Strength in Numbers

A Graduate Workshop in Number Theory and Related Areas

Queen's University, Kingston, Canada

May 11-12, 2018

Abstracts for Short Talks

- **Abdullah Al-Shaghay**, Dalhousie University
  Title: Irreducibility and Roots of a Class of Polynomials
  Abstract: In a 2012 paper, J. Harrington investigated the factorization properties of polynomials of the form

$$f(x) = x^n + cx^{n-1} + cx^{n-2} + \ldots + cx + c \in \mathbb{Z}[x].$$

  In particular, it was asked:

  1. For what positive integers n and nonzero integers c is $f(x)$ irreducible?
  2. If $f(x)$ is reducible, then how does it factor?

  We will discuss the results of Harrington's paper and talk about the idea of considering "Harrington polynomials with a gap size of a" for positive integers a:

$$g(x) = x^n + cx^{n-a} + cx^{n-a-1} + cx^{n-a-2} + \ldots + cx + c \in \mathbb{Z}[x].$$

- **Emilia Alvarez**, Concordia University
  Title: Introduction to Random Matrix Theory in Number Theory
  Abstract: In this short talk we'll introduce the relationship between random matrix theory and number theory, in particular how the statistics of families of L-functions have been "paired" to statistics of random matrix ensembles through symmetries. We'll describe the three main circular ensembles used in number theory (unitary, orthogonal and symplectic), discussing their measure, and if time permits, state their correlation and cluster functions.

- **Beatrice Chetard**, University of Western Ontario
  Title: Graded character rings
  Abstract: The characters (say, over the complex numbers) of a group G form a ring $R(G)$. Exterior powers of representations induce a filtration on this ring, defined by Grothendieck. Can we compute the associated graded ring? What information about the group does it remember?

- **Anup Dixit**, University of Toronto
  Title: On the universality of certain L-functions
  Abstract: In 1975, Voronin proved a remarkable result on the value distribution of the Riemann zeta-function $\zeta(s)$, which states that every non-vanishing holomorphic function in the critical strip is approximated infinitely often by vertical shifts of the $\zeta(s)$. This is called the universality property of the Riemann zeta-function. Ever since, the universality property has been established for many known L-functions, such as all L-functions in the Selberg class. It is also known that L-functions outside the Selberg class, such as the Hurwitz zeta-function and the Lerch zeta-function are universal. This led Linnik and Ibragimov to conjecture that every Dirichlet series with an analytic continuation satisfying some growth conditions should be universal. In this talk, we formulate this conjecture more precisely and prove some results that give evidence towards it.

- **Brandon Gill**, University of Saskatchewan
  Title: Bounded primes for hypergeometric series
  Abstract: A power series with rational coefficients is said to be bounded at a rational prime p if its coefficients are bounded in the p-adic topology. The question of when a hypergeometric series with rational parameters is bounded at a prime p was studied by Dwork and Christol in the 1970s and 1980s. In 2017, Franc-Gannon-Mason showed that the set of bounded primes for a fixed hypergeometric series has a Dirichlet density. Recently, in joint work with Franc-Goertzen-Pas-Tu, we found an efficient formula for computing this density, and we have used this formula to explore the generic global behaviour of the density of bounded primes for hypergeometric series. Unsurprisingly, the density of bounded primes appears to be quite small in general. In line with this we have established an upper bound on the density of bounded primes for certain specialisations of hypergeometric parameters. In this talk we will report on these results.

- **Seoyoung Kim**, Brown University
  Title: The Sato-Tate conjecture and Nagao's conjecture
  Abstract: Nagao's conjecture relates the rank of an elliptic surface to a limit formula arising from a weighted average of fibral Frobenius traces, and it is further generalized for smooth irreducible projective surfaces by M. Hindry and A. Pacheco. We show that the Sato-Tate conjecture based on the random matrix model implies Nagao's conjecture for certain twist families of elliptic curves and hyperelliptic curves.

- **Kim Klinger-Logan**, University of Minnesota
  Title: Differential Equations in Automorphic Forms
  Abstract: Physicists such as Green, Vanhove, et al show that differential equations involving automorphic forms govern the behavior of gravitons. One particular point of interest is solutions to $(\Delta - \lambda)u = E_\alpha E_\beta$ on an arithmetic quotient of the exceptional group E_8. We use spectral theory solve $(\Delta - \lambda)u = E_\alpha E_\beta$ on the domain. The construction of such a solution uses Arthur truncation, the Maass-Selberg formula, and automorphic Sobolev spaces.

- **Andrew Kobin**, University of Virginia
  Title: Understanding Artin-Schreier covers of stacks
  Abstract: In their paper "The canonical ring of a stacky curve", Voight and Zureick-Brown give a combinatorial description of the canonical ring of a tame stacky curve (similar to the notion of an orbifold curve) using the root stack construction, which encodes Kummer theory in the language of stacks. To allow wild ramification, one must replace root stacks with something analogous in characteristic $p > 0$. In this talk, I introduce such a construction, called a "universal Artin-Schreier stack", and suggest how it may be used to describe wild stacky curves in the $\mathbb{Z}/p\mathbb{Z}$ case.

- **Debanjana Kundu**, University of Toronto
  Title: On the $\mu = 0$ Conjecture for the Split Prime $\mathbb{Z}_p$-Extensions
  Abstract: Let F be a number field and F_∞/F be its cyclotomic $\mathbb{Z}_p$ extension. Iwasawa conjectured that in this setting the μ-invariant is 0. This was proven by Ferrero-Washington for all abelian extensions of $\mathbb{Q}$. When F_∞ is NOT the cyclotomic extension, Iwasawa gave examples where $\mu > 0$.

  In a recent project with Prof Coates, we were interested in the *split prime* $\mathbb{Z}_p$-extension; when F is an imaginary quadratic field and p is a rational prime that splits in F, $p = \mathfrak{p}\overline{\mathfrak{p}}$, the unique $\mathbb{Z}_p$ extension unramified outside $\mathfrak{p}$ is called the split prime $\mathbb{Z}_p$ extension.

  The split prime $\mathbb{Z}_p$-extension is believed to be similar to the cyclotomic $\mathbb{Z}_p$-extension in may ways. In particular, we study an analogue of the $\mu = 0$ conjecture. This is joint work with Anwesh Ray.

- **Somnath Kundu**, Ryerson University
  Title: Network Bargaining Games : A Fairness Approach
  Abstract: This work uses many different aspects of discrete mathematics, such as Elements of Graph Theory, Mathematical Optimization, Duality Theory, Complementary Slackness Condition, Integrality Gap, Cutting Planes, Bargaining Game, Outside Options, Notion of Fairness and Equilibrium, Cooperative Games, Core of Cooperative Games, etc.

  Say, in a village settings there are many farmers. But one person can't produce the crops by themselves. They need to team up with another person to run the agricultural machinery to generate different crops. The cost of buying and operating that machines must be shared by the participating farmers. Each farmer needs certain amount of foods to sustain that need to be fulfilled.

  These problems can be seen from many different angles. One is from the System perspective. From the above example, we can say the village council should make sure that no one in that village should get less food than they need. And the overall cost of the total crop production is minimum. This is a mathematical optimization problem. Where the feasible solution is, that each agent has fulfilled at least the amount they need. And the overall cost of the problem is minimum. Mathematically it is difficult to find an integer (whole) solution to this problem. But we can relax the constraints problem a little bit and try to get closer to the solution using other external constraints. There are various mathematical techniques that can be adopted like cutting planes to come closer to the actual solution.

  Another angle is from the perspective of an individual, where every agent would try to minimize his/her cost. They will look for different options among the people around them. And try to choose those which enables them to spend least cost for fulfilling their individual need. Mathematically this can be categorized under the domain of bargaining game theory.

  Another interesting angle is from the idea of group co-operation. Agents can choose to be part of the grand coalition or they can form a subgroup within the coalition to minimize their cost. For the above mentioned example the analogy could be that villagers could decide whether they will be a part of the whole village or form their own internal sub-group to minimize their cost. These approach can be categorized under the domain of cooperative game theory.

  The most intriguing part of this story is that when we apply some simple notion of fairness concept in it, every analysis merge to a single point, That means what the village council thinks, is best for them, will exactly match to the solution where every individual thinks, is the best solution for them. Means that if we work out the optimum solution individually for these three problems (optimization problem, bargaining problem and cooperative problem), the solutions in each cases will be exactly same, if we force the fairness constraint to each of them.

  Three seemingly different uncorrelated perspectives; but they all come together with the idea of fairness and a bit of magic of math. It can be proved that people can be selfish, and they can only favor their friends (nepotism), but still in larger perspective they will end up doing a greater good for the society as whole only if we just employ some very simple rule of Fairness.

- **Allysa Lumley**, York University
Title: Distribution of Values of L-functions associated to Hyperelliptic Curves over Finite Fields
Abstract: In 1992, Hoffstein and Rosen proved a function field analogue to Gauß' conjecture regarding the class number, h_D, of a discriminant D by averaging over all polynomials with a fixed degree. In this case $h_D = |\mathrm{Pic}(\mathcal{O}_D)|$, where $\mathrm{Pic}(\mathcal{O}_D)$ is the Picard group of $\mathcal{O}_D$. Andrade later considered the average value of h_D, where D is monic, squarefree and its degree varies. He achieved these results by calculating the first moment of $L(1, \chi_D)$ in combination with Artin's formula relating $L(1, \chi_D)$ and h_D. For this talk we discuss the complex moments of $L(1, \chi_D)$. We show that these moments are very nearly equal to those of a random probabilistic model. We also describe the distribution of values for both $L(1, \chi_D)$ and h_D.

- **Kamalakshya Mahatab**, Norwegian University of Science and Technology
Title: Large Values of Riemann Zeta Function and Dirichlet L-Functions
Abstract: Let $\zeta(s)$ be the Riemann Zeta function and let $L(s, \chi)$ be the Dirichelt L-function associated to a character χ modulo q. Let $\log_k$ stands for k iterated logarithms with base e. In this talk we shall briefly discuss the following three results:

  (A) Let $\mathfrak{m}$ denote the Lebesgue measure on $\mathbb{R}$. Then for all sufficiently large T,
  $$\mathfrak{m}\Big(t \in [0, T] : |\zeta(1 + it)| \geq e^{\gamma}(\log_2 T + \log_3 T) - H - \delta\Big) \geq T^{1-e^{-\delta}+o(1)},$$
  where $\delta > 0$ and $H = 1 + \log_2 4$.

  (B) Let H be the constant as in (A). Then for $\delta > 0$ and for large enough q,
  $$\Big|\{\chi \bmod q : |L(1, \chi)| \geq e^{\gamma}(\log_2 q + \log_3 q) - H - \delta\}\Big| \geq q^{1-e^{-\delta}+o(1)}.$$

  (C) Let $1/2 < \sigma < 1$ and $a(\sigma) = \frac{2\sigma-1}{2-\sigma}$. Then there exists a constant $\mathfrak{C}(\sigma)$ such that for all sufficiently large q and $\delta > 0$,
  $$\Big|\{\chi \bmod q : \log|L(\sigma, \chi)| \geq \mathfrak{C}(\sigma)(1 - \delta)(\log q)^{1-\sigma}(\log_2 q)^{-\sigma}\}\Big| \geq q^{1-a(\sigma)(1-\delta)+o(1)}.$$

  The results in (A) and (B) are improvements of some results of Granville and Soundararajan. The result in (C) is similar to a result obtained by Lamzouri under Generalized Riemann Hypothesis. The above results are from two different papers jointly written with Christoph Aistleitner, Marc Munsch and Alexandre Peyrot.

- **Caroline Matson**, University of Colorado at Boulder
Title: Higher dimensional formal groups
Abstract: A formal group is a power series that can be seen as specifying a group law "without points." To any elliptic curve we can associate a formal group that gives its group law at the identity, which can be a powerful tool for studying the algebraic structure of the curve, particularly over local fields. In this talk we will see some important properties of formal groups and will look at how they generalize to higher dimensional abelian varieties.

- **Patrick Milano**, Binghamton University
  Title: Long exact sequences in arithmetic cohomology
  Abstract: In 1998, Borisov introduced a cohomology theory for Arakelov divisors on number fields. Given an Arakelov divisor D, he defined $H^0(D)$ and $H^1(D)$ as new kinds of objects called ghost spaces. In this talk, we will further develop the theory of ghost spaces and show how they can be used to construct long exact sequences in Borisov's cohomology.

- **David Nguyen**, UC Santa Barbara
  Title: Breaking the square root barrier
  Abstract: The square root barrier is the essential obstacle preventing one from proving that gaps between primes are bounded. As you probably know, this obstruction was overcome recently. In this talk, I will survey the main ideas used and apply them to obtain equidistribution estimates for the generalized divisor functions to large moduli. This is joint work with Y. Zhang.

- **Andre Oliveira**, Wesleyan University
  Title: Continued Fractions and Geodesics on the Modular Surface
  Abstract: This expository talk will take a look at an example of the interplay between Homogeneous Dynamics and Number Theory. We will focus on C. Series' results which showcase a remarkable connection between continued fractions and geodesics on the modular surface. In particular, these results provide a coding that establishes a dictionary between continued fractions and cutting sequences for the Farey tessellation. This dictionary also transports Diophantine properties of a number (e.g. how bad/well approximable it is) to geometric properties of an associated trajectory (e.g. how far into a cusp it travels).

- **Abhishek Oswal**, University of Toronto
  Title: Curves over $\mathbb{Q}_p$ with torsion points of high order in their Jacobians
  Abstract: Recent work of M. Stoll and its generalization by Katz, Rabinoff and Zureick-Brown, prove the existence of a *uniform* bound on the number of $\mathbb{Q}_p$-points on a smooth curve/$\mathbb{Q}_p$ of a fixed genus $g \geq 3$ that lie in a finite-rank subgroup of the Jacobian (provided the rank of the subgroup is at most $g-3$). In particular, when $g \geq 3$, the number of $\mathbb{Q}_p$-rational points in a torsion packet on such genus g curves is uniformly bounded. In this talk, we give an overview of these results and explore the question of bounding the *order* of these torsion points.

- **Gaurav Patil**, University of Toronto
  Title: On an approach to the inverse Galois problem
  Abstract: For a finite group G and a field K, the classical inverse Galois problem is concerned with finding a Galois extension L/K such that its Galois group is G. In this talk, we will discuss an approach to this problem by studying compositions of polynomials. We will provide some results toward certain conjectures on the dynatomic polynomials. Further studying their structure sheds light on the polynomials whose splitting field has Galois group G over the base field.

- **Wayne Peng**, University of Rochester
  Title: When can two arboreal representations be isomorphic?
  Abstract: Let K be a number field. Let f and g be polynomials of degree greater than one over K, let a and b two elements of K, and let $\mathbb{T}_f(a)$ and $\mathbb{T}g(b)$ be the rooted tree of inverse images of a and b under iteration of f and g. We present a conjecture on when $\mathbb{T}_f(a)$ and $\mathbb{T}_g(b)$ can be Galois isomorphic. This may be seen as a dynamical analog of the Tate isogeny theorem. This is join work with Tom Tucker.

- **Amy Beth Prager**, recent MIT Alumna
  Title: Why Do They Come – Why Do They Stay? Career Motivations Among Technical Undergraduate Students
  Abstract: In this presentation I will discuss an empirical study examining the reasons why undergraduate female students select and remain computer science majors at Carnegie Mellon University. At the end we will explore together ways to increase the diversity and inclusivity of people entering the technology sector. My presentation can be found here:
  https://www.dropbox.com/s/hffqwk6gfyhfhld/
  WhyDoTheyCome_WhyDoTheyStay.pdf?dl=0.

- **François Séguin**, Queen's University
  Title: The two-variable Artin conjecture
  Abstract: In 2000, P. Moree and P. Stevenhagen formulated and gave a conditional proof to a variation of Artin's conjecture on primitive roots. During this talk, we will present new unconditional results towards two-variable Artin conjecture. We will also present analogues to the conjecture in other contexts.

- **Divyum Sharma**, Waterloo University
  Title: Joint distribution of the base-q and Ostrowski digital sums
  Abstract: In 1922, A. Ostrowski introduced a numeration system based on the denominators of the convergents in the continued fraction expansion of a fixed irrational number α. Coquet, Rhin and Toffin studied the joint distribution in residue classes of the base-q sum-of-digits function S_q and the Ostrowski sum-of-digits function S_α. They gave certain sufficient conditions for the set

$$\{n \in \mathbb{N} : S_q(n) \equiv a_1 \pmod{m_1},\ S_\alpha(n) \equiv a_2 \pmod{m_2}\}$$

  to have asymptotic density $1/m_1m_2$. In this talk, we present a quantitative version of their result when

$$\alpha = [0; \overline{1, m}],\ m \geq 2.$$

- **Hanson Smith**, University of Colorado Boulder
  Title: Monogenic S_4 Quartic Fields Arising from Elliptic Curves
  Abstract: Given a number field, one can find a basis for the ring of integers. Different monic, integral, irreducible polynomials yielding the same number field will yield different bases. A particularly nice basis, aesthetically and computationally, is a power basis consisting of 1 and powers of a root of a defining polynomial for the number field. Number fields admitting such bases are called *monogenic*. The problem of categorizing such number fields is called *Hasse's Problem* after its proponent Helmut Hasse.

  In this talk, we will outline recent work classifying a family of monogenic partial torsion fields. In other words, monogenic fields generated by a root of a division polynomial of an elliptic curve. We will discuss the main ingredients that enable us to classify these monogenic partial torsion fields and give some intuition for how these ingredients come together. If time allows, we will cover some further questions that are being pursued. This is joint work with Katherine Stange and Alden Gassert.

- **Asmita Sodhi**, Dalhousie University
  Title: Integer-Valued Polynomials and a Game Called p-ordering
  Abstract: In this talk we will visit the world of integer-valued polynomials, and also introduce the ring of polynomials that are integer-valued over a subset of $\mathbb{Z}$. We will explore Bhargava's "game called p-ordering", and see how p-orderings and p-sequences allow us to find a $\mathbb{Z}$-module basis for the ring of integer-valued polynomials for a subset of the integers. Finally, we will briefly see how Bhargava's tools may be extended to the noncommutative case of integer-valued polynomials over the ring $M_n(\mathbb{Z})$ of $n \times n$ integer matrices.

- **Hayley Tomkins**, University of Ottawa
  Title: Constructing Generators of Free Subgroups of $\mathrm{PGL}_2(\mathbb{F}_p((x)))$
  Abstract: In this talk we introduce a novel approach to constructing cryptographic hash functions using free subgroups of $\mathrm{PGL}_2(\mathbb{F})$, where $\mathbb{F}$ is the function field $\mathbb{F}_p((x))$. We present a new theorem which significantly extends Zémor and Tillich's original work by providing a general method for producing alternative generators. We then build the intuition behind this theorem, drawing on Tits's "Ping Pong Lemma" as well as the ideas of Breuillard and Gelander. Along the way, we will introduce and explore some pleasing properties of a metric on the projective space of dimension 1 over $\mathbb{F}_p((x))$.

- **Siddhesh Wagh**, University of Oklahoma
  Title: Maass space for liftings from $\mathrm{SL}(2,\mathbb{R})$ to $\mathrm{GL}(2,B)$ over a division quaternion algebra
  Abstract: Muto, Narita and Pitale created Saito-Kurokawa like lifts from $\mathrm{SL}(2,\mathbb{R})$ to $\mathrm{GL}(2,B)$ for a definite division quaternion algebra B. My talk is about the identification of Maass space for this construction. The methods used by Maass cannot be applied here and hence we will tackle the problem via a representation theory approach.

- **Jiuya Wang**, University of Wisconsin-Madison
  Title: Malle's conjecture for compositum of number fields
  Abstract: Malle's conjecture is a conjecture on the asymptotic distribution of number fields with bounded discriminant. We propose a general framework to prove Malle's conjecture for compositum of number fields based on known examples of Malle's conjecture and good uniformity estimates. By this method, we prove Malle's conjecture for $S_n \times A$ number fields for $n = 3, 4, 5$ and A in an infinite family of abelian groups. As a corollary, we show that Malle's conjecture is true for $C_3 \wr C_2$ in its S_9 representation, whereas its S_6 representation is the first counter example of Malle's conjecture given by Klüners.

- **Matthew Welsh**, Rutgers University
  Title: Parametrization, Approximation, and Spacing of Roots of Cubic Congruences
  Abstract: Roots of quadratic congruences, for example ν such that $\nu^2 = -1 \pmod m$, can be parametrized using binary quadratic forms, those with discriminant -4 for the example. By an LU decomposition, this parametrization leads to an approximation of $\frac{\nu}{m}$, to error $\ll \frac{1}{m}$, by a fraction with denominator of size $\asymp m^{1/2}$. This in turn shows that those roots with $m \leq M$ are typically spaced by at least $\gg \frac{1}{M}$, a fact central to Fouvry and Iwaniec's proof that there are infinitely many primes of the form $x^2 + p^2$.

  In this talk we will discuss similar parametrization, approximation, and spacing results for roots of cubic congruences, focusing on $\nu^3 = 2 \pmod m$. A main result is that inside any disc in $\mathbb{R}^2/\mathbb{Z}^2$ of radius $\frac{1}{M}$, there are $\ll 1$ points $\left(\frac{\nu}{m}, \frac{\nu^2}{m}\right) \pmod 1$ with $\nu^3 = 2 \pmod m$ and $M < m \leq 2M$.