NUMBER THEORY DOWN UNDER
23–26 SEPTEMBER 2016, NEWCASTLE
ABSTRACTS OF TALKS

1. **Shi Bai** (ENS Lyon, France)

   Title: Tuple lattice sieving

   Abstract: Lattice sieving is asymptotically the fastest approach for solving the shortest vector problem (SVP) on Euclidean lattices. All known sieving algorithms for solving SVP require space which (heuristically) grows as $2^{0.2075n+o(n)}$, where n is the lattice dimension. In high dimensions, the memory requirement becomes a limiting factor for running these algorithms. We show that sieving algorithms can be generalized to solve SVP with less memory. The idea is to consider reductions of tuples of vectors. We analyze the effects of using larger tuples for reduction, and conjecture how this provides a continuous tradeoff between the memory-intensive sieving and the asymptotically slower enumeration.

   The talk is based on a joint work with Thijs Laarhoven and Damien Stehlé.

2. **David Bailey** (California, USA)

   Title: Computer discovery and analysis of large Poisson polynomials using 64,000-digit arithmetic

   Abstract: In two earlier studies of lattice sums arising from the Poisson equation of mathematical physics, we established that a certain simple class of two-argument lattice sums $\phi(x, y)$ always reduce to an algebraic number when x and y are rational, and we also computed the explicit minimal polynomials associated with these algebraic numbers for a few specific rational arguments x and y. Based on these results, Jason Kimberley of the University of Newcastle conjectured a number-theoretic formula for the degree of the algebraic number in the case x = y = 1/s for some integer s.

   These earlier studies were hampered by the enormous cost and complexity of the requisite computations. In this study, we address the Poisson polynomial problem with significantly more capable computational tools. As a result of this improved capability, we have confirmed that Kimberley's formula holds for all integers s up to 52 (except for s = 41, 43, 47, 49, 51, which are still too costly to test), and also for s = 60 and s = 64. As far as we are aware, these computations, which employed up to 64,000-digit precision, producing polynomials with degrees up to 512 and integer coefficients up to 10^{229}, constitute the largest successful integer relation computations performed to date.

   By examining the computed results, we found connections to a sequence of polynomials defined in a 2010 paper by Savin and Quarfoot. These investigations subsequently led to a proof, by Watson Ladd of U.C. Berkeley, of Kimberley's formula and also the fact that when s is even, the polynomial is palindromic.

3. **Richard Brent** (ANU & Newcastle, Australia)

   Title: Accuracy of asymptotic approximations to the log-Gamma and Riemann-Siegel theta functions

   Abstract: This talk will describe some new bounds on the error in the asymptotic approximation of the log-Gamma function $\ln \Gamma(z)$ for complex z in the right half-plane. These improve on bounds by Hare (1997) and Spira (1971). I will show how to deduce similar bounds for asymptotic approximation of the Riemann-Siegel theta function $\vartheta(t)$,

and show that the attainable accuracy of a well-known approximation to $\vartheta(t)$ can be improved by including an exponentially small term in the approximation. This improves the attainable accuracy for real positive t from $O(\exp(-\pi t))$ to $O(\exp(-2\pi t))$

4. **YoungJu Choie** (POSTECH, Korea

Title: Period of modular forms on $\Gamma_0(N)$ and products of Jacobi Theta functions

Abstract: We give a closed formula for the sum of all Hecke eigenforms on $\Gamma_0(N)$, multiplied by their odd period polynomials in two variables, as a single product of Jacobi theta series for any squarefree level N. We also show that for $N = 2, 3$ and 5 this formula completely determines the Fourier expansions all Hecke eigenforms of all weights on $\Gamma_0(N)$. This is a Generalizing a result of Zagier in 1991 for modular forms of level one.

This is a joint work with Yoonkyung Park and Don Zagier.

5. **Shaun Cooper** (Massey, NZ)

Title: Hypergeometric modular transformations and Ramanujan's series for $1/\pi$

Abstract: We use the theory of theta functions to derive hypergeometric transformation formulas and show that a large number of functions are equal. We recover several identities of Goursat along with many that are new. We discuss applications to Ramanujan's series for $1/\pi$ and show how to obtain iterations that converge rapidly to $1/\pi$.

6. **Lassina Dembele** (Warwick, UK)

Title: On the compatibility between base change and Hecke action

Abstract: : Let F/E be a Galois extension of totally real number fields. In this talk, we will discuss the action of $Gal(F/E)$ on Hecke orbits of automorphic forms on GL_2. This reveals some compatibility between base change and Hecke action, which has several implications for Langlands functoriality.

7. **Karl Dilcher** (Halifax, Canada)

Title: Generalized Fermat Numbers: Some Results and Applications

Abstract: After reviewing the current status of factoring attempts of Fermat numbers, I will discuss some theoretical and computational results on generalized Fermat numbers. Finally, I will present a recent application of factors of generalized Fermat numbers to the study of congruences involving Gauss factorials.

This is joint work with John B. Cosgrave.

8. **Alexander Fish** (Sydney, Australia)

Title: Applications of a measure rigidity to recurrence.

Abstract: We present a new approach (joint with M. Bjorklund (Chalmers)) for establishing the recurrence of a set, through measure rigidity of associated action. Recall, that a subset S of integers (or of another amenable group G) is recurrent if for every set E in integers (in G) of positive density there exists a non-zero s in S such that the intersection of E and $E - s$ has positive density. By use of measure rigidity results of Bourgain-Furman-Lindenstrauss-Mozes and Benoist-Quint for algebraic actions on homogeneous spaces, we prove that for every set E of positive density inside traceless square matrices with integer values, there exists $k \geq 1$ such that the set of characteristic polynomials of matrices in $E - E$ contains ALL characteristic polynomials of traceless matrices divisible by k. As one of the corollaries we obtain that the set of all possible discriminants $D = \{xy - z^2 \mid x, y, z \in B\}$ over a Bohr-zero set B contains a non-trivial subgroup of the integers.

9. **Amy Glen** (Murdoch, Australia)

   Title: A combinatorial approach to a problem on the distribution of real numbers modulo 1

   Abstract: I will discuss a combinatorial approach to obtaining a complete description of the minimal intervals containing all fractional parts $\{r2^n\}$, $n \geq 0$, for some positive real number r, as well as some related open problems.

10. **David Harvey** (UNSW, Australia)

    Title: Fast integer multiplication and the distribution of primes

    Abstract: Several authors have recently proposed integer multiplication algorithms that depend on conjectures about the distribution of certain types of prime numbers. I will explain how these algorithms work and discuss a new algorithm of this type.

11. **Hidenori Katsurada** (Muroran, Japan)

    Title: L-functions and congruence of automorphic forms

    Abstract: As is well known, there is congruence between the Eisenstein series of weight 12 and Ramanujan?s delta function. In this talk, we consider its analogue in Siegel modular forms case, that is, we consider congruence between a 'lift? of an elliptic modular form and a Siegel modular form not coming from the lift.

12. **Simon Kristensen** (Aarhus, Denmnark)

    Title: Metric Diophantine approximation in absolute value

    Abstract: In classical Diophantine approximation, one considers the proximity to the integer lattice of a system of linear forms evaluated at integer points. In numerous applications, it is however more natural to consider the proximity to the origin rather than to the integer lattice.

    In the talk, I will outline results and methods from a series of joint papers with various authors, including Fischler, Levesley, Hussain and Simmons. Particular emphasis will be given to recent work on inhomogeneous approximation in absolute value, which is joint work with Hussain and Simmons. I will also discuss one or two applications of the theory.

13. **Brendan McKay** (ANU, Australia)

    Title: Counting Integer Matrices

    Abstract: Let $M(m, n, s, t)$ denote the number of $m \times n$ matrices of nonnegative integers such that each row sum is s and each column sum is t. Despite the simplicity of the question, there is no general solution known in closed form and in many cases even the asymptotic behaviour is unknown. In the talk we will survey number-theoretic methods for obtaining exact values, probabilistic methods for obtaining approximate values, and combinatorial and complex-analytic methods for finding asymptotic values. (Joint work with Rod Canfield, Catherine Greenhill, and Jeanette McLeod)

14. **Judy-anne Osborn** (Newcastle, Australia)

    Title: Probabilistic lower bounds on maximal determinants of binary matrices

    Abstract: I will talk about my work with Richard Brent and Warren Smith on the Hadamard maximal determinant problem.

    Hadamard (1893) proved an upper bound $n^{n/2}$ on the determinant of a $\{\pm 1\}$-matrix of order n. The bound is tight if and only if there exists a Hadamard matrix of order n.

Such n must be 1, 2, or a multiple of 4. The Hadamard conjecture is that a Hadamard matrix exists for every order n that is a multiple of 4.

For other ("non-Hadamard") orders various lower bounds on the maximal determinant have been proved by deterministic methods, but they differ from the Hadamard bound by a factor at least of order $n^{1/2}$. In this talk I will show how we used the probabilistic method of Erdős to obtain sharper lower bounds.

If the Hadamard conjecture is true, then our results imply that the best lower bounds are within a constant factor (11 percent) of the Hadamard upper bound.

15. **Alina Ostafe** (UNSW, Australia)

Title: On some extensions of the Ailon-Rudnick Theorem

Abstract: Let a, b be multiplicatively independent positive integers and $\varepsilon > 0$. Bugeaud, Corvaja and Zannier (2003) proved that

$$\gcd(a^n - 1, b^n - 1) \leq \exp(\varepsilon n)$$

for a sufficiently large n. Ailon and Rudnick (2004) considered the function field analogue and proved a much stronger result, that is, if $f, g \in \mathbb{C}[X]$ are multiplicatively independent polynomials, then there exists $h \in \mathbb{C}[X]$ such that for all $n \geq 1$ we have

$$\gcd(f^n - 1, g^n - 1) \mid h.$$

In this talk we present some extensions of the result of Ailon and Rudnick, both in the univariate and multivariate cases. These extensions rely on results on the intersection of curves with algebraic subgroups of codimension at least 2, Hilbert's irreducibility theorem and a result of Granville and Rudnick about torsion points on hypersurfaces.

16. **Min Sha** (Macquarie, Australia)

Title: Multiplicative dependence and independence of the translations of algebraic numbers

Abstract: We say that non-zero complex numbers $\alpha_1, \ldots, \alpha_n$ are multiplicatively dependent if there exist integers $k_1, \ldots, k_n$, not all zero, such that $\alpha_1^{k_1} \cdots \alpha_n^{k_n} = 1$. In this talk, we first present that given pairwise distinct algebraic numbers $\alpha_1, \ldots, \alpha_n$, the numbers $\alpha_1 + t, \ldots, \alpha_n + t$ are multiplicatively independent for all sufficiently large integers t. Then, for a pair (a, b) of distinct integers, we will say something about how many pairs $(a+t, b+t)$ are multiplicatively dependent when t runs through the integers. This is joint work with Art?ras Dubickas.

17. **Igor Shparlinski** (UNSW, Australia)

Title: Distribution of Points on Modular Hyperbolas

Abstract: We'll give a survey of various interesting results about the set of points on the modular hyperbola $xy \equiv 1 \pmod{p}$ for a prime p. These results show that this curve is not a typical curve $f(x, y) \equiv 0 \pmod{p}$ and also have many surprising applications to other, seemingly unrelated, areas. Some of these properties can also be extended to points satisfying the congruence $xy \equiv 1 \pmod{n}$ for a composite n, where they become even more special.

18. **Allan Steel** (Sydney, Australia)

Title: Reduce Everything to Multiplication (with GPUs)

Abstract: Most fundamental algorithms in computer algebra involving integers, polynomials or matrices can be reduced to some form of multiplication. This can lead to great speedups for large inputs when such multiplications are performed by asympotically-fast algorithms. In recent years I have developed algorithms within the Magma Computer

Algebra system which exploit NVIDIA Tesla Graphical Processing Units (GPUs) when possible, and the speedups are even more dramatic, as I will demonstrate.

19. **Yohei Tachiya** (Hirosaki, Japan)

Title: Arithmetical properties for the values of Jacobi theta functions

Abstract: In this talk, we will survey some results on arithmetical properties for the values of Jacobi theta functions. In particular, we will introduce algebraic independence (and dependence) results for the values of the function $\theta(q) = 1 + 2\sum_{n=1}^{\infty} q^{n^2}$ at some distinct algebraic points. This is joint work with Carsten Elsner.

20. **Tim Trudgian** (ANU, Australia)

Title: A Tale of Two Omegas

Abstract: Sums of $(-1)^{\Omega(n)}$, where $\Omega(n)$ is the total number of prime factors of n, have been thoroughly studied in the literature. They are connected to the Riemann zeta-function. Little has been written on sums of $(-1)^{\omega(n)}$, where $\omega(n)$ is the number of distinct prime factors of n. I shall present results that compare these sums.

This is joint work with Mike Mossinghoff.

21. **Bao-Wei Wang** (HUST, China)

Title: Dynamical Diophantine approximations in dynamical systems

Abstract: Dynamical Diophantine approximation concerns the Diophantine properties of the orbit in a dynamical system. More precisely, let (X, T) be a dynamical system with a metric $|\cdot|$. One concerns the size of the following limsup defined via a dynamical system:

$$W(\varphi) := \Big\{x \in X : |T^n x - y| < \varphi(n, x), \text{ i.o.}, n \in \mathbb{N}\Big\}.$$

In this talk, we pay attention to the Hausdorff dimension of the above set in a general framework when $\varphi(n, x) = e^{-(f(x)+\cdots+f(T^{n-1}x))}$. It is shown that, under some regular conditions on the system, the dimension of the $W(\varphi)$ is given by the solution to the pressure function

$$\mathsf{P}(-s(\log|T'| + f)) = 0.$$

while the dimension of the phase space X is given by the solution to

$$\mathsf{P}(-s\log|T'|) = 0.$$

For its partial analogy with the mass transference principle in classic Diophantine approximation, we call the dimension of $W(\varphi)$ as a *dynamical dimension transference principle.* This is a joint with Guahua Zhang.

22. **Yinan Zhang** (ANU, Australia)

Title: Valuations of p-adic regulators of cubic cyclic fields

Abstract: We observe the valuation of p-adic regulators of cubic cyclic fields, have computed them for fields with discriminant $< 10^{16}$ and odd prime $p < 100$, and present an interesting conjecture on their distribution. This is joint work with Tommy Hofmann (TU Kaiserslautern).

23. **Paul Zimmermann** (INRIA, France)

Title: Multiple-Precision Arithmetic: from MP to MPFR.

Abstract: Richard P. Brent published in 1978 the MP package for multiple-precision arithmetic in Fortran. Multiple-precision floating-point arithmetic is now mandatory in every mathematical software tool (Pari/GP, Maple, Mathematica, Sage, ...), and MP is

still a major reference. Inspired by both MP and the IEEE 754 standard, in 1999 started the design of GNU MPFR, a multiple-precision floating-point library for the C language with "correct rounding". As in MP, several efficient algorithms are implemented in MPFR. The talk will describe the main characteristics of MPFR, and will present some very recent work to speed up the basic arithmetic routines for small precision (up to 2 machine words).

24. **Ana Zumalacárregui** (UNSW, Australia)

Title: Strategies to solve congruence problems

Abstract: We will review some of the classical strategies to solve congruence problems and discuss the limits to them. We will focus in estimating the number of solutions to

$$f(x, y) \equiv 0 \pmod{p} \quad 1 \leq x, y \leq M$$

where f is some interesting function (polynomial, exponential, etc.).

When M is large, the classical approach on character sums/Fourier Analysis allow us to obtain asymptotics for this quantity. Nevertheless, there seems to be a barrier to this method at $M = p^{1/2}$ and new ideas, based on Additive Combinatorics, are required for the case when M is small.

We will discuss for some explicit examples the kind of results that can be obtained for very small M and which techniques are exploited as well as possible generalizations of these questions in finite fields.