NUMBER THEORY DOWN UNDER 5
29 SEPTEMBER–2ND OCTOBER 2017, BENDIGO
ABSTRACTS OF TALKS

1. **Dzmitry Badziahin (Sydney, Australia)**

   Title: Approximational properties of certain Mahler numbers.

   Abstract: In the talk we will present several results about irrationality exponents together with some more sensitive measures of irrationality for a class of Mahler numbers defined by infinite products. Many of the resuts from the talk were achieved with help of recently discovered recurrent formulae for the continued fraction of the corresponding Mahler functions.

2. **James Borger (ANU, Australia)**

   Title: Lambda-algebraic geometry as a framework for explicit class field theory

   Abstract: In classical explicit class field theories, one shows that abelian extensions of number fields can be generated using torsion points on certain algebraic groups. Over the rationals, we use the multiplicative group (Kronecker-Weber theorem), and over imaginary quadratic fields, we use elliptic curves with complex multiplication. Hilbert in his 12th problem asked whether it's possible to go beyond these two cases. Although there have been important developments since then (due to Shimura-Taniyama and Darmon, for instance), there is still no full solution known for any number field beyond the two cases above known to Kronecker.

   In this talk, I'll explain how 'lambda-algebraic geometry', an algebraic geometry based on lambda-rings instead of rings, provides an alternative framework for explicit class field theory, which in many respects is more satisfying than the traditional frameworks. In particular, it allows for some precise yes/no formulations of Hilbert's problem, which I'll discuss.

   This talk will be based on joint work with Bart de Smit.

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

   Title: The Kolakoski Sequence and Some Fast Algorithms, Part 2
   Abstract: This is part 2 of a talk describing joint work with Judy-anne Osborn. Let $\delta(n) := \sum_{1\le j\le n}(-1)^{k_j}$ be the Kolakoski discrepancy function, where k_j is the j-th term of the Kolakoski sequence.

   The obvious algorithm to compute $\delta(n)$ takes time and space linear in n. Nilsson (2012) gave an algorithm for computing $k_1 \ldots k_n$, and hence $\delta(n)$, in time $O(n)$ and space $O(\log n)$. We describe two algorithms that compute $\delta(n)$ faster, using a space-time tradeoff. The algorithms use ideas of Nilsson and Rao. It is conjectured that both algorithms run in time and space $O(n^{\alpha+\varepsilon})$, for all $\varepsilon > 0$, where $\alpha = \log(2)/\log(3) \approx 0.631$.

   Using our algorithms, we have computed $\delta(n)$ for various $n \le 5\times 10^{19}$, confirming and extending results of Rao (2012) for $n \le 10^{18}$. We find that $|\delta(n)| < 0.27\, n^{1/2}$ for all $n \in [1572, 5\times 10^{19}]$. This provides evidence for the conjecture that $\delta(n) = O((n \log\log n)^{1/2})$. The $(\log\log n)^{1/2}$ factor in this conjecture is motivated by Khinchin's 1924 "law of the iterated logarithm".

4. **Grant Cairns (La Trobe, Australia)**

   Title: The Quartic Residues Latin Square

   Abstract: We establish an elementary, but rather striking pattern concerning the quartic residues of primes p that are congruent to 5 modulo 8. Let g be a generator of the multiplicative group of $\mathbb{Z}_p$ and let M be the 4×4 matrix whose $(i+1),(j+1)-$th entry is the number of elements x of $\mathbb{Z}_p$ of the form $x \equiv g^k \pmod{p}$ where $k \equiv i \pmod{4}$ and $\lfloor 4x/p \rfloor = j$, for $i, j = 0, 1, 2, 3$. We show that M is a Latin square, provided the entries in the first row are distinct, and that M is essentially independent of the choice of g. As an application, we prove that the sum in $\mathbb{Z}$ of the quartic residues is $\frac{p}{5}(M_{11} + 2M_{12} + 3M_{13} + 4M_{14})$.
   This is joint work with Christian Aebi (Collège Calvin, Geneva) and has appeared in Integers **17** (2017) A35.

5. **Zhengyu Chen (Keio, Japan)**

   Title: On metrical theory of Diophantine approximations over imaginary quadratic fields

   Abstract: We discuss the Lebesgue measure and Hausdorff dimension of certain sets related to Duffin-Schaeffer conjecture over an imaginary quadratic field $\mathbb{Q}(\sqrt{d})$. Duffin-Schaeffer conjecture state that for an inequality of $|\alpha - m/n| < \psi(n)/n$ with $g.c.d.(m,n) = 1$, there are infinitely many solutions of positive integers m and n for almost all $\alpha \in \mathbb{R}$ if and only if $\sum_{n=2}^{\infty} \phi(n)\psi(n)/n = \infty$. In 1978, J.D.Vaaler proved this conjecture under the additional condition $\psi(n) = \mathcal{O}(n^{-1})$. We first define the Duffin-Schaeffer conjecture over an imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ with d is a square-free negative integer, and then show a Vaaler-type theorem over the imaginary quadratic field. We also look at the Hausdorff dimension of certain sets related to Diophantine approximations over the imaginary quadratic field and show that, for an infinite subset $\mathcal{A}$ of $\mathbb{Z}[\omega]\backslash\{0\}$, the set of $z \in \mathbb{C}$ with $|z - a/r| < 1/|r|^{1+\rho}$ having infinitely many solutions of $a \in \mathbb{Z}[\omega]$ and $r \in \mathcal{A}$ with some $\rho > 0$ has Hausdorff dimension $2(1+\gamma)/(1+\rho)$, where γ is the sup of h such that $\sum_{r \in \mathcal{A}} 1/(|r|^2)^h$ diverges. We also discuss the Hausdorff dimension of the set of the Diophantine inequality concerning the Duffin-Schaeffer conjecture over $\mathbb{Q}(\sqrt{d})$.

6. **Shaun Cooper (Massey, New Zealand)**

   Title: The Ramanujan–Mordell theorem for sums of squares, and some extensions.

   Abstract: Jacobi's sum of four squares theorem states that for any positive integer n, the number of solutions in integers of the equation

$$x^2 + y^2 + z^2 + w^2 = n$$

   is equal to eight times the sum of the divisors of n that are not multiples of 4. It implies Lagrange's theorem that every positive integer is a sum of four squares. Jacobi's theorem can be stated in the analytic form

$$\left(\sum_{j=-\infty}^{\infty} q^{j^2} \right)^4 = 1 + 8 \sum_{j=1}^{\infty} \left(\frac{jq^j}{1-q^j} - \frac{4jq^{4j}}{1-q^{4j}} \right)$$

   where q is a complex variable with $|q| < 1$. There are analogous results for sums of 2, 6 and 8 squares, all due to Jacobi, and there are also results for 10, 12, 14, 16 and 18 squares due to Eisenstein, Liouville and Glaisher. A general result for sums of an even number of squares was stated by Ramanujan and proved by Mordell.

   This talk will survey these results and present some extensions which are new.

7. **Rob Corless (Western Ontario, Canada)**

   Title: Bohemian Eigenvalues

   Abstract: The BOunded HEight Matrix of Integers Eigenvalue project, or "Bohemian Eigenvalue Project" for short, has its original source in the work of Peter Borwein and Loki Jörgenson on visible structures in number theory (c 1995), which did computational work on roots of polynomials of bounded height (following work of Littlewood). Some time in the late 90's I realized that because their companion matrices also had bounded height entries, such problems were equivalent to a subset of the Bohemian eigenvalue problems. That they are a proper subset follows from the Mandelbrot matrices, which have elements -1, 0 but whose characteristic polynomials have coefficients that grow doubly exponentially, in the monomial basis. There are a great many families of Bohemian eigenvalues to explore: companion matrices in other bases such as the Lagrange basis (my work here dates to 2004), general Bohemian dense matrices, circulant and Toeplitz matrices, complex symmetric matrices, and many more. The conference poster contains an image from this project. This talk presents some of our recent results. Joint work with Steven Thornton, Sonia Gupta, Jonny Brino-Tarasoff, and Venkat Balasubramanian.

8. **Brendan Cruetz (Canterbury, New Zealand)**

   Title: Arithmetic of Bielliptic Surfaces

   Abstract: A bielliptic surface over the complex numbers is a quotient of a product of elliptic curves by a finite group acting by a combination of translations and automorphisms of the elliptic curves. The study of these surfaces over number fields has played an important role in our understanding of rational points on algebraic varieties. I will review this history and then describe my recent work showing that Skorobogatov's famous bielliptic surface does indeed have a zero-cycle of degree 1, as predicted by a conjecture of Colliot-Thélène

9. **Daniel Delbourgo (Waikato, New Zealand)**

   Title: Congruences modulo p between ρ-twisted L-values

   Abstract: In his 1999 paper in Duke Math J, Vinayak Vatsal showed that there exists a canonical choice of periods for the L-function of a modular form. In joint work with Antonio Lei, we extend this result to allow twists by Artin representations, ρ, factoring through a Kummer extension F of the rationals. We also prove mod p congruences for these type of L-functions. A nice corollary is that if two semi-stable elliptic curves share the same mod p Galois representation (over F) at a good ordinary prime p, then they must have the same μ- and λ-invariants.

10. **Karl Dilcher (Dalhousie, Canada)**

    Title: On the polynomial part of a restricted partition function

    Abstract: This talk is about a topic in the wider area of partitions, which itself is an important part of additive number theory, drawing on various methods from other areas of number theory, analysis, and combinatorics.

    We prove an explicit formula for the polynomial part of a restricted partition function, also known as the first Sylvester wave. This is achieved by way of some identities for higher-order Bernoulli polynomials, one of which is analogous to Raabe's well-known multiplication formula for the ordinary Bernoulli polynomials. As a consequence of our main result we obtain an asymptotic expression for the first Sylvester wave as the coefficients of the restricted partition grow arbitrarily large. (Joint work with Christophe Vignat).

11. **Alexander Dunn (Illinois, USA)**

Title: Polynomial partition asymptotics

Abstract: Let $f \in \mathbb{Z}[y]$ be a polynomial such that $f(\mathbb{N}) \subseteq \mathbb{N}$, and let $p_{\mathcal{A}_f}(n)$ denote number of partitions of n whose parts lie in the set $\mathcal{A}_f := \{f(n) : n \in \mathbb{N}\}$. Under hypotheses on the roots of $f - f(0)$, we use the Hardy–Littlewood circle method, a polylogarithm identity, and the Matsumoto–Weng zeta function to derive asymptotic formulae for $p_{\mathcal{A}_f}(n)$ as n tends to infinity. This generalises asymptotic formulae for the number of partitions into perfect kth powers, established by Vaughan for $k = 2$, and Gafni for the case $k \geq 2$, in 2015 and 2016 respectively.

12. **Sasha Fish (Sydney, Australia)**

Title: Twisted recurrence via polynomial walks

Abstract: We will show how polynomial walks can be used to establish a twisted recurrence for sets of positive density in Z^d. In particular, we will demonstrate that if $\Gamma \leq GL_d(Z)$ is finitely generated by unipotents and acts irreducibly on R^d, then for any set $B \subset Z^d$ of positive density, there exists $k \geq 1$ such that for any $v \in kZ^d$ one can find $\gamma \in \Gamma$ with $\gamma v \in B - B$. Also we will show a non-linear analog of Bogolubov's theorem–for any set $B \subset Z^2$ of positive density, and $p(n) \in Z[n], p(0) = 0, \deg p \geq 2$ there exists $k \geq 1$ such that $kZ \subset \{x - p(y) | (x, y) \in B - B\}$. Joint work with Kamil Bulinski.

13. **Peter Forrester (Melbourne, Australia)**

Title: Volumes and distributions for random lattices

Abstract: Fundamental to random matrix theory is various factorisations of Lebesgue product measure implied by matrix change of variables. In number theory, factorisation of Siegel's invariant measure for $\mathrm{SL}_N(\mathbb{R})$ is an ingredient in Duke, Rudnik and Sarnak's asymptotic computation of the number of matrices in $\mathrm{SL}_N(\mathbb{Z})$, with a bounded norm. In this talk it will shown how factorisation of measure allows for calculations in the space of integral lattices $\mathrm{SL}_N(\mathbb{R})/\mathrm{SL}_N(\mathbb{Z})$ and generalisations such as $\mathrm{SL}_N(\mathbb{C})/\mathrm{SL}_N(\mathbb{Z}[i])$.

14. **Steven Galbraith (Auckland, New Zealand)**

Title: Open questions in elliptic curve isogenies
Abstract: I will survey new applications of elliptic curves in public key cryptography. I will discuss some computational problems related to the problem of finding an isogeny between two given elliptic curves over a finite field. The supersingular case is of particular interest, and (if there is time) I will discuss some analogous problems involving ideals in quaternion algebras.

15. **Hamish Gilmore (Waikato, New Zealand)**

Title: Computing $\mathcal{L}$-invariants for the symmetric square of an elliptic curve

Abstract: The p-adic L-function for the symmetric square of an elliptic curve E, with good ordinary reduction at $p \neq 2$, always vanishes at $s = 1$, even though the complex L-function does not. The $\mathcal{L}$-invariant relates the derivative of the p-adic L-function to the value of the complex L-function at $s = 1$ via the formula

$$\frac{d}{ds}\mathbf{L}_p(\mathrm{Sym}^2 E, s)\Big|_{s=1} = \mathcal{L}_p^{\mathrm{an}}(\mathrm{Sym}^2 E) \times (1 - \alpha_p^{-2})(1 - p\alpha_p^{-2}) \times \frac{L_\infty(\mathrm{Sym}^2 E, 1)}{(2\pi i)^{-1}\Omega_E^+\Omega_E^-}$$

where α_p is the p-adic unit root of the Hecke polynomial of E at p.

In this talk I will present a method for calculating $\mathcal{L}_p^{\mathrm{an}}(\mathrm{Sym}^2 E)$ numerically, and the results of computations for all elliptic curves E of conductor $N_E \leq 300$ with $4|N_E$, and at every ordinary prime $p \leq 13$.

This is joint work with Daniel Delbourgo.

16. **Randell Heyman (UNSW, Australia)**

Title: Pairwise coprimality of tuples
Abstract: In 200 Tóth determined the probability that k positive integers are pairwise coprime. We will review developments since then. These include tuples where designated (not all) pairs are coprime, estimating the number of pairwise coprime tuples of constrained height and generalisations to tuples in finite fields. The finite field result is joint work with Juan Arias de Reyna.

17. **Danesh Jogia (Defence, Australia)**

Title: Principal Roots of Unity in Integer Residue Rings

Abstract: Principal roots of unity are the analogue of primitive roots of unity in more general settings. They see use in computing Fourier transforms over these more general structures. In this talk I'll talk about my work independently rediscovering some work of Dubois and Venetsanopoulos from 1978 and give a simple algorithm (that I believe is not a rediscovery) for constructing principal roots of unity in integer residue rings.

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

Title: Explicit formula for Siegel series
Abstract: The Siegel-Eisenstein series over a totally real algebraic number field is one of the simplest but most important Hilbert-Siegel modular forms, and is related with various types of arithmetic theories of modular forms. It plays very important roles in the study of various types of L-functions associated with cusp forms through the pullback formula (cf. Shimura [4]). Moreover, it is closely related to arithmetic algebraic geometry (cf. Kudla [3]). In all cases, precise information on the Fourier coefficients of Siegel Eisenstein series is necessary. As is well known, the Fourier coefficient of Siegel Eisenstein series can be expressed in terms of the product of the (local) Siegel series. Thus it is very important to give an explicit form for the Siegel series. In [2], we gave an explicit formula for the Siegel series of a half-integral matrix over $\mathbb{Z}_p$ with any prime number p of any degree. It is useful for a practical computation of the Siegel series. However, it is not satisfactory in the following reasons. Firstly, the formula is complicated in the case $p = 2$, and it seems difficult to unify it with the formula in the case that p is odd as it is. Secondly, it does not seem clear what invariants determine the Siegel series. In this talk, we give an explicit formula of the Siegel series of a half-integral matrix B of any degree over any non-archimedean local field of characteristic 0 in terms of the Gross-Keating invariant of B and its related invariants defined in [1]. This is a generalization and improvement of [2]

This talk is based on a joint work with T. Ikeda.

References

[1] T. Ikeda and H. Katsurada, *On the Gross-Keating invariants of a quadratic forms over a non-archimedean local field*, To appear in Amer. J. Math. http://arxiv.org/abs/1504.07330.

[2] H. Katsurada, *An explicit formula for Siegel series*, Amer. J. Math. **121**(1999) 415–452.

[3] S. Kudla, *Central derivatives of Eisenstein series and height pairings*, Ann. of Math. **146**(1997) 545–646.

[4] G. Shimura, *Euler products and Fourier coefficients of automorphic forms on symplectic groups*, Inv. Math. **116**(1994) 531–576.

19. **Byoung Du Kim (Victoria, New Zealand)**

Title: The rational points over cyclotomic extensions of abelian varieties defined over number fields ramified at p with non-ordinary reduction at the primes above p.

Abstract: Efforts to study elliptic curves and the Galois representations attached to modular forms are often hampered by reduction types. Especially from the perspective of Iwasawa Theory, good ordinary reduction and split multiplicative reduction are comparatively easier to study, and the other reduction types (good supersingular/non-ordinary reduction, additive/potentially semistable reduction, etc.) are considered much harder.

The model that everyone wants to follow is Barry Mazur's "Rational Points of Abelian Varieties with Values in Towers of Number Fields", Inventiones math. 18, 183–266 (1972). With his work, when p is good ordinary or multiplicative, we can precisely express the relation between the characteristic ideal of the p-adic Selmer groups of elliptic curves or modular forms, and their p-adic L-functions. In particular, if the p-adic L-functions are not 0, then we know that the rational points over $\mathbb{Q}(\mu_{p^\infty})$ of elliptic curves or abelian varieties attached to newforms have a finite rank.

Various attempts have been made to crack the case of the good supersingular/non-ordinary reduction case. Time permitting, I will discuss my construction of $\pm/\pm$-Selmer groups over $\mathbb{Z}_p^2$-extensions of imaginary quadratic fields ("Signed-Selmer Groups over the $\mathbb{Z}_p^2$-extension of an Imaginary Quadratic Field", Canad. J. Math. 66(2014), 826–843), and multi-variable p-adic L-functions of elliptic curves over imaginary quadratic fields ("Two-variable p-adic L-functions of modular forms for non-ordinary primes", Journal of Number Theory Volume 144, November 2014, Pages 188–218), which were much further generalized by Loeffler, and resulted in the $\pm/\pm$-p-adic L-functions ("P-adic integration on ray class groups and non-ordinary p-adic L-functions", Proceedings of the Conference Iwasawa, 2012). But, the most important theme of this presentation is my work on the rational points of elliptic curves and abelian varieties over $\mathbb{Z}_p$-extensions of a number field when the elliptic curves or abelian varieties have good supersingular/non-ordinary reduction at p. Here, the biggest difference between my work and the predecessors' work is that I do not assume that the primes of the number field above p are unramified. First, I show a weak bound for the ranks of rational points by building up an Iwasawa Theory for non-ordinary primes, and second, I establish a stronger Iwasawa Theory for elliptic curves under certain conditions, and show a finite bound for ranks.

20. **Dong Han Kim (Dongguk, Korea)**

Title: The irrationality exponent of real numbers and the expansion in integer base

Abstract: We deduce a lower bound for the irrationality exponent of real numbers whose sequence of b-ary digits is a Sturmian sequence over $\{0, 1 \ldots, b-1\}$ and we prove that this lower bound is best possible. 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. Let r and s be multiplicatively independent positive integers. We establish that the r-ary expansion and the s-ary expansion of an irrational real number, viewed as infinite words on $\{0, 1, \ldots, r-1\}$ and $\{0, 1, \ldots, s-1\}$, respectively, cannot have simultaneously a low block complexity. In particular, they cannot be both Sturmian words. This talk is based on joint work with Yann Bugeaud.

21. **Chris King (Waikato, New Zealand)**

Title: K_1-congruences for the three-dimensional Lie groups

Abstract: In joint work with Daniel Delbourgo, we completely describe $\mathrm{K}_1(\mathbb{Z}_p[\![\mathcal{G}_\infty]\!])$ and its localisations by using an infinite family of p-adic congruences, where $\mathcal{G}_\infty$ is any solvable p-adic Lie group of dimension 3. This builds on earlier work of Kato when $\dim(\mathcal{G}_\infty) = 2$, and of Daniel Delbourgo and Lloyd Peters when $\mathcal{G}_\infty \cong \mathbb{Z}_p^\times \ltimes \mathbb{Z}_p^d$ with a scalar action of $\mathbb{Z}_p^\times$. The method exploits the classification of 3-dimensional p-adic Lie groups due to González-Sánchez and Klopsch, as well as the fundamental ideas of Kakde, Burns, etc. in non-commutative Iwasawa theory.

22. **Jingbo Liu (Hong Kong)**

Title: On a Waring's problem for integral quadratic and hermitian forms

Abstract: For each positive integer n, let $g_{\mathbb{Z}}(n)$ be the smallest integer such that if an integral quadratic form in n variables can be written as a sum of squares of integral linear forms, then it can be written as a sum of $g_{\mathbb{Z}}(n)$ squares of integral linear forms. We show that as n goes to infinity, the growth of $g_{\mathbb{Z}}(n)$ is at most an exponential of $\sqrt{n}$. Our result improves the best known upper bound on $g_{\mathbb{Z}}(n)$ which is in the order of an exponential of n. We also define an analogous number $g^*_{\mathcal{O}}(n)$ for writing hermitian forms over the ring of integers $\mathcal{O}$ of an imaginary quadratic field as sums of norms of integral linear forms, and when the class number of the imaginary quadratic field is 1, we show that the growth of $g^*_{\mathcal{O}}(n)$ is at most an exponential of $\sqrt{n}$.

This is a joint work with Constantin N. Beli, Wai Kiu Chan, Maria Ines Icaza.

23. **Maike Massierer (UNSW, Australia)**

Title: Reduction strategies for computing zeta functions of projective hypersurfaces

Abstract: The algorithm of Abbott, Kedlaya, and Roe computes the Hasse–Weil zeta function of a given projective hypersurface defined over a finite field by computing an approximation of the Frobenius action on a certain Monsky–Washnitzer cohomology space. For this purpose, it applies the (approximate) Frobenius to each element of the basis of the cohomology space. The most costly part of the algorithm is to then reduce each of these images, in order to obtain yet again a representation in terms of the basis. We explore various reduction strategies, with the goal of obtaining a more efficient algorithm for hypersurfaces defined over large finite fields. One of the key tasks is to analyse the loss of p-adic precision during the reduction. For the purposes of the talk, we will mainly concentrate on the case of $K3$ surfaces. Joint work with David Harvey.

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

Title: The Kolakoski Sequence and Some Fast Algorithms, Part 1

Abstract: The *Kolakoski sequence* $(1, 2, 2, 1, 1, 2, 1, 2, 2, 1, 2, 2, 1, 1, 2, 1, 1, 2, 2, \ldots)$ is defined recursively so that the 1's and 2's in it represent the lengths of the contiguous blocks of 1's and 2's in it. It is OEIS sequence A000002.

The sequence was defined by Oldenburger in 1939 and rediscovered by Kolakoski in 1965. Much more is conjectured about it than is known, as this talk will describe. For instance, it is conjectured that the density of 1's exists and is equal to $\frac{1}{2}$, but the best theorem to date (Rao, 2012) is that, if the density exists, it lies in the interval $(0.4999, 0.5001)$.

The sequence may be visualised as a lattice path by drawing an up-step for each '2' and a down-step for each '1'. In such a visualisation, similarities and differences with random walks become apparent.

The Kolakoski discrepancy function gives the height above the x-axis in the lattice path. It is algebraically defined as $\delta(n) := \sum_{1\leq j\leq n}(-1)^{k_j}$, where k_j is the j-th term of the Kolakoski sequence.

This is part 1 of a 2-part talk, in the second part of which Richard Brent will describe algorithms for fast computation of the Kolakoski discrepancy function.

25. **Gopal Krishna Panda (Rourkela, India)**

Title: Almost balancing-like sequences

Abstract: It is well known that the pair (n, r), where n is a balancing number and r is the corresponding balancer, is a solution of the Diophantine equation $1+2+\cdots+(n-1) = (n+1)+\cdots+(n+r)$. The sequence of balancing numbers $\{B_n\}$ satisfies the binary recurrence $B_{(n+1)} = 6B_n - B_{(n-1)}$ with initial values $B_0 = 0$ and $B_1 = 1$. It is well-known that a natural number x is a balancing number if and only if $8x^2 + 1$ is a perfect square. As generalizations of the balancing sequence, Panda and Rout studied a class of binary recurrences defined by $x_{(n+1)} = Ax_n - x_{(n-1)}, x_0 = 0, x_1 = 1$, where $A > 2$ is any natural number. They showed that these sequences enjoy many properties resembling to the corresponding properties of the balancing sequence and hence these sequences are subsequently known as balancing-like sequences. Panda and Rout proved that for a fixed natural number A, x is a balancing-like number if and only if $Dx^2 + 1$, where $D = (A^2 - 4)/4$, is a perfect rational square. In a recent paper, Panda and Panda introduced almost balancing numbers as a generalization of balancing numbers. They call a natural number n an almost balancing number if it satisfies the Diophantine equation $|1+2+\cdots+(n-1)-(n+1)+\cdots+(n+r)| = 1$ for some natural number r, which they call the almost balancer corresponding n. Thus, a natural number x is an almost balancing number if and only if $8(x^2 \pm 1)+1$ is a perfect square. If x is a natural numbers for which $8(x^2+1)+1$ is a perfect square, then x is called an A_1-balancing number while if $8(x^2 - 1) + 1$ is a perfect square, then x is called an A_2-balancing number. Since, the balancing-like numbers do not have defining equations like the balancing numbers, we define almost balancing-like numbers as follows: A natural number x an almost balancing-ike number if and only if $D(x^2 \pm 1) + 1$ is a perfect rational square. Like the case of almost balancing numbers, we call x an A_1-balancing-like number if $D(x^2+1)+1$ is a perfect rational square while if $D(x^2 - 1) + 1$ is a perfect rational square, we call x an A_2-balancing-like number. Each type of almost balancing-like numbers partition in multiple class and are realized as linear combinations of balancing-like numbers.

26. **Pooja Punyani (Delhi), India**

Title: On changes in Frobenius and Sylvester numbers.

Abstract: For any set of positive integers A with $\gcd(A) = 1$, let $\Gamma(A)$ denote the set of integers that are expressible as a linear combination of elements of A with non-negative integer coefficients. Then $\mathtt{g}(A), \mathtt{n}(A), s(A)$ denote the *largest*, the *number* of, the *sum* of positive integer(s) not in $\Gamma(A)$ respectively. We investigate the change in $\mathtt{g}(A), \mathtt{n}(A)$, and $s(A)$ when A changes from a two- element set to a three-element set. In particular, we determine these numbers for certain families $A = \{a, b, c\}$. For the same families A, we also determine the set $S^*(A)$ which consists of positive integers n not in $\Gamma(A)$ for which $n + (\Gamma(A)\backslash\{0\}) \subset \Gamma(A)\backslash\{0\}$. The largest element in $S^*(A)$ is $\mathtt{g}(A)$.

27. **Prasanta Kumar Ray (Sambalpur, India)**

Title: A Brief Remark on Balancing Wieferich Primes

Abstract: A Wieferich prime is defined as an odd prime p satisfying $2^{p-1} \equiv 1 \pmod{p^2}$. Equivalently, an odd prime p is a non-Wieferich prime if

$$2^{p-1} \not\equiv 1 \pmod{p^2}.$$

The primes 1093 and 3511 are only two Wieferich primes found till date.

A natural number n is a balancing number with balancer r if they are the solutions of the Diophantine equation $1 + 2 + \cdots + (n-1) = (n+1) + (n+2) + \cdots + (n+r)$. Balancing numbers satisfy the linear recurrence $B_{n+1} = 6B_n - B_{n-1}$ and the non-linear recurrence $B_n^2 - B_{n+1}B_{n-1} = 1$, where B_n denotes n^{th} balancing number.

Panda and Rout (2014) studied the periodicity of balancing numbers modulo any integer that help to explore some divisibility properties of balancing numbers. They also conjectured that there are three primes, 13, 31, and 1546463, satisfying $\pi(p) = \pi(p^2)$, where $\pi(m)$, $m \geq 2$, the period of the sequence of balancing number modulo t is the least positive integer m satisfying $(B_t, B_{t+1}) \equiv (0,1) \pmod{m}$. Subsequently, Rout (2016) named these numbers as balancing Wieferich primes which is analogous to the congruence

$$B_{p-\left(\frac{8}{p}\right)} \equiv 0 \pmod{p^2},$$

where $\left(\frac{8}{p}\right)$ denotes the Jacobi symbol.

In this talk, some fascinating criteria concerning balancing-Wieferich primes are explored. For instance, if $p \neq 2, w \in \mathcal{O}_p$ for which $g(w) \equiv 0 \pmod{p}$, then p is a balancing-Wieferich prime if and only if

$$w^{2q} - 6w^q + 1 \equiv 0 \pmod{p^2},$$

or equivalently,

$$g(w) + (w^q - w)g'(w) \equiv 0 \pmod{p^2}.$$

28. **Arnab Saha (ANU, Australia)**

Title: Arithmetic jet spaces of Drinfeld modules and de Rham cohomology

Abstract: The arithmetic jet space theory is developed by A. Buium as an arithmetic analogue to the differential algebra in the case of function fields. In this talk, we will talk about application of this theory in the case of Drinfeld modules. Drinfeld modules, introduced by Drinfeld himself, can be though of as analogues of the multiplicative group and the elliptic curves in the positive characteristic case. We will classify the structure of the group of differential characters of a Drinfeld module which also shows the existence of a family of interesting differential modular functions on the moduli of Drinfeld modules. But strikingly, this also leads to a finite rank F-crystal that can be canonically attached to any Drinfeld module using our arithmetic jet space theory. This F-crystal has a 'Hodge-type' filtration as well and also maps to the original Hodge sequence preserving the filtration but is intrinsically different from the crystalline cohomology module of a Drinfeld module.This is joint work with Jim Borger.

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

Title: Abelian multiplicatively dependent points on curves

Abstract: In this talk, I will present some recent work about the structure of abelian multiplicatively dependent points on curves (whose coordinates are from the abelian closure and are multiplicatively dependent). For example, under some natural condition, the set of abelian multiplicatively dependent points on an irreducible curve over a number field is a finite union of preimages of roots of unity by a finite set of morphisms, and a finite set. This is joint work with Alina Ostafe, Igor Shparlinski and Umberto Zannier.

30. **Nicole Sutherland (Sydney, Australia)**

Title: Further computations with Galois groups

Abstract: Algorithms to compute Galois groups of irreducible polynomials over the rational field have been available in some way for some time. These algorithms have been extended to polynomials of larger degrees and also polynomials over other coefficient rings. Currently the widest ranging algorithm is that of Fieker and Klüners which has no degree restriction on input polynomials and has been adapted for use with reducible as well as irreducible polynomials over algebraic number fields, rational function fields of all characteristics and global algebraic function fields.

In this talk I will briefly summarise this algorithm and discuss how we can do further computations with Galois groups using the information we have from the initial computation.

31. **Tim Trudgian (UNSW, Australia)**

Title: A souped up Ford

Abstract: In the absence of the Riemann hypothesis one has to make do with zero-free regions of the Riemann zeta-function. The Korobov–Vinogradov region was proved in 1957 and is still the strongest asymptotic result known. An explicit version of this region was provided by Ford in 2002. With a better choice of parameters one can improve Ford's result. This is joint work with Mike Mossinghoff.

32. **Cindy Tsang (Tsinghua, China)**

Title: Galois module structure of rings of integers and the Hilbert-Speiser theorem

Abstract: A Galois extension L/K of number fields with group G is said to have a normal integral basis if the ring of integers O_L in L admits a basis B over the ring of integers O_K in K such that elements in B are permuted by the action of G.The celebrated theorem of Hilbert and Speiser states that every tame and abelian extension L/K admits a normal integral basis when $K = \mathbb{Q}$, while a result of Greither et al. states that $\mathbb{Q}$ is the only number field satisfying this property. I am interested in two possible refinements of this result, one of which takes the self-duality of O_L as an O_KG-module into account and the other regards O_L as a module over the maximal O_K-order in KG. In this talk, I will give an overview of what has been done in the literature related to the Hilbert-Speiser theorem/result of Greither et al, and then explain the two refinements as well as state some new results about them.

33. **Lee Zhao (UNSW, Australia)**

Title: Elliptic Curves in Isogeny Classes.

Abstract: We show that the distribution of elliptic curves in isogeny classes of curves with a given value of the Frobenius trace t becomes close to uniform even when t is averaged over very short intervals inside the Hasse-Weil interval. This is joint work with I. E. Shparlinski.