
Number Theory Down Under 14

Abstracts

31 August–4 September 2026

Canberra, Australia

Contents

1	Plenary talks	1
2	Contributed talks	3
3	Student talks	7

Plenary talks

Van der Waerden’s conjecture via twisted Chowla

Sam Chow

University of Warwick

In 1936, Van der Waerden conjectured that irreducible polynomials without full Galois group are substantially rarer than reducible polynomials. Bhargava spectacularly resolved the “Big O” version of this, leaving open the more refined “little o” version. I will present a conditional resolution of the latter, which is joint work with Anderson, Dietmann, Hokken, Koymans, and Lemke Oliver.

Rational points on subvarieties of abelian varieties

Brendan Creutz

University of Canterbury

The rational points on abelian varieties and their subvarieties are governed by celebrated theorems of Mordell, Weil, and Faltings. In this talk, I will consider these point sets from a topological perspective, using the topology induced by the adelic points of the ambient abelian variety. I will discuss conjectural descriptions of the resulting adelic closures and some recent results toward these conjectures and their consequences for rational points on subvarieties of abelian varieties.

Sharp lower bounds for sumsets

Felipe Gonçalves

Instituto de Matemática Pura e Aplicada

I will present a recent result obtained with Danylo Radchenko, where we solve a conjecture of Bourgain–Dilworth–Ford–Konyagin–Kutzarova. We prove a sharp lower bound for the cardinality of sumsets of subsets of $\mathbb{Z}^d$ confined to a hypercube. We prove that, for $A_j \subseteq \{0, 1, 2, \dots, m\}^d$,

$$|A_1 + \dots + A_n| \geq (|A_1| \cdots |A_n|)^{1/p}, \quad p = \frac{n \log(m+1)}{\log(nm+1)},$$

with the exponent best possible. The only previously known sharp cases were $A_j \subseteq \{0, 1\}^d$, for all $n \geq 1$, and $A_j \subseteq \{0, 1, 2\}^d$ for $n = 2$. The result is a corollary of a stronger sup-convolution inequality, whose proof is based on a novel mixed-volume representation of a lattice path norm, an application of the Alexandrov–Fenchel inequality, together with a sharp one-dimensional functional inequality.

Uniform bounds for fixed vectors in representations of a p -adic GL_N

Simon Marshall

University of Melbourne

Let G be a reductive p -adic group, K a compact open subgroup of G , and π a representation of G . Bernstein’s uniform admissibility theorem states that the dimension of fixed vectors in π under K , denoted $\dim \pi^K$, is bounded independently of π . On the other hand, if π is fixed and K varies in a family of principal congruence subgroups of G , $\dim \pi^K$ grows in a manner governed by the Gelfand–Kirillov dimension of π . In this talk, I will present a theorem for GL_N that combines these results, by proving a bound for $\dim \pi^K$ that is essentially as strong as the Gelfand–Kirillov bound but which is uniform in π . This is joint work with Rahul Dalal and Mathilde Gerbelli-Gauthier.

Zeros of the Riemann zeta-function under an “alternative” pair correlation setting

Ade Irma Suriajaya

Kyushu University

In recent work with Siegfried Alan C. Baluyot, Daniel Alan Goldston, Junghun Lee, Jordan Schettler, and Caroline L. Turnage-Butterbaugh, we studied the pair correlation of nontrivial zeros of the Riemann zeta-function without assuming the Riemann Hypothesis (RH). The pair correlation method was first suggested by H. L. Montgomery in 1973, when he proved, under RH, an asymptotic formula for the appropriate pair-correlation detecting function within a limited range.

Montgomery’s function in the remaining range is conjectured to satisfy a simple asymptotic formula that would imply the famous Montgomery Pair Correlation Conjecture (PCC) for zeros of the Riemann zeta-function. If, instead of the Riemann zeta-function alone, we consider a product of the Riemann zeta-function and a real (indeed quadratic) Dirichlet L -function, D. R. Heath-Brown showed at a 1996 AIM conference that the pair correlation of zeros of the two functions exhibits a contradictory distribution depending on whether or not the Dirichlet L -function has an exceptional (or Landau–Siegel) zero. If such an exceptional zero exists, we obtain a distribution that contradicts PCC and is now known as the Alternative Hypothesis (AH).

Although massive numerical evidence supports PCC and contradicts AH, AH is consistent with everything proven so far about the distribution of the zeros and is still far from being disproved. In our papers on pair correlation, we showed how to remove RH from Montgomery’s method and recover known results on the proportion of simple zeros under weaker hypotheses than previously required. By not assuming RH, our method also clarifies that the zeros captured are not only simple but lie on the critical line, giving the first result of this type.

In particular, with Daniel Goldston, Junghun Lee, and Jordan Schettler, we showed that asymptotically 100% of the zeros are simple and on the critical line assuming only either PCC or an appropriate form of AH. The former recovers Gallagher and Mueller’s 1978 conditional result under both RH and PCC, using only PCC by showing that PCC alone forces the zeros onto the critical line.

In this talk, I would like to introduce some of our basic ideas and show how to adapt them to AH. I hope to explain our approach using a new notion, the “horizontal multiplicity” of zeros, which is exactly the usual multiplicity if RH is true, but which, without RH, clarifies possible deviations in the horizontal positioning of the zeros.

Simple Zeros and Critical Zeros of the Riemann Zeta-Function

Caroline Turnage-Butterbaugh

Carleton College

Assuming the Riemann Hypothesis, Montgomery (1973) proved a theorem concerning the pair correlation of nontrivial zeros of the Riemann zeta-function. One consequence of this theorem is that, under RH, at least $(2/3)$ of the zeros are simple. In this talk, I will show that the pair correlation method can be used to prove results not only on the vertical distribution of zeros but on their horizontal distribution as well. In particular, I will discuss how to remove RH from Montgomery's theorem, and, upon assuming a much weaker hypothesis than RH, conclude that at least $(2/3)$ of the zeros are simple and that at least $(2/3)$ of the zeros are on the critical line.

Randomness and arithmetic in module lattices

Ilaria Viglino

École Polytechnique Fédérale de Lausanne

We study the extent to which lattices carrying additional arithmetic structure exhibit the statistical behaviour of random lattices. Using an effective number field analogue of a matrix counting theorem of Katznelson, we obtain quantitative versions of Rogers' moment formula for module lattices. This leads to Poisson-type statistics for short vectors and, in particular, sharp results on the distribution of the shortest vector.

Local–Global Visibility

Sneha Chaubey

Indraprastha Institute of Information Technology Delhi

Local–global principles ask whether a global arithmetic property can be detected from its behaviour at every prime, as in the Hasse principle and related questions in arithmetic geometry. In this talk, I will discuss a geometric instance of this theme for lattice points on parameterised algebraic curves through the origin. We introduce notions of global and p -adic visibility and investigate when visibility can be recovered prime by prime. Symmetry under a positive-weight $\mathbb{G}_m$ -action leads to a local–global principle, while the corresponding density questions connect local conditions, Euler products, and zeta values. Moreover, using nonhomogeneous families, we illustrate how local detectability can fail and provide a setting to study the size of the resulting local–global defect.

Contributed talks

Some Diophantine properties of coordinates and denominators of rational points on elliptic curves

Subham Bhakta

UNSW

The coordinates and denominators of rational points on elliptic curves carry interesting arithmetic information. Multiplicative dependence among such quantities is related to unlikely intersections in algebraic tori. Moreover, asking when denominators or their products are perfect powers leads to counting rational points on generalized Fermat curves, while representability as sums of two squares is connected to the existence of rational points on families of conics parameterized by products of elliptic curves. In this talk, I shall discuss how often these Diophantine phenomena occur.

Ducci Sequences and Codes

Florian Breuer

University of Newcastle

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

$$D : (x_1, x_2, \dots, x_n) \mapsto (|x_1 - x_2|, |x_2 - x_3|, \dots, |x_n - x_1|).$$

These sequences have been studied for nearly a century and still throw up some surprises. In this talk, I will outline new results linking Ducci sequences to cyclic codes, as well as new upper and lower bounds on their eventual periods.

Faster enumeration of primes

David Harvey

UNSW

I will discuss my recent paper on fast algorithms for finding all primes up to N (<https://arxiv.org/abs/2606.22851>). These are the first algorithms to achieve a speedup by a positive power of $\log N$ over the ancient sieve of Eratosthenes.

Computing Isotropic Vectors over Number Fields using Singular Square Classes

Przemysław Koprowski

University of Silesia

Isotropy is a central concept in the theory of quadratic forms. An isotropic vector of a given quadratic form is a nonzero vector where the form vanishes. Equivalently, an isotropic vector represents a non-trivial solution to a homogeneous quadratic equation. The problem of computing such vectors has a rich history, originating with the 18th-century works of Lagrange and Legendre, and continuing through modern developments in computational number theory by authors such as Cochrane and Mitchell, Cremona and Rusin, Simon, Castel, Kutas, and others.

Current approaches are limited in scope: while explicit algorithms exist for quadratic forms of arbitrary dimension over the rationals, these methods rely on properties specific to the rational numbers and do not generalize to other fields. Conversely, existing techniques for general number fields are restricted to forms of dimension no greater than three. This talk presents a novel method that utilizes the structure of singular square classes to compute isotropic vectors for quadratic forms of arbitrary dimension over any global field of characteristic not equal to 2.

The proposed method is of both theoretical and practical significance. I will discuss not only the mathematical framework of this approach, but also demonstrate its computational efficiency through its implementation as a function in the Magma computational algebra system.

Partitions with parity constraints on multiplicities

Darlison Nyirenda

University of the Witwatersrand

In this talk, partitions in which multiplicities of parts have restrictions on their parity are presented. Recurrence formulas and various partition identities are proved. A new refinement of Euler's partition theorem is obtained.

On finitely many Li coefficients

Neea Palojarvi

UNSW

In 1997, X.-J. Li proved an equivalent condition for the Riemann hypothesis. He showed that the Riemann hypothesis holds if and only if the real numbers

$$\lambda_n := \sum_{\rho} \left(1 - \left(1 - \frac{1}{\rho} \right)^n \right),$$

where the sum runs over the non-trivial zeros of the Riemann zeta-function, are non-negative for all positive integers n . The terms λ_n are called the *Li coefficients*. The condition has since been generalised for different functions.

A natural follow-up question is: what do finitely many Li coefficients tell us about the location of zeros? In this talk, I will discuss results answering that question. The talk is based on joint work with Samprit Ghosh and Nicol Leong.

The symbolic dynamics and parameter spaces of a piecewise linear map and its related circle map

John Roberts

UNSW

Lagarias and Rains introduced an area-preserving piecewise-linear map F_{ab} that is defined by applying

$$A = \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix} \quad \text{on the left half-plane, and} \quad B = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \quad \text{on the right half-plane,}$$

so the associated parameter space is (a, b) . This map sends the set of rays from the origin to itself and induces a homeomorphism f_{ab} of the unit circle. The natural parameter space of a circle map with the simplest symbolic dynamics of two symbols is (θ, ρ) , where θ is the rotation number and ρ is the density of one of the symbols in the infinite word associated with the circle map's orbits. For f_{ab} , θ and ρ are in general unknown functions of a, b . Nevertheless, we can begin to explore what part of the (θ, ρ) -space is accessible to f_{ab} , which is a manifestation of the constraints on the rotational language induced by the symbolic dynamics of F_{ab} . Continued fractions and Diophantine approximation play an important role in our analysis.

This is joint work with Franco Vivaldi (Queen Mary University of London) and Asaki Saito (Future University Hakodate).

Some stories about Liouville numbers: From Erdős and Mahler to today

Johannes Schleischitz

Western Sydney University

Liouville numbers are irrational real numbers that admit very good rational approximations. Several aspects of them have been studied in number theory and topology. We present selected results and open problems, from Erdős and Mahler to very recent findings. Regarding the latter, it will be discussed that an appropriate analogue of an open problem of Mahler (1984) on the image of Liouville numbers under transcendental functions fails in higher dimension.

Nine-distance theorem in three-dimensional space

Nikita Shulga

University of Sydney

The classical three-distance theorem (also known as the Steinhaus conjecture) states that the gaps determined by a finite one-dimensional Kronecker sequence have at most three distinct lengths. We prove that its natural d -dimensional analogue has at most $2^d + 1$ distinct lengths, which is the optimal bound in dimensions $d = 1, 2, 3$. This proves the conjecture of Haynes and Marklof about the three-dimensional distance conjecture.

An orthogonal perspective on Gauss composition

John Voight

University of Sydney

We revisit Gauss composition over number rings, showing that it is provided by the Clifford and norm maps, building on work of Kneser and Wood. We go further and clarify the emergence of narrow class groups, which arises naturally from the perspective of orthogonal groups. This is joint work with Haochen Wu.

The second moment of Ramanujan sums

Ziwei Hong

Renmin University of China

We study $C(x, y)$, the smoothed second moment of Ramanujan sums. Assuming the Riemann Hypothesis (RH), we establish an asymptotic formula for $C(x, y)$ with an improved error term. Our analysis applies uniformly to the case where x and y are arbitrarily close. In particular, we provide a meaningful comparison with the work of [1] in the case $y = 2x^2$. The method relies on the use of smooth cutoff functions, which provide greater flexibility in contour shifting.

Large values of Dirichlet L -functions over sets with small doubling

Bryce Kerr

UNSW

This talk is based on joint work with Pranendu Darbar, Marc Munsch and Igor Shparlinski. We study large values of Dirichlet L -functions $L(\sigma, \chi)$ when χ ranges over a set of characters with small doubling modulo q , obtaining conditional and unconditional results throughout the critical strip. Our methods use new zero-density estimates for Dirichlet L -functions over sets of characters with small doubling.

Student talks

Small(er) least primitive roots

Gustav Kjaerbye Bagger

UNSW

For a given prime p , a primitive root is a generator for the multiplicative group of integers modulo p . Burgess' inequality gives an asymptotic upper bound of roughly $p^{0.25}$ for the least such root, $g(p)$. Grosswald conjectured that $g(p)$ does not exceed $p^{0.5}$ whenever $p > 409$, which has been proven outside the interval $10^{15} < p < 10^{56}$. I will discuss progress towards the conjecture, both in terms of shrinking the interval and proving a weaker global bound for $g(p)$.

Equidistribution at the level of primes and upper bounds on L -functions at the edge of the critical strip

Saunak Bhattacharjee

UNSW

In this talk, we discuss how equidistribution of coefficients at primes can lead to improved upper bounds for certain L -functions at the edge of the critical strip. As applications, we establish new upper bounds for the L -function associated with non-CM elliptic curves over $\mathbb{Q}$, as well as for their symmetric power L -functions.

Estimating Ranks of Elliptic Curves: A Gaussian Approach

Blair Butler

University of Sydney

As the height of an elliptic curve becomes “large”, computations to determine the analytic or algebraic rank can be prohibitively expensive. We instead use the method of Bober to compute upper bounds, but exchange a compactly supported Fourier transform for a smooth log-Gaussian tail, which gives a tractable statistical formalism for truncation and sampling. We present results of calibration experiments for curves of height up to 10^{30} , and compare this with heuristics for the distribution of ranks.

This is joint work with John Voight and Edgar Costa.

Almost Primes Between Consecutive Squares

Peter Campbell

University of Queensland

Legendre’s conjecture asserts that there is a prime between every pair of consecutive squares. While this remains open, one can ask for the smallest k such that every interval $(n^2, (n+1)^2)$ contains an integer with at most k prime factors, counted with multiplicity.

Dudek and Johnston recently showed that $k = 4$ suffices for every $n \geq 1$. In this talk, I will describe an improvement showing that one may take $k = 3$. The proof combines analytic and computational methods. For $n^2 > 10^{31}$, the argument adapts Richert’s logarithmic weighted sieve to intervals between consecutive squares, together with an explicit linear sieve. For $n^2 \leq 10^{31}$, computational results on primes between consecutive squares and explicit bounds on maximal prime gaps yield the stronger result that every such interval contains an integer with at most two prime factors.

Refinements of Ingham’s Zero-Density Method

Shashi Chourasiya

UNSW

In this talk, I will revisit Ingham’s method for obtaining zero-density estimates for the Riemann zeta-function. The method combines a truncated Möbius approximation to $1/\zeta(s)$ with moment estimates for $\zeta(s)$ and a contour argument to bound $N(\sigma, T)$.

I will discuss several refinements to the original argument, including an improved estimate for a restricted Möbius sum, sharper bounds for the associated error terms, and the incorporation of recent results into the method. These updates lead to an improved zero-density estimate and demonstrate how recent developments can be used to sharpen different components of Ingham’s argument.

Transformation formulæ for Eisenstein series

Chandler Corrigan

UNSW

In this talk, we discuss an analogue of the van der Corput B -process for exponential sums twisted by the Fourier coefficients of newforms in the space of Eisenstein series of arbitrary weight and level. We also give an application of such results to estimating the associated Dirichlet polynomials. Similar results also hold for cusp forms.

Arithmetic Progressions of Primitive Elements in Finite Fields

Pasidhu Matthew Maseuge Fernando

UNSW

Primitive elements are fundamental objects in finite field theory. There is an extensive literature on the existence of m consecutive primitive elements in $\mathbb{F}_{q^n}$, where q is a prime power. A generalisation is to consider arithmetic progressions with a given non-zero common difference, requiring all terms to be primitive and at least one term to be normal. Lemos, Neumann and Ribas obtained concrete results for $m = 2, 3$ and asymptotic results for larger m . In this talk, I present further work on the $m = 4$ case, substantially improving their bound. This is joint work with Gustav Bagger.

Supersingularity testing

Leigh Greville

University of Melbourne

Supersingular elliptic curves have various cryptographic applications. González gives an elementary test for supersingularity in terms of the discriminant and the four torsion points of an elliptic curve. We prove that it is isomorphism invariant and determine its asymptotic error rate.

The Global Siegel Φ -operator and Satake compactification of Siegel quotient spaces for square-free level

Bowan Hafey

University of Melbourne

The Siegel Φ -operator takes Siegel modular forms of a certain degree to modular forms of a lower degree. When the weight is large enough, this is known to be surjective, but less is known for small weights. In Böcherer and Ibukiyama's 2012 paper, they prove surjectivity of the *global* Siegel Φ -operator for small weight and square-free level N . I will outline how their argument using theta series and the Witt operator can be extended. In doing so, we also give an arithmetic description of the configuration of cusps in the Satake compactification of Siegel quotient spaces of degree n with square-free level N . This is joint work with Chengjing Zhang and Alex Ghitza.

In search of explosive primes: the inverse volcano problem

Max Kortge

University of Melbourne

The connected components of the graph of ℓ -isogenies between ordinary elliptic curves over a finite field have a remarkable structure called ℓ -volcanoes. The inverse volcano problem asks whether a given volcano can occur as a connected component over $\mathbf{F}_{p^k}$, and for which primes p . We call such primes k -explosive. Every volcano has infinitely many 1-explosive primes, but existence can fail for larger k .

Our recent work, joint with Alex Ghitza and Dhruv Gupta, resolves the problem in most cases. After briefly surveying our results, I will work through one case from start to finish. Along the way, we will see how a question about isogeny graphs becomes one about class groups of imaginary quadratic orders, and why the depth of the volcano must be compared with the ℓ -adic valuation of k .

Rings of algebraic modular forms on special orthogonal groups

Miles Koumouris

University of Melbourne

By understanding the irreducible algebraic representations of a special orthogonal group over the rational numbers, we obtain a natural ring structure on the associated space of algebraic modular forms (AMFs) of fixed level. We then explicitly compute generators and relations for rings of AMFs on the related norm-1 group of a definite quaternion algebra, and discuss integral structure and reduction modulo p .

Subconvexity in algebraic number fields

Giulia Pelizzari

UNSW

The subconvexity problem for the Riemann zeta-function is a central topic in modern analytic number theory. What happens when one passes from $\mathbb{Q}$ to general number fields? In this talk, I will briefly review the current state of the art for the Riemann zeta-function before turning to Dedekind zeta-functions of number fields. I will conclude by discussing work in progress.

The number of primes in the interval (cp_i, p_i)

James Punch

UNSW

While working on a project related to explicit Burgess-strength bounds for character sums, I came across the following problem: for a positive integer i and real number $c \in (0, 1)$, how many prime numbers are in the open interval (cp_i, p_i) ? Call this $P(c, i)$. The prime number theorem tells us that, as i goes to infinity, $P(c, i)$ is asymptotic to $(1 - c)i$. However, some computation reveals

that $P(c, i)$ is typically less than or equal to $(1 - c)i$. I proved that this holds if c is not too large and i is not too small; in this talk, I will give an overview of the proof.

Positivity, Finiteness, and Flatness

Snehinh Sen

Australian National University

This talk will discuss some aspects of the intriguing and evolving theory of semirings. In short, a semiring is a “ring possibly without subtraction”. Thus we allow $\mathbb{N}$, $\mathbb{R}_{\geq 0}$, and the Booleans $\mathbb{B}$. More generally, for any ring homomorphism $f : R \rightarrow \mathbb{R}$, the canonical positive model $S_f = f^{-1}[0, \infty)$ is a semiring. For example, when R is a subring of $\mathbb{R}$, we may look at $S = R_{\geq 0}$.

The main goal of the talk is to discuss finiteness and flatness properties for modules over semirings, with particular attention to canonical positive models $R_{\geq 0}$. Among the finiteness properties considered is congruence Noetherianity. This is ongoing work with James Borger.

References

1. James Borger, “Witt vectors, semirings, and total positivity”, in *Absolute Arithmetic and $\mathbb{F}_1$ -Geometry*, pp. 273–329, EMS Zürich, 2016.
2. James Borger and Jaiung Jun, “Facets of module theory over semirings”, *Advances in Mathematics* **479** (2025), 110431.
3. Yefim Katsov, “On flat semimodules over semirings”, *Algebra Universalis* **51** (2004), 287–299.

Primes between cubes and explicit formulae

Simon Thomas

University of Queensland

The Riemann–von Mangoldt explicit formula provides useful estimates for the Chebyshev ψ -function and allows us to tie information about the zeros of the Riemann zeta-function to the distribution of primes. It is often beneficial to work instead with weighted versions of the ψ -function, and these have their own explicit formulae. In this talk, I will outline how optimizing these weights using techniques from Fourier analysis can help us find primes between cubes.

Spacing statistics of S -unit sequences

Ameya Tilgul

UNSW

Spacing statistics describe the local distribution of a sequence modulo 1, and provide a way of measuring how closely its behaviour resembles that of random points. In this talk, I will discuss the spacing statistics of sequences that arise from S -units. In particular, I will focus on how concepts from the theory of Diophantine equations can be used to study these local statistics.

On the summatory function of $d_3(n)$ **Sebastian Tudzi**

UNSW

In this talk, we discuss a sharper explicit bound for the error term $\Delta_3(x)$ in the summatory function

$$T_3(x) = \sum_{n \leq x} d_3(n),$$

where $d_3(n)$ counts the number of ways to write n as a product of three positive integers. This is obtained by combining an explicit third-moment estimate for $\zeta(\frac{1}{2} + it)$ with new convexity bounds for $\zeta(\sigma + it)$ on $\sigma \in [\frac{1}{2}, c]$.

Squarefree values of random polynomials

Watcharakiet Wongcharoenbhorn

UNSW

It is expected that every irreducible polynomial of degree $k \geq 4$ with integral coefficients and with no trivial obstruction assumes squarefree values infinitely often. Let $\varepsilon > 0$ be small and $A \geq 1$ be large. In 2024, Browning and Shparlinski proved a quantitative form of this conjecture on average over polynomials of height

$$N^{k-3+\varepsilon} \leq H \leq N^A.$$

In this talk, we will discuss our approach to extending this allowable range of height to

$$N^{\varpi+\varepsilon} \leq H \leq N^A,$$

where $\varpi \approx 0.382$ is an absolute constant independent of the degree. This is based on recent joint work with Bryce Kerr.

Height bounds on modular polynomials for various modular functions

Abraham Zhang

University of Newcastle

The classical modular polynomials Φ_N characterise isogenies between elliptic curves. This is useful in cryptography, for example in isogeny-based cryptography and efficient point counting on elliptic curves. The coefficients of Φ_N are large enough that storing them is difficult, so one may want to work with the modular polynomials $\Phi_{f,N}$ for other modular functions f . In this talk, I will give new explicit height bounds on modular polynomials for the j -invariant, the cube root of j , and the Weber $\mathfrak{f}$ -function. The preprint is available at <https://arxiv.org/abs/2607.22214>.

Quadratic characters on locally compact Hausdorff modules

Chengjing Zhang

University of Melbourne

I will discuss quadratic characters on locally compact Hausdorff modules over locally compact Hausdorff rings, as an analogue of quadratic forms over rings. In particular, I will describe the Witt group of quadratic characters over the integers, and explain its connection to the existence of even positive-definite unimodular lattices and the Weil index.

Sum-freeness and Point Counting

Zoë Gemmell

UNSW

Sum-free functions: what they are, where they came from, and where the area is going. This talk will cover joint work with Tim Trudgian and a concept introduced by Claude Carlet.