930s, and they possess many interesting properties. For example, since the entries of the tuples are bounded, every Ducci sequence will eventually become periodic. Moreover, every Ducci sequence for which \( n \) is a power of 2 will eventually vanish. While much is known about their periodic nature, there are still many open problems.

In this talk we generalise to the operator \( \mathcal{D}_2 : M_{m \times n}(\mathbb{Z}) \to M_{m \times n}(\mathbb{Z}) \) where

\[ \mathcal{D}_2(a_{i,j}) = (|a_{i,j} + a_{i+1,j+1} - a_{i+1,j} - a_{i,j+1}|). \]
Under this generalisation there now exist diverging Ducci sequences, yet there still appear to be certain values of $m$ and $n$ for which every $m \times n$ Ducci sequence is bounded and therefore eventually periodic. This talk will be a report on the experimental and theoretical results that we have obtained in our investigation thus far.

- Nicole Sutherland, University of Sydney

**Galois groups of reducible polynomials and Hilbert’s irreducibility theorem**

We take a detailed look at 2 computations which require the availability of an algorithm to compute Galois groups of reducible polynomials over $\mathbb{Q}(t)$ and also both rely on Hilbert’s Irreducibility Theorem.

- Chenyan Wu, University of Melbourne

**Arthur parameters, theta correspondence and period integrals**

We discuss how the theory of theta correspondence relates to the study of Arthur parameters attached to irreducible cuspidal automorphic representations. We also propose a refinement in terms of period integrals.

- Marley Young, UNSW Sydney

**Algebraic integers of bounded house in polynomial semigroup dynamics**

We consider semigroup dynamical systems defined by polynomials over a number field, and the orbit (tree) they generate at a given point. We obtain results for the set of initial points in the cyclotomic closure of this number field for which the orbit contains an algebraic integer of bounded house. This extends previous results for classical orbits generated by one polynomial obtained by Dvornicich and Zannier (for preperiodic points), and then by Chen and Ostafe (for roots of unity and elements of bounded house in orbits). This is joint work with Alina Ostafe.

- Yinan Zhang, ANU

**Cyclic extensions of prime degree and their $p$-adic regulator**

We present a conjecture on the distribution of the valuations of $p$-adic regulators of cyclic extensions of $\mathbb{Q}$ of odd prime degree. This is based on the observation of computational data of $p$-adic regulators of cyclic quintic and septic extensions of $\mathbb{Q}$ for $2 < p < 100$ with discriminant up to $5 \times 10^{31}$ and $10^{42}$ respectively, and noting that the observation matches the model that the entries in the regulator matrix are random elements with respect to the obvious restrictions. This is joint work with Tommy Hofmann (TU Kaiserslautern).