# Number Theory Down under 9 Abstracts

September 21, 2021

**Can You Hear the Shape of a Curve?**

Jeremy Booher
University of Canterbury, NZ

The zeta function of a curve over a finite field encodes the number of points on that curve. How much information does the zeta function of a curve plus the zeta function of natural covers give about the original curve? As the zeta function encodes the spectrum of Frobenius acting on the Tate module of the curve's Jacobian, this is analogous to the well-known question "Can You Hear The Shape of a Drum" concerning the spectrum of the Laplacian. I'll discuss several variants of this question considering different types of covers arising from geometric class field theory.

**A Sum Over Nontrivial Zeros of the Riemann Zeta-Function**

Richard Brent
Australian National University

Sums over nontrivial zeros of the Riemann zeta-function often arise in analytic number theory. In this talk I consider a special case that is analogous to the harmonic series. Although the sum diverges, we can estimate its "finite part" $H$ by a process of normalisation, analogous to how we can estimate Euler's constant $\gamma$ using the harmonic series.

I will describe three algorithms for the numerical approximation of $H$. The first is straightforward, with error $\ll (\log T)/T$ if we use the zeros $\rho$ satisfying $0 < \Im\rho < T$.

The second algorithm is more accurate, with error $\ll (\log T)/T^2$. It obtains about twice as many correct digits in the same time as the first algorithm.

The first two algorithms and their error bounds are unconditional. The third algorithm, due to Juan Arias de Reyna, is faster for the same accuracy, but assumes the Riemann Hypothesis.

This is joint work with Dave Platt and Tim Trudgian. For preprints, see arXiv:2009.05251 (for the case considered in this talk) and arXiv:2009.13791 (for more general results).

**Prime Spectroscopy**

Florian Breuer
University of Newcastle (AU)

This talk contains no new results; instead, I will show you a tool written in Sage for analysing sequences of prime numbers to determine if there is an L-function underlying their distribution. Perhaps somebody can put it to good use.

**Glasner property for polynomials and linear groups acting on the torus**

Kamil Bulinski
University of Sydney

A theorem of Glasner from 1979 shows that if $A$ is an infinite subset of the torus (real numbers mod 1) then for each $\epsilon > 0$ there exists an integer $n$ such that $nA$ is $\epsilon$-dense and Berend-Peres later showed that in fact one can take $n$ to be of the form $f(m)$ for any non-constant integer polynomial $f(x)$. Alon and Peres provided a general framework for this problem that has been used by Kelly-Lê and Dong to show that the same property holds for various linear actions on the $d$-dimensional torus. We complement the result of Kelly-Lê on the $\epsilon$-dense images of integer polynomial matrices in some subtorus (of the $d$ dimensional torus) by classifying those integer polynomial matrices that have the Glasner property in the full $d$-dimensional torus. We also extend a recent result of Dong by showing that if an irreducible linear group $\Gamma$ is generated by finitely many unipotent integer matrices then the action of $\Gamma$ on the torus has a uniform Glasner property. Based on joint work with Sasha Fish.

**Regular Sequences, Riesz Products and Ergodicity**

James Evans
University of Newcastle

Regular sequences are a generalisation of the automatic sequences which encompass many important number theoretic sequences. Unlike their predecessors however, the regular sequences may be unbounded, necessitating the development of new tools for their study. One such recent development is the concept of the Ghost Measure, which captures the sequences limiting shape. This talk discusses some recent work which connects this measure to the much more familiar Riesz Product construction. These similarities lead naturally to a proof that, under certain conditions, the ghost measures have pure Lebesgue decomposition. The core property which makes this possible is $D$-ergodicity, a generalisation of standard ergodicity. Finally, we discuss some of the number theoretic applications and consequences of this work.

**Modular forms of level divisible by the characteristic**

Alex Ghitza
University of Melbourne

The structure of the algebra of modular forms over finite fields has been studied extensively, motivated by applications to proving congruences. Many of the results can be stated as equivariant isomorphisms between certain modules for the Hecke operators. We give a framework for proving such isomorphisms (somewhat painfully, and only up to semisimplification) via calculations with the Eichler-Selberg trace formula. One reason to love this method (despite the parenthetical shortcomings given above) is that it applies in the case when the level is divisible by the residue characteristic, while the more elegant pre-existing approaches do not. This is joint work with Samuele Anni and Anna Medvedovsky.

**Recent progress on deterministic integer factorisation**

David Harvey
UNSW

There are several deterministic factoring algorithms of complexity $N^{1/4+o(1)}$ going back to the 1970s. Last year Hittmeir lowered the exponent to 2/9, and I subsequently improved it further to 1/5. In this talk I will explain the key ideas behind these new algorithms.

**Representation of an even number as a sum of four squares of primes**

Shehzad Hathi
UNSW Canberra at ADFA

In 1951, Linnik proved the existence of a constant $K$ such that every sufficiently large even number is the sum of two primes and at most $K$ powers of 2. Since then, this style of approximation has been considered for problems similar to the Goldbach conjecture. One such problem is the representation of a sufficiently large even number as a sum of four squares of primes and at most $k$ powers of two. In 2014, Zhao proved $k = 46$. We will discuss an improvement of this result.

**The Sum of a Prime and a Square-free Number with Divisibility Conditions**

Daniel Johnston
UNSW Canberra at ADFA

Every integer greater than two can be expressed as the sum of a prime and a square-free number. Expanding on recent work, we provide explicit and asymptotic results when divisibility conditions are imposed on the square-free number. We also discuss applications to other Goldbach-like problems.

**Cubic Weyl sums**

Bryce Kerr
University of Turku, Finland

In this talk I'll sketch some ideas which lead to new bounds for short exponential sums over cubic polynomials. After some motivation, I'll indicate how ideas of Enflo may be developed to make progress on the problem of improving Weyl's estimate and conclude with a discussion of potential applications and limitations.

**Approximating reals by rationals**

Dimitris Koukoulopoulos
University of Montreal

Given any irrational number $\alpha$, Dirichlet proved that there are infinitely many reduced fractions $a/q$ such that $|\alpha - a/q| \leqslant 1/q^2$. A natural question that arises is whether the fractions $a/q$ can get even closer to $\alpha$. For certain "quadratic irrationals" such as $\alpha = \sqrt{2}$ the answer is no. However, Khinchin proved that if we exclude such thin sets of numbers, then we can do much better. More precisely, let $(\Delta_q)_{q=1}^{\infty}$ be a sequence of error terms such that $q^2\Delta_q$ decreases. Khinchin showed that if the series $\sum_{q=1}^{\infty} q\Delta_q$ diverges, then almost all $\alpha$ (in the Lebesgue sense) admit infinitely many reduced rational approximations $a/q$ such that $|\alpha - a/q| \leqslant \Delta_q$. Conversely, if the series $\sum_{q=1}^{\infty} q\Delta_q$ converges, then almost no real number is well-approximable with the above constraints. In 1941, Duffin and Schaeffer set out to understand what is the most general Khinchin-type theorem that is true, i.e., what happens if we remove the assumption that $q^2\Delta_q$ decreases. In particular, they were interested in choosing sequences $(\Delta_q)_{q=1}^{\infty}$ supported on sparse sets of integers. They came up with a general and simple criterion for the solubility of the inequality $|\alpha - a/q| \leqslant \Delta_q$. In this talk, I will explain the conjecture of Duffin-Schaeffer as well as the key ideas in joint work with James Maynard that settles it.

**Number theory and modern cryptography**

Veronika Kuchta
University of Queensland

Cryptography is the science of hiding a message in such a way that only the eligible receiver of the message can read it. Number theory is a crucial mathematical discipline for public-key cryptography. The broadly used public-key cryptosystems such as RSA and elliptic-curve cryptography (ECC) are heavily based on number theoretical problems which assure the security of those cryptoschemes. In this talk we will see how the hardness of number theoretical problems can provide cryptographic security and how it affects the computational complexity of cryptosystems. As we all know, a fully-fledge quantum computer will be able to break public-key cryptography and will be a real threat to all information systems based on RSA or ECC. Cryptographers are working on solutions to this problem which constitute the new area of cryptography also known as post-quantum cryptography. In this talk we will also have an outlook at some areas of post-quantum cryptography such as lattice-based and isogeny-based cryptography.

**A new algorithm for computing zeta functions of algebraic curves**

Madeleine Kyng
UNSW

The zeta function of an algebraic curve over a finite field is a rational function which encodes algebraic and geometric information about the curve. An important problem in computational number theory is to give efficient algorithms to compute zeta functions of curves. Efficient algorithms have been developed for computing the zeta function for specific classes of curves (e.g. hyperelliptic curves), but at present there is no practical algorithm capable of handling an arbitrary curve. In this talk, we describe a new method for computing the zeta function of an arbitrary curve.

**Four Methods to Prove Mertens' Theorems and their Analogues**

Ethan Lee
UNSW Canberra at ADFA

In 1874, and 22 years prior to a rigorous proof of the celebrated prime number theorem, Mertens proved a series of three estimates that enable us to explore the distribution of prime numbers. Like the prime number theorem, Mertens' theorems can be generalised into other settings such as for number fields, primes in arithmetic progressions, or prime ideals which belong to a fixed conjugacy class and do not ramify in some Galois extension of number fields. In fact, because we can prove Mertens' theorems using different techniques to the prime number theorem, we can bypass some difficulties (such as exceptional zeros) when we seek to obtain explicit descriptions of the error terms in analogues of Mertens' theorems! This motivates the content of my talk; four methods to prove Mertens' theorems and their analogues, and some commentary on which method can suit different situations.

**On a Waring's problem for Hermitian lattices**

Jingbo Liu
Texas A&M University, San Antonio

Assume $E$ is an imaginary quadratic field and $\mathcal{O}$ is its ring of integers. For each positive integer $m$, let $I_m$ be the free Hermitian lattice of rank $m$ over $\mathcal{O}$ having an orthonormal basis. For each positive integer $n$, let $\mathfrak{S}_{\mathcal{O}}(n)$ be the set of all Hermitian lattices of rank $n$ over $\mathcal{O}$ that can be represented by some $I_m$. Denote by $g_{\mathcal{O}}(n)$ the smallest positive integer $g$ such that each Hermitian lattice in $\mathfrak{S}_{\mathcal{O}}(n)$ can be represented by $I_g$. In this talk, we shall provide an explicit upper bound for $g_{\mathcal{O}}(n)$ for all imaginary quadratic fields $E$ and positive integers $n$.

**Zeta functions in two-dimensional arithmetic**

Sean Lynch
UNSW

In 1955, G. Lustig computed the (Solomon) zeta function of a (commutative) two-dimensional regular local ring with finite residue field. The ring of power series in two variables over a finite field is an example of such a ring. In 1997, D. Segal computed the zeta function of the polynomial ring in one variable over a Dedekind domain that satisfies certain finiteness conditions. The ring of integers of a global field is an example of such a Dedekind domain. In this talk, we explore these zeta functions and how they are connected to interesting number theoretic problems e.g. integer partitions, number of isomorphism classes of finite modules and the distribution of primes.

**Finitary analysis in homogeneous spaces and applications**

Amir Mohammadi
University of California, San Diego

Rigidity phenomena in homogeneous dynamics have been extensively studied over the past few decades with several striking results and applications. In this talk, we will give an overview of recent activities related to quantitative aspect of the analysis in this context; we will also highlight some applications.

**Dynamical irreducibility of polynomials modulo primes**

Alina Ostafe
UNSW

In this talk we look at polynomials having the property that all compositional iterates are irreducible, which we call dynamical irreducible. After surveying some previous results (mostly over finite fields), we will concentrate on the question of the dynamical irreducibility of integer polynomials being preserved in reduction modulo primes.

More precisely, for a class of integer polynomials $f$, which in particular includes all quadratic polynomials, and also trinomials of some special form, we show that, under some natural conditions, the set of primes $p$ such that $f$ is dynamical irreducible modulo $p$ is of relative density zero. The proof of this result relies on a combination of analytic (the square sieve) and diophantine (finiteness of solutions to certain hyperelliptic equations) tools, which we will briefly describe.

**A combinatorial model for birational maps over finite fields**

John Roberts
UNSW

In the development of Pollard's integer factorization algorithm, the action of polynomials over finite fields is approximated by assuming, on average, it is modelled by a random mapping which then implies exploitable statistical behaviours. In previous work, we showed that a random permutation well approximates the expected dynamics of a "generic" polynomial automorphism over $d$-dimensional affine space, when reduced modulo a prime. Here, we extend this investigation to the expected dynamics of a birational map where a new dynamical feature is the singularities arising from denominators. We propose a combinatorial model and derive its expected statistical properties and compare these to actual experiments on birational maps. The broader aim of this work is to find the signature over finite fields of various dynamical properties of birational maps. The model presented here gives the background signature before other dynamical structures are imposed, which will have their own different combinatorial models. This is joint work with Tim Siu (UNSW).

**Regularity properties of $k$-Brjuno and Wilton functions**

Tanja Schindler
Scuola Normale Superiore di Pisa

The Brjuno function, first introduced by Yoccoz, is related to the continued fraction expansion and has already been studied extensively. In this talk we will look at functions related to the classical Brjuno function, namely, $k$-Brjuno functions and the Wilton function, the latter one going back to John Raymond Wilton. Both functions appear in the study of boundary regularity properties of (quasi) modular forms and their integrals. We consider various possible versions of them, based on the $\alpha$-continued fraction developments. We study their bounded mean oscillation properties and their behaviour near rational numbers of their finite truncations. If time allows we will further consider an extension of the $k$-Brjuno function and the Wilton function to the complex plane extending previous work by Marmi, Moussa and Yoccoz. This is joint work with Seul Bee Lee, Stefano Marmi and Izabela Petrykiewicz.

**The Lucas and Lehmer sequences in polynomial rings**

Min Sha
UNSW

In this talk, I will present some analogues of Zsigmondy's theorem and the primitive divisor results for the Lucas and Lehmer sequences in polynomial rings of several variables.

**Maximal Operators and Restriction Bounds for Weyl Sums**

Igor Shparlinski
UNSW

We describe several recent results on so called maximal operators on Weyl sums

$$S(u;N) = \sum_{1 \leqslant n \leqslant N} \exp(2\pi i(u_1 n + \ + u_d n^d)),$$

where $u = (u_1, ..., u_d) \in [0,1)^d$. Namely, given a partition $I \cup J \subseteq \{1,,,d\}$, we define the map

$$(u_i)_{i\in I} \mapsto \sup_{u_j,\, j\in J} |S(u;N)|$$

which corresponds to the maximal operator on the Weyl sums associated with the components $u_j$, $j \in J$, of $u$. We are interested in understanding this map for almost all $(u_i)_{i\in I}$ and also in the various norms of these operators. Questions like this have several surprising applications, including outside of number theory, and are also related to restriction theorems for Weyl sums.

**Explicit Atkinson formula**

Valeriia Starichkova
UNSW Canberra at ADFA

This talk is based on the joint work with Aleksander Simonic, a PhD student from UNSW Canberra. Atkinson provided a formula for the remainder term of the mean value of the Riemann zeta function on the critical line. This appeared to be a useful tool in order to get an upper bound for the remainder term and for the mean value of the Riemann zeta function itself. Atkinson formula contains a non-explicit term $O(log^2(T))$ depending on some parameter $T$, which was expressed explicitly in our work.

**Realizing Galois representations in abelian varieties by specialization**

Arvind Suresh
University of Georgia

Let K be a number field, and let G denote its absolute Galois group. We outline a method by which one may realize a given Galois module $V$ (i.e. $\mathbb{Q}[G]$-module) in the group $J(\bar{K})$ of points of an abelian variety $J/K$ (we say "$J$ realizes $V$"). The method can be regarded as a "twisted" version of the classical specialization method used by Neron, Mestre, Shioda, etc. to construct Jacobians with large Mordell–Weil rank. As an application, we prove that any Galois module V can be realized in infinitely many absolutely simple hyperelliptic Jacobians (of some fixed dimension $g$). As a corollary, we show that if $L/K$ is a finite extension and $R$ is a positive integer, then for any sufficiently large integer $g$ (the implied lower bound depending on $[L : K]$ and $R$), one can find infinitely many absolutely simple $g$-dimensional abelian varieties $J/K$ such that $\mathrm{rk}J(L) - \mathrm{rk}J(K)$ is at least $R$.

**Recent progress on Mobius pseudorandomness**

Terence Tao
University of California, Los Angeles

The (somewhat imprecise) Mobius pseudorandomness principle asserts that the Mobius function $\mu(n)$ (or close relatives of this function, such as the Liouville function $\lambda(n)$) asymptotically would not be expected to correlate with any other natural function that is not obviously sensitive to the prime factorisation of $n$ (except possibly at small primes). We discuss three closely related formalisations of this principle: the Chowla conjecture, the Sarnak conjecture, and the higher order uniformity conjecture. There have been many recent

advances on these conjectures, thanks to a landmark advance in analytic number theory by Matomaki and Radziwill, tools from additive combinatorics such as the inverse conjecture for the Gowers norms, as well as arguments from information theory and graph theory; these advances have in turn led to further applications, such as the solution to the Erdos discrepancy problem. We will survey these developments in this talk.

**Not zero, and then some!**

Tim Trudgian
UNSW Canberra at ADFA

To prove the prime number theorem is to show that $\zeta(1+it) \neq 0$. Showing that $\zeta(s)$ is even more non-zero near $s = 1 + it$ is surely better we get the prime number theorem and then some. The same remark applies to primes in arithmetic progressions and $L(1, \chi)$. The more non-zero it is, the better! I shall discuss recent work on this, available at arXiv:2107.09230, which is joint with Mike Mossinghoff (CCR, Princeton) and Valeriia Starichkova (UNSW Moscow).

**On a Diophantine equation of Erdős and Graham**

Maciej Ulas
Jagiellonian University, Poland

We study solvability of the Diophantine equation

$$\frac{n}{2^n} = \sum_{i=1}^{k} \frac{a_i}{2^{a_i}},$$

in integers $n, k, a_1, \ldots, a_k$ satisfying the conditions $k \geq 2$ and $a_i < a_{i+1}$ for $i = 1, \ldots, k-1$. The above Diophantine equation (of polynomial-exponential type) was mentioned in the monograph of Erdős and Graham, where several questions were stated. Some of these questions were already answered by Borwein and Loring. We extend their work and investigate other aspects of Erdős and Graham equation. In particular we construct an infinite set $\mathcal{K}$, such that for each $k \in \mathcal{K}$, the considered equation has at least five solutions and offer the upper bound for the value $a_k$ given in terms of $k$ only. As an application of our findings we enumerate all solutions of the equation for $k \leq 8$. Moreover, by apply greedy algorithm, we extend Borwein and Loring calculations and check that for each $n \leq 10^4$ there is a value of $k$ such that the considered equation has a solution in integers $n + 1 = a_1 < a_2 < \ldots < a_k$. Based on our numerical calculations we formulate some further questions and conjectures. This is joint work with Szabolcs Tengely nad Jakub Zygadło.

**Cylindric partitions and character identities**

Ole Warnaar
University of Queensland

As was shown in the 1980s by Kac, Peterson and Wakimoto, the characters of infinite dimensional Lie algebras provide a rich source of modular forms. Finding manifestly positive expressions for such characters remains, however, a difficult open problem. In this talk I will describe an approach to this problem using an affine variant of plane partitions.

**Arthur Parameters, Theta Correspondence and Periods for Unitary Groups**

Chenyan Wu
University of Melbourne

Let $\sigma$ be a cuspidal automorphic representation of a unitary group and let $\chi$ be a conjugate self-dual character. We analyse periods of Eisenstein series attached to the cuspidal datum $\chi \otimes \sigma$ and Fourier coefficients of theta lifts of $\sigma$. From this, we derive a constraint on the poles of the partial $L$-function $L^S(s, \sigma \times \chi)$ and hence also on certain simple factors of the global Arthur parameter of $\sigma$. In particular, we show certain types of Arthur packets cannot possess a cuspidal member.

**Moments of central values of quartic Dirichlet L-functions**

Liangyi (Lee) Zhao
UNSW

I will present asymptotic formula and bounds for the first and second moments of the central values of quartic Dirichlet L-functions. A corollary of the results is a quantitative non-vanishing theorem for these L-values. One of the key inputs is a large sieve type inequality for quartic Dirichlet characters. This is joint work with P. Gao.