PAST SPEAKERS IN THE

NUMBER THEORY AND COMBINATORICS SEMINAR

OF THE DEPARTMENT OF MATHEMATICS & COMPUTER SCIENCE AT THE

UNIVERSITY OF LETHBRIDGE

http://www.cs.uleth.ca/~nathanng/ntcoseminar/

Organizers:

Nathan Ng and Dave Witte Morris (starting Fall 2011)

Amir Akbary (Fall 2007 – Fall 2010)

Contents

Spring 2020

Open problem session Jan 13, 2020

Please bring your favourite (math) problems. Anyone with a problem to share will be given about 5 minutes to present it. We will also choose most of the speakers for the rest of the semester.

Joy Morris (University of Lethbridge) Jan 20, 2020
Regular Representations of Groups

A natural way to understand groups visually is by examining objects on which the group has a natural permutation action. In fact, this is often the way we first show groups to undergraduate students: introducing the cyclic and dihedral groups as the groups of symmetries of polygons, logos, or designs. For example, the dihedral group D_8 of order 8 is the group of symmetries of a square. However, there are some challenges with this particular example of visualisation, as many people struggle to understand how reflections and rotations interact as symmetries of a square.

Every group G admits a natural permutation action on the set of elements of G (in fact, two): acting by right- (or left-) multiplication. (The action by right-multiplication is given by $\{\tau_g : g \in G\}$, where $\tau_g(h) = hg$ for every $h \in G$.) This action is called the *right- (or left-) regular representation* of G. It is straightforward to observe that this action is regular (that is, for any two elements of the underlying set, there is precisely one group element that maps one to the other). If it is possible to find an object that can be labelled with the elements of G in such a way that the symmetries of the object are precisely the right-regular representation of G, then we call this object a *regular representation* of G.

A Cayley (di)graph $\mathrm{Cay}(G, S)$ on the group G (with connection set $S \subset G$) is defined to have the set G as its vertices, with an arc from g to sg for every $s \in S$. It is straightforward to see that the right-regular representation of G is a subset of the automorphism group of this (di)graph. However, it is often not at all obvious whether or not $\mathrm{Cay}(G, S)$ admits additional automorphisms. For example, $\mathrm{Cay}(\mathbb{Z}_4, \{1, 3\})$ is a square, and therefore has D_8 rather than $\mathbb{Z}_4$ as its full automorphism group, so is not a regular representation of $\mathbb{Z}_4$. Nonetheless, since a regular representation that is a (di)graph must always be a Cayley (di)graph, we study these to determine when regular representations of groups are possible.

I will present results about which groups admit graphs, digraphs, and oriented graphs as regular representations, and how common it is for an arbitrary Cayley digraph to be a regular representation.

Habiba Kadiri (University of Lethbridge) Jan 27, 2020
Explicit results about primes in Chebotarev's density theorem

Let L/K be a Galois extension of number fields with Galois group G, and let $C \subset G$ be a conjugacy class. Attached to each unramified prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ is the Artin symbol $\sigma_{\mathfrak{p}}$, a conjugacy class in G. In 1922 Chebotarev established what is referred to his density theorem (CDT). It asserts that the number $\pi_C(x)$of such primes with $\sigma_{\mathfrak{p}} = C$ and norm $N_{\mathfrak{p}} \leq x$ is asymptotically $\frac{|C|}{|G|}Li(x)$ as $x \to \infty$, where $Li(x)$ is the usual logarithmic integral. As such, CDT is a generalisation of both the prime number theorem and Dirichlet's theorem on primes in arithmetic progressions. In light of Linnik's result on the least prime in an arithmetic progression, one may ask for a bound for the least prime ideal whose Artin symbol equals C. In 1977 Lagarias and Odlyzko proved explicit versions of CDT and in 1979 Lagarias, Montgomery and Odlyzko gave bounds for the least prime ideal in the CDT. Since 2012 several unconditional explicit results of these theorems have appeared with contributions by Zaman, Zaman and Thorner, Ahn and Kwon, and Winckler. I will present several recent results we have proven with Das, Ng, and Wong.

Selcuk Aygin (University of Lethbridge) Feb 3, 2020
On the eta quotients whose derivatives are also eta quotients

In classical q-series studies there are examples of eta quotients whose derivatives are also eta quotients. The most famous examples can be found in works of S. Ramanujan and N. Fine. In 2019, in a joint work with P. C. Toh, we have given 203 pairs of such eta quotients, which we believe to be the complete list (see "When is the derivative of an eta quotient another eta quotient?", J. Math. Anal. Appl. 480 (2019) 123366). Recently, D. Choi, B. Kim and S. Lim have given a complete list of such eta quotients with squarefree levels (see "Pairs of eta-quotients with dual weights and their applications", Adv. Math. 355 (2019) 106779). Their findings support the idea that our list is complete.

In this talk we introduce a beautiful interplay between eta quotients, their derivatives and Eisenstein series. Then we share our work in progress (joint with A. Akbary) in proving the completeness of our list beyond squarefree levels.

Amir Akbary (University of Lethbridge) Feb 10, 2020
Reciprocity Laws

The Artin reciprocity law provides a solution to Hilbert's ninth problem (9. Proof of the Most General Law of Reciprocity in any Number Field). In this talk we provide an exposition of this theorem with emphasis on its relation with the classical law of quadratic reciprocity and describe its motivating role in the far reaching Langlands Reciprocity Conjecture.

Peng-Jie Wong (University of Lethbridge) Feb 24, 2020
Cyclicity of CM Elliptic Curves Modulo p

Let E be a CM elliptic curve defined over $\mathbb{Q}$. In light of the Lang-Trotter conjecture, there is a question asking for an asymptotic formula for the number of primes $p \leq x$ for which the reduction modulo p of E is cyclic. This has been studied by Akbary, Cojocaru, Gupta, M.R. Murty, V.K. Murty, and Serre. In this talk, we will discuss their work and some variants of the question.

Nathan Ng (University of Lethbridge) Mar 2, 2020
Moments of the Riemann zeta function and mean values of long Dirichlet polynomials

The $2k$-th moments $I_k(T)$ of the Riemann zeta function have been studied extensively. In the late 90's, Keating-Snaith gave a conjecture for the size of $I_k(T)$. At the same time Conrey-Gonek connected $I_k(T)$ to mean values of long Dirichlet polynomials with divisor coefficients. Recently this has been further developed by Conrey-Keating in a series of 5 articles. I will discuss my work relating $I_3(T)$ to smooth shifted ternary additive divisor sums and also recent joint work with Alia Hamieh on mean values of long Dirichlet polynomials with higher divisor coefficients.

Nathan Ng (University of Lethbridge) Mar 9, 2020
The size of prime number error terms

Montgomery made a conjecture for the size of the error term in the prime number theorem. Similarly, Gonek made a conjecture for the size of the error term for the summatory function of the Mobius function. I will discuss these conjectures and the connection to large deviations of infinite sums of identically distributed random variables. This is joint work with Amir Akbary and Majid Shahabi.

Daniel Fiorilli (University of Ottawa and University of Paris – Saclay) May 20, 2020
On the distribution of the error term in Chebotarev's density theorem and applications

We will discuss both extreme and generic values of the error term in Chebotarev's density theorem. This will allow us to deduce applications on a conjecture of K. Murty on the least unramified prime ideal in a given Frobenius set as well as on asymptotic properties of Chebyshev's bias. This is joint work with Florent Jouve, and builds on ideas of Rubinstein-Sarnak, Ng, K. Murty, R. Murty, and others.

Olivier Ramaré (Institut de Mathématiques de Marseille) May 25, 2020
Explicit Average Orders: News & Problems

We mix some of the novelties that have occurred recently in the field of explicit multiplicative number theory, together with some questions that have not been answered yet and with several new results.

Forrest Francis (UNSW Canberra, Australia) June 8, 2020
Explicit Improvements to the Burgess Bound

The standard estimate for the size of a (Dirichlet) character sum is the well-known Pólya-Vinogradov inequality. However, this inequality only uses the modulus of the character and does not consider the length of the sum. For a bound that does consider the length of the sum, we have a family of estimates known as the Burgess bound. Owing to the size of their effective ranges, the Burgess bound is sometimes considered a "better" estimate.

Despite this, in an explicit setting, some improvements to the Pólya-Vinogradov inequality end up yielding improvements to the Burgess bound. In this talk, we will look at two such results. One involves the leading constant for the Burgess bound for characters of prime modulus, while the other makes improvements to the effective range of the Burgess bound for odd quadratic characters. The second topic is joint work with Matteo Bordignon.

Ethan Lee (UNSW Canberra, Australia) June 15, 2020
Goldbach's Conjecture and Square-free Numbers

We introduce the Goldbach conjecture and some heuristic evidence to support it. Goldbach's conjecture is hard, so we consider some relaxations of Goldbach's conjecture, which has lead to theorems by Helfgott and Dudek. Then, I give an account of the results and the main method used in joint work with F. Francis (submitted), which builds upon Dudek's result. Finally, we observe some conjectures, which would build upon the aforementioned results from myself and F. Francis.

Asif Zaman (University of Toronto) June 22, 2020
An effective Chebotarev density theorem for fibres

Let K/k be a Galois extension of number fields. The Chebotarev density theorem asserts that, as x tends to infinity, the primes of k with norm at most x equidistribute according to their splitting behaviour in K. How large must x be to actually observe this equidistribution? Pierce, Turnage-Butterbaugh, and Wood have made remarkable progress on this central question for certain families of number fields. Their results rely on two key ingredients: (1) the Artin conjecture is known for every field in the family and (2) there are few common intermediate field extensions within the family. Dependence on (1) was removed in recent joint work with Thorner.

I will discuss forthcoming work with Lemke Oliver and Thorner where we prove an unconditional result that allows both (1) and (2) to be bypassed in many cases of interest. For example, we prove that almost all degree n S_n-extensions have GRH-quality bounds on the ℓ-torsion subgroups of their class groups.

Shabnam Akhtari (University of Oregon) June 29, 2020
How to count (cubic and quartic) binary forms

In order to study interesting arithmetic, algebraic, analytic and geometric properties of binary forms, we often need a way to order them. I will discuss some natural ways to order binary forms $F(x, y)$ with integer coefficients, especially those of degree 3 and 4. I will show some of my recent works as examples of the importance of understanding the invariant theory of integral binary forms in order to count these important arithmetic objects.

Fall 2019

Open problem session Sept 9, 2018

Please bring your favourite (math) problems. Anyone with a problem to share will be given about 5 minutes to present it. We will also choose most of the speakers for the rest of the semester.

Gabriel Verret (University of Auckland, New Zealand) Sept 16, 2019
An update on the Polycirculant Conjecture

One version of the Polycirculant Conjecture is that every finite vertex-transitive digraph admits a non-trivial semiregular automorphism. I will give an overview of the status of this conjecture, as well as describe some recent progress with Michael Giudici, Ademir Hujdurovic and Istvan Kovacs.

Selcuk Aygin (Math and CS, U of Lethbridge) Sept 23, 2019
Extensions of Ramanujan-Mordell Formula with Coefficients 1 *and* p

We use properties of modular forms to extend the Ramanujan-Mordell formula. Our result yields formulas for representation numbers by the quadratic form $\sum_{i=1}^{2a} x_i^2 + \sum_{i=1}^{2b} py_i^2$, for all non-negative integers a, b and for all odd prime p. We obtain this result by computing the Fourier series expansions of modular forms at all cusps of $\Gamma_0(4p)$.

Amir Akbary (Math and CS, U of Lethbridge) Oct 7, 2019
The prime number theorem for automorphic L*-functions*

We describe a theorem due to Jianya Liu and Yangbo Ye (Pure and Applied Mathematics Quarterly, Volume 3, Number 2, 481–497, 2007) concerning the prime number theorem for automorphic L-functions. We state the theorem and review the strategy of the proof in comparison with the classical prime number theorem. An important ingredient is a new version of Perron's formula that represents a sum of complex numbers as a contour integral plus some specific error terms.

Khoa Dang Nguyen (University of Calgary) Oct 21, 2019
An analogue of Ruzsa's conjecture for polynomials over finite fields

In 1971, Ruzsa conjectured that if $f : \mathbb{N} \to \mathbb{Z}$ with $f(n+k) \equiv f(n) \bmod k$ for every $n, k \in \mathbb{N}$ and $f(n) = O(\theta^n)$ with $\theta < e$ then f is a polynomial. In this paper, we investigate the analogous problem for the ring of polynomials over a finite field. This is joint work with Jason Bell.

Quanli Shen (Math and CS, U of Lethbridge) Oct 28, 2019
The fourth moment of quadratic Dirichlet L-functions

In this talk, I will talk about the fourth moment of quadratic Dirichlet L-functions. Under the generalized Riemann hypothesis, we showed an asymptotic formula for the fourth moment. Unconditionally, we established a precise lower bound.

Peng-Jie Wong (Math and CS, U of Lethbridge) Nov 4, 2019
Primes in Short Intervals

Bertrand's postulate states that there is always a prime in the interval $[x, 2x]$ for any $x \geq 1$. Applying the prime number theorem, one may further show that there is approximately $\int_x^{2x} \frac{dt}{\log t}$ primes in $[x, 2x]$ for sufficiently large x. There is a more difficult question concerning the distribution of primes p in short intervals when $[x, 2x]$ is replaced by $[x, x + h]$ for some $h \leq x$ and p is required to be congruent to a modulo q for some $(a, q) = 1$. In this talk, we will discuss how short $[x, x + h]$ can be. If time allows, we will sketch a proof of the Bombieri-Vinogradov theorem in short intervals, which answers such a question.

Allysa Lumley (Centre de Recherches Mathématiques, Montreal) Nov 18, 2019
Distribution of Values of L-functions over Function Fields

Let $q \equiv 1 \pmod 4$ be a prime power and $\mathbb{F}_q$ be the finite field with q elements. Let $1/2 < \sigma < 1$ be fixed. We consider D a monic square-free polynomial in $\mathbb{F}_q[T]$ and χ_D the Kronecker symbol associated with D. In this talk, we will discuss the distribution of large values of $\log L(\sigma, \chi_D)$ with D varying over monic square-free polynomials with degree $n \to \infty$. We will highlight the expected similarities to the situation over quadratic extensions of $\mathbb{Q}$ as well as the surprising differences.

Po-Han Hsu (Louisiana State University) Nov 25, 2019
Large deviation principle for the divisor function

Let $\omega(n)$ denote the number of distinct prime divisors of n. Let $W(m)$ be a random integer chosen uniformly from $\{n : n \leq m, n \in \mathbb{N}\}$. Let $X(m)$ be $\omega(W(m))$. The celebrated Erdős-Kac theorem asserts that

$$\frac{X(m) - \log\log m}{\sqrt{\log\log m}} \to N(0, 1),$$

where $N(0, 1)$ is the standard normal distribution.

In 2016, Mehrdad and Zhu studied the large and moderate deviations for the Erdő-Kac theorem. In this talk, we will give a brief introduction to the theory. Then we will discuss how to establish the large deviation principle for $X(m)/\log\log m$. If time allows, we will discuss some generalisations.

This is a joint work with Dr Peng-Jie Wong.

Andrew Fiori (Math and CS, U of Lethbridge) Dec 2, 2019

Simplicity of ABV-packets for Arthur Type Parameters in GL_n

In this talk we will discuss a combinatorial approach to studying the geometry of the moduli space of Langlands parameters for GL_n. We will first discuss several connections between the study of partitions and the study of nilpotent conjugacy classes. We then generalize some of these ideas to describe a relationship between multi-segments and orbits in the moduli space of Langlands parameters. Finally we shall explain how these ideas lead to a proof that simple parameters have simple packets.

Spring 2019

Open problem session Jan 14, 2018

Please bring your favourite (math) problems. Anyone with a problem to share will be given about 5 minutes to present it. We will also choose most of the speakers for the rest of the semester.

Amir Akbary (Math and CS, U of Lethbridge) Jan 21, 2019

Ambiguous Solutions of a Pell Equation

It is known that if the negative Pell equation $X^2 - DY^2 = -1$ is solvable (in integers), and if (x, y) is its solution with smallest positive x and y, then all of its solutions (x_n, y_n) are given by the formula

$$x_n + y_n\sqrt{D} = \pm(x + y\sqrt{D})^{2n+1}$$

for $n \in \mathbb{Z}$. Furthermore, a theorem of Walker from 1967 states that if the equation $aX^2 - bY^2 = \pm 1$ is solvable, and if (x, y) is its solution with smallest positive x and y, then all of its solutions (x_n, y_n) are given by

$$x_n\sqrt{a} + y_n\sqrt{b} = \pm(x\sqrt{a} + y\sqrt{b})^{2n+1}$$

for $n \in \mathbb{Z}$. We describe a unifying theorem that includes both of these results as special cases. The key observation is a structural theorem for the non-trivial ambiguous classes of the solutions of Pell equations $X^2 - DY^2 = \pm N$. This talk is based on the work of Forrest Francis in an NSERC USRA project in summer 2015.

Hadi Kharaghani (Math and CS, U of Lethbridge) Feb 4, 2019

Two new classes of Hadamard matrices

A Hadamard matrix H of order $4n^2$ is said to be *skew-regular* if it is of skew-type and the absolute values of the row sums are all $2n$.

It is conjectured that for each odd integer n there is a skew-regular matrix of order $4n^2$. A Hadamard matrix H of order m is said to be *balancedly splittable* if there is an $\ell \times m$ submatrix H_1 of H such that inner products for any two distinct column vectors of H_1 take at most two values.

It is conjectured that only (Sylvester) Hadamard matrices of order 4^n are balancedly splittable. The existence and applications of these two very interesting classes of matrices to Hadamard diagonalizable strongly regular graphs, maximal equiangular lines set, doubly regular tournament, and unbiased Hadamard matrices will be discussed in detail.

Nathan Ng (Math and CS, U of Lethbridge) Feb 11, 2019
Discrete moments of the Riemann zeta function

In this talk I will consider the discrete moments

$$J_k(T) = \sum_{0<\gamma<T} |\zeta'(\rho)|^{2k},$$

where $\zeta(s)$ is the Riemann zeta function, $\rho = \beta + i\gamma$ is a non-trivial zero of $\zeta(s)$, and $T > 0$. In the 1980's Steve Gonek and Dennis Hejhal (independently) studied these moments and proposed a conjecture for the size of $J_k(T)$. I will give a survey of the known results towards the Gonek-Hejhal conjecture on $J_k(T)$. If time permits, I will present several new results.

Jack Klys (University of Calgary) Feb 25, 2019
Cohen-Lenstra heuristics and counting number fields

We will discuss the Cohen-Lenstra heuristics, both in the classical and non-abelian setting. In particular we will make the connection between these heuristics and the problem of counting extensions of quadratic fields with fixed Galois groups, and when knowledge of the latter implies such heuristics. Finally we will discuss our recent work on the non-abelian case and counting unramified 2-group extensions of quadratic fields.

Joy Morris (Math and CS, U of Lethbridge) Mar 4, 2019
Counting Digraphical Regular Representations (DRRs)

A *Digraphical Regular Representation* (DRR) for a group G is a directed graph whose full automorphism group is the regular representation of G. In 1981, Babai showed that with five small exceptions, there is at least one DRR for every finite group.

A *Cayley digraph* on a group G is a group that contains the regular representation of G in its automorphism group. So when a Cayley digraph is a DRR, its automorphism group is as small as possible given that constraint.

The question of whether or not requiring a certain level of symmetry (in this case, a Cayley digraph) makes having additional symmetry more likely is a natural one, particularly in light of results by Erdös and others proving that almost every graph is asymmetric.

In some 1981 and 1982 papers, Babai and Godsil conjectured that as $r \to \infty$, over all groups G of size r, the proportion of Cayley digraphs that are DRRs tends to 1. They proved this to be true for the restricted family of nilpotent groups of odd order.

I will talk about recent joint work with Pablo Spiga in which we prove this conjecture.

Peng-Jie Wong (Math and CS, U of Lethbridge) Mar 11, 2019
On Siegel Zeros

Siegel zeros (or Landau-Siegel zeros) are potential counterexamples to the generalised Riemann hypothesis (for L-functions). Such zeros, if exist, have to be "very close" to 1 over the complex plane.

In this talk, we will discuss some results concerning Siegel zeros and their applications. If time permits, we will talk about the corresponding "Siegel-Walfisz theorems" for certain L-functions.

Lee Troupe (Math and CS, U of Lethbridge) Mar 18, 2019
Sums of divisors

What happens when you add up the divisors of an integer? This seemingly innocuous question has motivated mathematicians across the ages, from antiquity to the present day. In this talk, we'll survey some conjectures and results on the functions $s(n)$, the sum of the proper divisors of an integer n, and $\sigma(n) = s(n) + n$, the sum of all divisors of n. The ancient Greeks derived religious significance from certain values of these functions; we'll do no such thing in this talk. However, by asking simple questions whose answers turn out to be very complicated – if they're known at all – we will see that an air of mystery continues to surround these two fascinating functions. **The first half of this talk, at the very least, will be extremely accessible to everyone**; tell your students!

Qing Zhang (University of Calgary) Mar 25, 2019
On the holomophy of adjoint L-function for GL(3)

L-functions associated with automorphic forms are vast generalizations of Riemann zeta functions and Dirichlet L-functions. Although the theory of L-functions play a fundamental role in number theory, it is still largely conjectural. If π is an irreducible cuspidal automorphic representation of GL_n over a number field F and $\tilde{\pi}$ is its dual representation, it is conjectured that the Dedekind zeta functions $\zeta_F(s)$ (which is the Riemann zeta function when $F = \mathbb{Q}$) "divides" the Rankin-Selberg L-function $L(s, \pi \times \tilde{\pi})$, i.e., the quotient $L(s, \pi \times \tilde{\pi})/\zeta_F(s)$ (which is called the adjoint L-function of π) should be entire. For $n = 2$, this conjecture was proved by Gelbart-Jacquet. In this talk, I will give a sketchy survey of constructions of some L-functions, including the Rankin-Selberg L-function $L(s, \pi_1 \times \pi_2)$, and report our recent work on the above conjecture when $n = 3$. This is a joint work with Joseph Hundley.

Quanli Shen (Math and CS, U of Lethbridge) Apr 1, 2019
The ternary Goldbach problem with primes in positive density sets

The ternary Goldbach problem stated that every odd integer greater than 5 can be written as sums of three primes. This was proved by Vinogradov for all sufficiently large odd integers and completely proved by Helfgott. On the other hand, by using Green's transference principle method one can extend Vinogradov's result to a density version. In this talk, I will talk about recent results in this direction.

Majid Shahabi May 30, 2019
The appearance of p-adic numbers

In this talk, we present an introduction to p-adic numbers and their appearance in number theory. In particular, we give a proof of Ostrowski's theorem.

Cameron Franc (University of Saskatchewan) Jun 24, 2019

Classification of some three-dimensional vertex operator algebras

Vertex operator algebras (VOAs) as discussed in this talk are graded complex vector spaces with a collection of many bilinear operations satisfying some intricate identities. They first arose in mathematics and physics via the study of string theory and conformal field theories, in the study of the Monster group and moonshine, and in the study of the representation theory of affine Lie algebras. From their inception it has been known that VOAs are deeply connected with the theory of modular forms.

In this talk we will explain how results on vector valued modular forms can be used to classify VOAs satisfying certain finiteness conditions. Our classification for VOAs with exactly three simple representations rests on using arithmetic properties of a family of modular forms expressed in terms of generalized hypergeometric series. The classification of the integral specializations of this family relies on properties of the monodromy, and on results on distributions of primes in arithmetic progressions. No prior familiarity with VOAs will be assumed, and we will focus primarily on the number theoretic aspects of the problem.

Fall 2018

Allysa Lumley (York University, Ontario) Aug 27, 2018
Distribution of Values of L-functions associated to Hyperelliptic Curves over Finite Fields

In 1992, Hoffstein and Rosen proved a function field analogue to Gauß' conjecture (proven by Siegel) 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 $2g+1$ 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. Later, Jung averaged $L(1,\chi_D)$ over monic, squarefree polynomials with degree $2g+2$ varying. Making use of the second case of Artin's formula he gives results about $h_D R_D$, where R_D is the regulator of $\mathcal{O}_D$.

For this talk we discuss the complex moments of $L(1,\chi_D)$, with D monic, squarefree and degree n varying. Using this information we can describe the distribution of values of $L(1,\chi_D)$ and after specializing to $n = 2g+1$ we give results about h_D and specializing to $n = 2g+2$ we give results about $h_D R_D$.

Open problem session Sept 10, 2018

Please bring your favourite (math) problems. Anyone with a problem to share will be given about 5 minutes to present it. We will also choose most of the speakers for the rest of the semester.

Darcy Best (Monash University, Australia) Sept 17, 2018
Transversal This, Transversal That

We will discuss several results related to transversals in Latin squares (think "Sudoku") and other Latin square-like objects. These results centre around showing the existence of, the number of, or the structure of transversals in different cases. Several patterns have been unearthed via computation that will also be discussed. These patterns are often related to the permanent of certain 0-1 matrices that can be used to count the number of transversals in Latin squares.

Nathan Ng (Math and CS, U of Lethbridge) Sept 24, 2018
Mean values of L-functions

In the past twenty years there has been a flurry of activity in the study of mean values of L-functions. This was precipitated by groundbreaking work of Keating and Snaith in which they modelled these mean values by random matrix theory. In this talk I will survey the best known asymptotic results for the mean values of L-functions in certain families (the Riemann zeta function on the half line and/or quadratic Dirichlet L-functions at the central point $s = 1/2$).

Lee Troupe (Math and CS, U of Lethbridge) Oct 1, 2018
Distributions of polynomials of additive functions

How is the set of values of an arithmetic function distributed? In a seminal 1940 paper, Erdős and Kac answered this question for a class of additive functions satisfying certain mild hypotheses, a class which includes the number-of-prime-divisors function. Using ideas from both probability and number theory, they showed that the values of these additive functions tend toward a Gaussian normal distribution. In the intervening years, this "Erdős–Kac class" of additive functions has been broadened to include certain compositions of arithmetic functions, as well as arithmetic functions defined on natural sequences of integers, such as shifted primes and values of polynomials. In this talk, we will discuss recent joint work with Greg Martin (UBC) which further expands the Erdős–Kac class to include arbitrary sums and products of additive functions (satisfying the same mild hypotheses).

Khoa Dang Nguyen (University of Calgary, Alberta) Oct 4, 2018
Linear recurrence sequences and some related results in arithmetic dynamics and ergodic theory

First we introduce some results about certain simple diophantine equations involving linear recurrence sequences. Then we present 2 applications. The first application involves the so-called Orbit Intersection Problem for the arithmetic dynamics of semiabelian varieties and linear spaces. The second application involves certain ergodic averages for surjective endomorphisms of compact abelian groups. Parts of this come from joint work with Dragos Ghioca.

Muhammad Khan (Math and CS, U of Lethbridge) Oct 15, 2018
Fractional clique k-covers, vertex colorings and perfect graphs

The relationship between independence number, chromatic number, clique number, clique cover number and their fractional analogues is well-established for perfect graphs. Here, we study the clique k-cover number $cc_k(G)$ and the fractional clique k-cover number $cc_{fk}(G)$ of a graph G. We relate $cc_{fk}(G)$ to the fractional chromatic number of the complement $\overline{G}$, obtaining a Nordhaus–Gaddum type result. We modify the method of Kahn and Seymour, used in the proof of the fractional Erdős–Faber–Lovász conjecture, to derive an upper bound on $cc_{fk}(G)$ in terms of the independence number $\alpha(G')$ of a particular induced subgraph G' of G. When G is perfect, we get the sharper relation $cc_{fk}(G) = kcc_1(G) = k\alpha(G) \leq cc_k(G)$. This is in line with a result of Grötschel, Lovász, and Schrijver on clique covers of perfect graphs. Moreover, we derive an upper bound on the fractional chromatic number of any graph, which is tight for infinitely many perfect as well as non-perfect graphs. This is joint work with Daya Gaur (Lethbridge).

Andrew Fiori (Math and CS, U of Lethbridge) Oct 22, 2018
The Least Prime in the Chebotarev Density Theorem

The classic theorem of Chebotarev tells us that for any Galois extension L/K of degree n the proportion of primes of K, whose Frobenius conjugacy class is a given conjugacy class of the Galois group is proportional to the size of that conjugacy class. If one interprets this as a statement that the Frobenius of a randomly chosen prime is uniformly distributed, then a natural consequence is that if we begin selecting primes at random, by the time we select roughly $n\log(n)$ primes, we should expect to encounter every conjugacy class at least once. Given that selecting the first m primes is hardly random, and there are infinitely many fields it is hardly surprising that this expectation will often not be met by simply looking at the first m unramified degree one primes.

None the less, there are many known and conjectured upper bounds, relative to the absolute discriminant of L, on the smallest prime for the Chebotarev theorem.

In this talk we will discuss several aspects of this problem, including, as time allows, some recent work on computationally verifying some of these conjectures for all fields with small discriminants and on the discovery, by way of this computational verification, of an infinitely family of fields for which the smallest prime in the Chebotarev theorem is "large".

Dave Morris (Math and CS, U of Lethbridge) Oct 29, 2018
Cayley graphs of order kp are hamiltonian for $k < 48$

For every generating set S of any finite group G, there is a corresponding Cayley graph $\mathrm{Cay}(G;S)$. It was conjectured in the early 1970's that $\mathrm{Cay}(G;S)$ always has a hamiltonian cycle, but there has been very little progress on this problem. Joint work with Kirsten Wilk has established the conjecture in the special case where the order of G is kp, with $k < 48$ and p prime. This was not previously known for values of k in the set $\{24, 32, 36, 40, 42, 45\}$.

Peng-Jie Wong (Math and CS, U of Lethbridge) Nov 5, 2018
Dirichlet's Theorem for Modular Forms

Dirichlet's theorem on arithmetic progressions states that for any $(a, q) = 1$, there are infinitely many primes congruent to a modulo q. Such a theorem together with Euler's earlier work on the infinitude of primes represents the beginning of the study of L-functions and their connection with the distribution of primes.

In this talk, we will discuss some ingredients of the proof for the theorem. Also, we will explain how such an L-function approach leads to Dirichlet's theorem for modular forms that gives a count of Fourier coefficients of modular forms over primes in arithmetic progressions.

Kirsty Chalker (Math and CS, U of Lethbridge) Nov 19, 2018
Perron's formula and explicit bounds on sums

Previously, in this seminar series, we have heard about explicit bounds on

$$\psi(x) := \sum_{n \leq x} \Lambda(n),$$

which refers to the von Mangoldt function $\Lambda(n)$. The point of lift-off for bounding this sum is the explicit formula, which pulls the zeros of the Riemann zeta-function into the equation. However, there are other sums for which using an explicit formula is currently unconditionally impossible. In this talk, I will outline the work of my current thesis, in which I prove bounds for a somewhat general function $\sum_{n \leq x} \frac{a_n}{n^s}$ with $a_n, s \in \mathbb{C}$, and apply these bounds to the sums

$$M(x) := \sum_{n \leq x} \mu(n) \quad \text{and} \quad m(x) = \sum_{n \leq x} \frac{\mu(n)}{n},$$

which refer to the Möbius function $\mu(n)$.

Farzad Maghsoudi (Math and CS, U of Lethbridge) Nov 26, 2018
Finding Hamiltonian cycles in Cayley graphs of order $6pq$

Suppose G is a finite group of order $6pq$ such that p and q are distinct prime numbers. It is conjectured that, if S is any generating set of G, then there is a Hamiltonian cycle in $\mathrm{Cay}(G; S)$. The talk will discuss a special case of this problem which is solved.

Lucile Devin (University of Ottawa, Ontario) Dec 3, 2018
Continuity of the limiting logarithmic distribution in Chebyshev's bias

Following the framework of Rubinstein and Sarnak for Chebyshev's bias, one obtains a limiting logarithmic distribution μ. Then assuming that the zeros of the L-functions are linearly independent over $\mathbf{Q}$, one can show that the distribution μ is smooth.

Inspired by the notion of self-sufficient zeros introduced by Martin and Ng, we use a much weaker hypothesis of linear independence to show that the distribution μ is continuous. In particular the existence of one self-sufficient zero is enough to ensure that the bias is well defined.

Spring 2018

Open problem session Jan 15, 2018

Please bring your favourite (math) problems. Anyone with a problem to share will be given about 5 minutes to present it. We will also choose most of the speakers for the rest of the semester.

Nathan Ng (Math and CS, U of Lethbridge) Jan 29, 2018
Mean values of long Dirichlet polynomials

A Dirichlet polynomial is a function of the form

$$A(t) = \sum_{n \leq N} a_n \, n^{-it}$$

where a_n is a complex sequence, $N \in \mathbb{N}$, and $t \in \mathbb{R}$. For $T \geq 1$, the mean values

$$\int_0^T |A(t)|^2 \, dt$$

play an important role in the theory of L-functions. I will discuss work of Goldston and Gonek on how to evaluate these integrals in the case that $T < N < T^2$. This will depend on the correlation sums

$$\sum_{n \leq x} a_n \, a_{n+h} \text{ for } h \in \mathbb{N}.$$

If time permits, I will discuss a conjecture of Conrey and Keating in the case that a_n corresponds to a generalized divisor function and $N > T$.

Ha Tran (University of Calgary, Alberta) Feb 12, 2018
Reduced Ideals from the Reduction Algorithm

Reduced ideals of a number field F have inverses of small norms and they form a finite and regularly distributed set in the infrastructure of F. Therefore, they can be used to compute the regulator and the class number of a number field [5, 3, 2, 1, 4]. One usually applies the reduction algorithm (see Algorithm 10.3 in [4]) to find them. Ideals obtained from this algorithm are called 1-reduced. There exist reduced ideals that are not 1-reduced. We will show that these ideals have inverses of larger norms among reduced ones. Especially, we represent a sufficient and necessary condition for reduced ideals of real quadratic fields to be obtained from the reduction algorithm.

[1] Johannes Buchmann. A subexponential algorithm for the determination of class groups and regulators of algebraic number fields. In *Séminaire de Théorie des Nombres, Paris 1988–1989*, volume 91 of *Progr. Math.*, pages 27–41. Birkhäuser Boston, Boston, MA, 1990.

[2] Johannes Buchmann and H. C. Williams. On the infrastructure of the principal ideal class of an algebraic number field of unit rank one. *Math. Comp.*, 50(182):569–579, 1988.

[3] H. W. Lenstra, Jr. On the calculation of regulators and class numbers of quadratic fields. In *Number theory days, 1980 (Exeter, 1980)*, volume 56 of *London Math. Soc. Lecture Note Ser.*, pages 123–150. Cambridge Univ. Press, Cambridge, 1982.

[4] René Schoof. Computing Arakelov class groups. In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 447–495. Cambridge Univ. Press, Cambridge, 2008.

[5] Daniel Shanks. The infrastructure of a real quadratic field and its applications. In *Proceedings of the Number Theory Conference (Univ. Colorado, Boulder, Colo., 1972)*, pages 217–224. Univ. Colorado, Boulder, Colo., 1972.

Andrew Fiori (Math and CS, U of Lethbridge) Feb 26, 2018
A Geometric Description of Arthur Packets

In this talk I will discuss joint work with Clifton Cunningham, Ahamed Moussaui, James Mracek and Bin Xu.

I will begin by giving a brief overview of the (conjectural) Langlands Correspondence, focusing in particular on Vogan's geometric reformulation of the local Langlands Correspondence. We will then discuss some geometric objects that arise as part of several conjectures which give geometric interpretations to Arthur packets and their associated stable distributions under the LLC. More specifically we shall discuss equivariant perverse sheaves and their vanishing cycles.

Amir Akbary (Math and CS, U of Lethbridge) Mar 5, 2018
On the size of the gcd of a^n-1 and b^n-1

We review some results, from the last twenty years, on the problem of bounding

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

as n varies. Here either a and b are integers or a and b are polynomials with coefficients in certain fields. In spite of elementary nature of the problem, the results are depended on tools from Diophantine approximation and Diophantine geometry.

Steve Wilson (Northern Arizona University) Mar 12, 2018
The BGCG Construction

Well, it's not really a construction yet — it's more like a template for constructions. It's a way to take many copies of one tetravalent graph B, the 'base graph', and identify each edge-midpoint with one other according to another graph C, the 'connection graph' to produce a bipartite tetravalent graph. If the identifying is done with caution, wisdom and, um, insouciance, the resulting graph will have lots of symmetry.

The cunning of the identifications is related to edge-colorings of the base graph which are themselves nicely symmetric, and we will give several examples where the symmetry can actually be achieved.

Peng-Jie Wong (Math and CS, U of Lethbridge) Mar 19, 2018
On Generalisations of the Titchmarsh divisor problem

The study of the asymptotic behaviour of the summatory function of the number of divisors of shifted primes was initiated by Titchmarsh, who showed that under the generalised Riemann hypothesis, one has

$$\sum_{p\leq x}\tau(p-a)=x\prod_{p\nmid a}\left(1+\frac{1}{p(p-1)}\right)\prod_{p\mid a}\left(1-\frac{1}{p}\right)+O\left(\frac{x\log\log x}{\log x}\right),$$

where τ denotes the divisor function. The above formula was first proved unconditionally by Linnik via the dispersion method. Moreover, applying the celebrated Bombieri-Vinogradov theorem, Halberstam and Rodriguez independently gave another proof.

In this talk, we shall study the Titchmarsh divisor problem in arithmetic progressions by considering the sum

$$\sum_{\substack{p\leq x\\ p\equiv b \pmod r}}\tau(p-a).$$

Also, we will try to explain how to obtain an asymptotic formula for the same, uniform in a certain range of the modulus r. If time allows, we will discuss a number field analogue of this problem by considering the above sum over primes satisfying Chebotarev conditions.

(This is joint work with Akshaa Vatwani.)

Joy Morris (Math and CS, U of Lethbridge) Mar 26, 2018
Cayley index and Most Rigid Representations (MRRs)

For any finite group G, a natural question to ask is the order of the smallest possible automorphism group for a Cayley graph on G. A particular Cayley graph whose automorphism group has this order is referred to as an MRR (Most Rigid Representation), and its *Cayley index* is the index of the regular representation of G in its automorphism group. Study of GRRs (Graphical Regular Representations, where the full automorphism group is the regular representation of G) showed that with the exception of two infinite families and ten individual groups, every group admits a Cayley graph whose MRRs are GRRs, so that the Cayley index is 1. I will present results that complete the determination of the Cayley index for those groups whose Cayley index is greater than 1. This is based on joint work with Josh Tymburski, who was an undergraduate student here at the time.

Jean-Marc Deshouillers (University of Bordeaux, France) Apr 9, 2018
Values of arithmetic functions at consecutive arguments

We shall place in a general context the following result recently (*) obtained jointly with Yuri Bilu (Bordeaux), Sanoli Gun (Chennai) and Florian Luca (Johannesburg).

Theorem. *Let $\tau(\cdot)$ be the classical Ramanujan τ-function and let k be a positive integer such that $\tau(n) \neq 0$ for $1 \leq n \leq k/2$. (This is known to be true for $k < 10^{23}$, and, conjecturally, for all k.) Further, let σ be a permutation of the set $\{1, \dots, k\}$. We show that there exist infinitely many positive integers m such that*

$$\big|\tau\big(m+\sigma(1)\big)\big| < \big|\tau\big(m+\sigma(2)\big)\big| < \cdots < \big|\tau\big(m+\sigma(k)\big)\big|.$$

The proof uses sieve method, Sato-Tate conjecture, recurrence relations for the values of τ at prime power values.

(*) Hopefully to appear in 2018.

Alia Hamieh (University of Northern British Columbia) May 7, 2018
Non-vanishing of L-functions of Hilbert Modular Forms inside the Critical Strip

In this talk, I will discuss recent joint work with Wissam Raji. We show that, on average, the L-functions of cuspidal Hilbert modular forms with sufficiently large weight k do not vanish on the line segments $\Im(s) = t_0$, $\Re(s) \in (\frac{k-1}{2}, \frac{k}{2} - \epsilon) \cup (\frac{k}{2} + \epsilon, \frac{k+1}{2})$. The proof follows from computing the Fourier expansion of a certain kernel function associated with Hilbert modular forms and estimating its first Fourier coefficient. This result is analogous to the case of classical modular forms which was proved by W. Kohnen in 1997.

Allysa Lumley (York University, Ontario) Aug 27, 2018
Distribution of Values of L-functions associated to Hyperelliptic Curves over Finite Fields

In 1992, Hoffstein and Rosen proved a function field analogue to Gauß' conjecture (proven by Siegel) 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 $2g+1$ 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. Later, Jung averaged $L(1, \chi_D)$ over monic, squarefree polynomials with degree $2g+2$ varying. Making use of the second case of Artin's formula he gives results about $h_D R_D$, where R_D is the regulator of $\mathcal{O}_D$.

For this talk we discuss the complex moments of $L(1, \chi_D)$, with D monic, squarefree and degree n varying. Using this information we can describe the distribution of values of $L(1, \chi_D)$ and after specializing to $n = 2g+1$ we give results about h_D and specializing to $n = 2g+2$ we give results about $h_D R_D$.

Fall 2017

Open problem session Sept 11, 2017

Please bring your favourite (math) problems. Anyone with a problem to share will be given about 5 minutes to present it. We will also choose most of the speakers for the rest of the semester.

Peng-Jie Wong (Math and CS, U of Lethbridge) Sept 18, 2017
Nearly supersolvable groups and Artin's conjecture

Let K/k be a Galois extension of number fields with Galois group G, and let ρ be a non-trivial irreducible representation of G of dimension n. The Artin holomorphy conjecture asserts that the Artin L-function attached to ρ extends to an entire function.

It is well-known that when $n = 1$, this conjecture follows from Artin reciprocity. Also, by the works of Langlands and many others, we know that this conjecture is valid for $n = 2$ under certain conditions. However, in general, the Artin holomorphy conjecture is wildly open.

In this talk, we will discuss how elementary group theory plays a role in studying the Artin holomorphy conjecture and introduce the notion of "nearly supersolvable groups". If time allows, we will explain how such groups lead to a proof of the Artin holomorphy conjecture for Galois extensions of degree less than 60.

Muhammad Khan (Math and CS, U of Lethbridge) Sept 25, 2017
The contact graphs of totally separable packings

Contact graphs have emerged as an important tool in the study of translative packings of convex bodies and have found numerous applications in materials science. The contact number of a packing of translates of a convex body is the number of edges in the contact graph of the packing, while the Hadwiger number of a convex body is the maximum vertex degree over all such contact graphs. In this talk, we investigate the Hadwiger and contact numbers of totally separable packings of convex bodies, known as the separable Hadwiger number and the separable contact number, respectively. We show that the separable Hadwiger number of any smooth strictly convex body in dimensions $d = 2, 3, 4$ is $2d$ and the maximum separable contact number of any packing of n translates of a smooth strictly convex domain is $\lfloor 2n - 2\sqrt{n} \rfloor$. Our proofs employ a characterization of total separability in terms of hemispherical caps on the boundary of a smooth convex body, Auerbach bases of finite dimensional real normed spaces, angle measures in real normed planes, minimal perimeter polyominoes and an approximation of smooth o-symmetric strictly convex domains by, what we call, Auerbach domains. This is joint work with K. Bezdek (Calgary) and M. Oliwa (Calgary).

Andrew Fiori (Math and CS, U of Lethbridge) Oct 2, 2017
The average number of quadratic Frobenius pseudoprimes

Primality testing has a number of important applications. In particular in cryptographic applications the complexity of existing deterministic algorithms causes increasing latency as the size of numbers we must test grow and the number of tests we must run before finding a prime grows aswell. These observations lead one to consider potentially non-deterministic algorithms which are faster, and consequently leads one to consider the false positives these algorithms yield, which we call pseudoprimes.

In this talk I will discuss my recent work with Andrew Shallue where we study Quadratic Frobenius Pseudoprimes. I shall describe our results on an asymptotic lower bounds on the number of false positives. These results represent a generalization of those Erdos-Pomerance concerning similar problems for (Fermat) pseudoprimes.

Lee Troupe (University of British Columbia) Oct 16, 2017
Normally distributed arithmetic functions

In the late 1930s, Paul Erdős attended a seminar at Cornell University given by Mark Kac, who suspected that divisibility by primes satisfies a certain "statistical independence" condition. If this were true, the central limit theorem could be used to show that the number of distinct prime factors of n, as n varies over the natural numbers, is normally distributed, with mean $\log\log n$ and standard deviation $\sqrt{\log\log n}$. Erdős used sieve methods to confirm Kac's intuition, and the resulting Erdős-Kac theorem is a foundational result in the field of probabilistic number theory. Many different proofs of and variations on the Erdős-Kac theorem have been given in the intervening decades. This talk will highlight some of these results and the techniques used to obtain them, including recent work of the speaker and Greg Martin (UBC).

Sam Broadbent, Habiba Kadiri, and Kirsten Wilk (Math and CS, U of L) Oct 23, 2017
Sharper bounds for Chebyshev functions $\theta(x)$ and $\psi(x)$

In this talk we report on some research projects from summer 2017 supported by NSERC-USRA. In the first part of the project, we surveyed all existing explicit results from the past 60 years on prime counting functions, with a special focus on $\theta(x)$ (counting $\log p$ for each prime $p \leq x$). In the second part, we provided new bounds for the Chebyshev function $\psi(x)$ based on a recent zero density result for the zeros of the Riemann zeta function (due to Kadiri-Lumley-Ng). Finally, we have established the current best results for the prime counting function $\theta(x)$ for various ranges of x.

(Joint work with Noah Christensen, Allysa Lumley, and Nathan Ng)

Akshaa Vatwani (University of Waterloo, Ontario) Oct 30, 2017
Variants of equidistribution in arithmetic progression

It is well known that the prime numbers are equidistributed in arithmetic progression. Such a phenomenon is also observed more generally for a class of multiplicative functions. We derive some variants of such results and give an application to tuples of squarefree integers in arithmetic progression. We also discuss an interesting application that relates to the Chowla conjecture on correlations of the Möbius function, and show its relevance to the twin prime conjecture.

Károly Bezdek (University of Calgary, Alberta) Nov 6, 2017

Bounds for totally separable translative packings in the plane

A packing of translates of a convex domain in the Euclidean plane is said to be totally separable if any two packing elements can be separated by a line disjoint from the interior of every packing element. This notion was introduced by G. Fejes Toth and L. Fejes Toth (1973) and has attracted significant attention. In this lecture I will discuss the separable analogue of the classical inequality of N. Oler (from geometry of numbers) for totally separable translative packings of convex domains and then derive from it some new results. This includes finding the largest density of totally separable translative packings of an arbitrary convex domain and finding the smallest area convex hull of totally separable packings (resp., totally separable soft packings) generated by given number of translates of a convex domain (resp., soft convex domain). Last but not least, we determine the largest covering ratio (that is, the largest fraction of the plane covered) of totally separable soft circle packings with given soft parameter. This is a joint work with Zsolt Langi (Univ. of Technology, Budapest, Hungary).

Forrest Francis (Math and CS, U of Lethbridge) Nov 20, 2017

Euler's function on products of primes in progressions

Let $\phi(n)$ be Euler's totient function and let q and a be fixed coprime natural numbers. Denote by $S_{q,a}$ the set of natural numbers whose prime divisors are all congruent to a modulo q. We can establish

$$\limsup_{n\in S_{q,a}} \frac{n}{\phi(n)\big(\log(\phi(q)\log n)\big)^{1/\phi(q)}} = \frac{1}{C(q,a)},$$

where $C(q,a)$ is a constant associated with a theorem of Mertens. We may then wish to know whether there are infinitely many n in $S_{q,a}$ for which

$$(*) \qquad \frac{n}{\phi(n)\big(\log\phi(q)\log n\big)^{1/\phi(q)}} > \frac{1}{C(q,a)}$$

is true. In the case $q = a = 1$, Nicolas (1983) established that if the Riemann hypothesis is true, then $(*)$ holds for all primorials (products of the form $\prod_{p\le x} p$), but if the Riemann hypothesis is false then there are infinitely many primorials for which $(*)$ is true and infinitely many primorials for which $(*)$ is false.

In this talk we will show that, for some $q > 1$, the work of Nicolas can be generalized by replacing the Riemann hypothesis with analogous conjectures for Dirichlet L-functions and replacing the primorials with products of the form

$$\prod_{\substack{p\le x\\ p\equiv a \,(\mathrm{mod}\, q)}} p.$$

Sara Sasani (Math and CS, U of Lethbridge) Nov 27, 2017

A strongly regular decomposition of the complete graph and its association scheme

A *Strongly Regular Graph*, $\mathrm{SRG}(\nu, k, \lambda, \mu)$, is a k-regular graph with ν vertices such that every two adjacent vertices have λ common neighbors, and every two non-adjacent vertices have μ common neighbors. For each positive integer m, a construction for 2^m disjoint $\mathrm{SRG}(2^{2m}(2^m+2), 2^{2m}+2^m, 2^m, 2^m)$ will be shown to form a decomposition of the complete graph with $2^{2m}(2^m+2)$ vertices, if the cliques of size 2^{2m} is considered as a strongly regular graph with parameter $(2^{2m}(2^m+2), 2^{2m}-1, 2^{2m}-2, 0)$.

By decomposing the cliques and the strongly regular graphs further, we show the existence of a symmetric association scheme with $2^{m+2}-2$ classes and explain, by an example, how to find the first and second eigenmatrices of the scheme.

Clifton Cunningham (University of Calgary, Alberta) Dec 4, 2017

On the modularity conjecture for abelian varieties over $\mathbb{Q}$

The modularity theorem tells us that for every elliptic curve E over $\mathbb{Q}$, there is a modular form f_E such that the L-function $L(s, f_E)$ for f_E coincides with the L-function $L(s, \rho_E)$ for the Galois representation on the Tate module of E. In fact, f_E is a cusp form and its level is determined by the conductor of ρ_E. Since the modular form f_E determines an automorphic representation π_E of $\mathrm{GL}_2(\mathbb{A}_\mathbb{Q})$ with the same L-function as f_E, we have

$$L(s, \rho_E) = L(s, \pi_E).$$

The modularity conjecture for abelian varieties is the obvious generalization of this theorem from the case of one-dimensional abelian varieties: For every abelian variety A over $\mathbb{Q}$ there is an automorphic representation π_A of a group $G(\mathbb{A}_\mathbb{Q})$ such that

$$L(s, \rho_A) = L(s, \pi_A),$$

where ρ_A is the Galois representation on the Tate module of A.

In this talk I will describe recent joint work with Lassina Dembélé giving new instances of the modularity conjecture for abelian varieties over $\mathbb{Q}$. Where do we hunt for π_A? What is the group G over $\mathbb{Q}$? What is the level of π_A? Can we find a generalized modular form f_A from which π_A can be built? I will explain how we use work of Benedict Gross, Freydoon Shahidi and others to answer these questions. I will also explain how thesis work by Majid Shahabi illuminates the level of π_A.

This is joint work with Lassina Dembélé.

Spring 2017

Darcy Best (Monash University, Australia) Jan 9, 2017
Transversals in Latin arrays with many symbols

A transversal of a latin square of order n is a set of n entries picked in such a way that no row, column or symbol is present more than once. As you add more symbols to a latin square, you expect the number of transversals to increase. We show that once the number of symbols reaches a certain threshold, the square is guaranteed to have a transversal.

Open problem session Jan 16, 2017

Please bring your favourite (math) problems. Anyone with a problem to share will be given about 5 minutes to present it. We will also choose most of the speakers for the rest of the semester.

Alia Hamieh (Math and CS, U of Lethbridge) Jan 23, 2017
Non-vanishing of central values of Rankin-Selberg L-functions

In this talk, we discuss some results on the non-vanishing of the central values of Rankin-Selberg convolutions of families of Hilbert modular forms. Such results are obtained by establishing some asymptotics of certain twisted first and second moments. This is an on-going joint work with Naomi Tanabe.

Nathan Ng (Math and CS, U of Lethbridge) Jan 30, 2017
A subconvexity bound in the $\boldsymbol{t}$-aspect for degree two L-functions

Let f be a primitive modular form and $L_f(s)$ its associated L-function. Anton Good (1982) showed that $L_f(\frac{1}{2}+it) \ll |t|^{\frac{1}{3}+\varepsilon}$ in the case f is a modular form on the full modular group. In 1987, Matti Jutila gave a different proof and this was later refined by Martin Huxley. In this talk, we explain how the Jutila-Huxley approach can be generalized to the case of modular forms with arbitrary character χ, weight k, and level N. This is joint work with Andrew Booker (Bristol) and Micah Milinovich (Mississippi).

Joy Morris (Math and CS, U of Lethbridge) Feb 6, 2017
Oriented Regular Representations

An oriented graph is a digraph with at most one arc between any pair of vertices. We say that the action of a group on a set of points is regular if it is sharply transitive; that is, there is exactly one group element mapping any point to any other point. An oriented regular representation (ORR) for a group G is an oriented graph whose automorphism group is isomorphic to the regular action of G on the vertices.

In 1980, Babai asked which groups admit an ORR. I will discuss this problem, and present joint work with Pablo Spiga in which we showed that every non-solvable group admits an ORR.

Habiba Kadiri (Math and CS, U of Lethbridge) Feb 13, 2017
Explicit results in prime number theory

The prime number theorem, proven in 1896, is one of the first major theorems in analytic number theory. It provides estimates for prime counting functions. In 1962, Rosser and Schoenfeld gave a method to estimate the error term in the approximation of the prime counting function $\psi(x)$. Since then, progress on the numerical verification of the Riemann Hypothesis and widening the zero-free region of the Riemann zeta function have allowed numerical improvements of these bounds. In this talk, we present various new explicit methods such as introducing some smooth weights and establishing some zero density estimates for the Riemann zeta function. We also present some explicit results for primes in short intervals and for primes in arithmetic progressions.

Dave Morris (Math and CS, U of Lethbridge) Feb 27, 2017
Modern approach to the Traveling Salesman Problem

The Traveling Salesman Problem asks for the shortest route through a collection of cities. This classical problem is very hard, but, by applying Linear Programming (and other techniques), the optimal route has been found in test cases that have tens of thousands of cities. This talk will present some of the powerful methods that are explained in W. J. Cook's book "In Pursuit of the Traveling Salesman".

Hadi Kharaghani (Math and CS, U of Lethbridge) Mar 6, 2017
An association scheme for twin prime powers

Twin prime powers are used in the construction of some very interesting combinatorial objects. In an old paper they are used in the construction of regular Hadamard matrices. In a recent work, they are used to show the existence of an infinite class of Hadamard matrices lacking a certain algebraic structure.

In this talk I will discuss the use of twin prime powers in order to show the existence of a class of translation commutative association schemes. I will use the twin primes 3 and 5, as an example, to make the talk accessible to everyone.

Forrest J. Francis (Math and CS, U of Lethbridge) Mar 13, 2017
Special values of Euler's function

In 1909, Landau showed that

$$\limsup \frac{n}{\phi(n)\log\log n} = e^{\gamma},$$

where $\phi(n)$ is Euler's function. Later, Rosser and Schoenfeld asked whether there were infinitely many n for which $n/\phi(n) > e^{\gamma}\log\log n$. This question was answered in the affirmative in 1983 by Jean-Louis Nicolas, who showed that there are infinitely many such n both in the case that the Riemann Hypothesis is true, and in the case that the Riemann Hypothesis is false.

One can prove a generalization of Landau's theorem where we restrict our attention to integers whose prime divisors all fall in a fixed arithmetic progression. In this talk, I will discuss the methods of Nicolas as they relate to the classical result, and also provide evidence that his methods could be generalized in the same vein to provide answers to similar questions related to the generalization of Landau's theorem.

Sahar Siavashi (Math and CS, U of Lethbridge) Mar 27, 2017
On the solutions of certain congruences

An odd prime p is called a *Wieferich prime* (in base 2), if

$$2^{p-1} \equiv 1 \pmod{p^2}.$$

These primes first were considered by A. Wieferich in 1909, while he was working on a proof of Fermat's last theorem. This notion can be generalized to any integer base $a > 1$. In this talk, we discuss the work that has been done regarding the size of the set of non-Wieferich primes and show that, under certain conjectures, there are infinitely many non-Wieferich primes in certain arithmetic progressions. Also we consider the congruence

$$a^{\varphi(m)} \equiv 1 \pmod{m^2},$$

for an integer m with $(a, m) = 1$, where φ is Euler's totient function. The solutions of this congruence lead to Wieferich numbers in base a. In this talk we present a way to find the largest known Wieferich number for a given base. In another direction, we explain the extensions of these concepts to other number fields such as quadratic fields of class number one. We also consider the solutions of the congruence

$$g^m - g^n \equiv 0 \pmod{f^m - f^n},$$

where m and n are two distinct natural numbers and f and g are two relatively prime polynomials with coefficients in the field of complex numbers. We prove this congruence has finitely many solutions.

Amir Akbary (Math and CS, U of Lethbridge) Apr 3, 2017
Elliptic sequences

An *elliptic sequence* is a solution over an arbitrary integral domain of the recursion

$$W_{m+n}\, W_{m-n} \,=\, W_{m+1}\, W_{m-1}\, W_n^2 - W_{n+1}\, W_{n-1}\, W_m^2,$$

where $m, n \in \mathbb{Z}$. The theory of integral elliptic sequences was developed by Morgan Ward in 1948. We describe the fundamental classification theorem of Ward for these sequences. Our emphasis will be on the so called "singular" sequences and their relation to the classical Lucas sequences.

Fall 2016

Open problem session Sept 12, 2016

Please bring your favourite (math) problems. Anyone with a problem to share will be given about 5 minutes to present it. We will also choose most of the speakers for the rest of the semester.

Hadi Kharaghani (Math and CS, U of Lethbridge) Sept 19, 2016
The strongly regular graph SRG(765, 192, 48, 48)

Andries Brouwer is 65 and a special issue of Designs, Codes and Cryptography is issued to celebrate the occasion.

Professor Brouwer maintains an elegant public database of existence results for all possible strongly regular graphs on $n \leq 1300$ vertices. In a very nice paper, Cohen and Pasechnik implemented most of the graphs listed there in the open source software Sagemath and obtained a graph for each set of parameters mentioned in the database. In their initial version of the paper, they mentioned 11 cases as *missing values*. A number of the cases were related to my work with professors Janko, Tonchev, and Ionin. I tried to help out with these cases and four cases were resolved quickly, after I sent detailed instructions. However, there was a problem with the case of SRG$(765, 192, 48, 48)$. This talk relates to this special case and a nice application of generalized Hadamard matrices.

To make the talk accessible to general audiences, I will provide many examples illustrating the concepts involved.

Farzad Aryan (Université de Montréal, Quebec) Sept 26, 2016
On the zero free region of the Riemann zeta function

We discuss the possibility that the Riemann zeta function has a zero $\sigma + iT$ to the left of the classical zero free region. We will show how the existence of this zero forces the function to have many more zeros in the vicinity of $\sigma + iT$ or/and $\sigma + 2iT$.

Dave Morris (Math and CS, U of Lethbridge) Oct 3, 2016
Hamiltonian paths in projective checkerboards

Place a checker in some square of an $m \times n$ rectangular checkerboard, and glue opposite edges of the checkerboard to make a projective plane. We determine whether the checker can visit all the squares of the checkerboard (without repeating any squares), by moving only north and east. This is joint work with Dallan McCarthy, and no advanced mathematical training will be needed to understand most of the talk.

Mikhail Muzychuk (Netanya Academic College, Israel) Oct 17, 2016
Non-commutative association schemes of rank 6

An association scheme is a coloring of a complete graph satisfying certain regularity conditions. It is a generalization of groups and has many applications in algebraic combinatorics. Every association scheme yields a special matrix algebra called the Bose-Mesner algebra of a scheme. A scheme is called commutative if its Bose-Mesner algebra is commutative. Commutative schemes were the main topic of the research in this area for decades. Only recently non-commutative association schemes attracted the attention of researchers. In my talk I'll present the results about non-commutative association schemes of the smallest possible rank, rank 6. This is a joint work with A. Herman and B. Xu.

Nathan Ng (Math and CS, U of Lethbridge) Oct 24, 2016
The sixth moment of the Riemann zeta function and ternary additive divisor sums

Hardy and Littlewood initiated the study of the $2k$-th moments of the Riemann zeta function on the critical line. In 1918 Hardy and Littlewood established an asymptotic formula for the second moment and in 1926 Ingham established an asymptotic formula for the fourth moment. In this talk we consider the sixth moment of the zeta function on the critical line. We show that a conjectural formula for a certain family of ternary additive divisor sums implies an asymptotic formula for the sixth moment. This builds on earlier work of Ivic and of Conrey-Gonek.

Amir Akbary (Math and CS, U of Lethbridge) Oct 31, 2016
Value-distribution of quadratic L-functions

We describe a theorem of M. Mourtada and V. Kumar Murty on the distribution of values of the logarithmic derivative of the L-functions attached to quadratic characters. Under the assumption of the generalized Riemann Hypothesis they prove the existence of a density function that gives the distribution of values of the logarithmic derivative of such L-functions at a fixed real point greater than $1/2$. Following classical results of Wintner, we also describe how this distribution can be described as an infinite convolution of local distributions.

Alia Hamieh (Math and CS, U of Lethbridge) Nov 15, 2016
Value-distribution of cubic L-functions

In this talk, we describe a method for studying the value-distribution of L-functions based on the Jessen-Wintner theory. This method has been explored recently by Ihara and Matsumoto for the case of logarithms and logarithmic derivatives of Dirichlet L-functions of prime conductor and by Mourtada and V. K. Murty for the case of logarithmic derivatives of Dirichlet L-functions associated with quadratic characters. We show how to extend such results to the case of cubic characters. In fact, we describe a distribution theorem for the values of the logarithms and logarithmic derivatives of a certain family of Artin L-functions associated with cubic Hecke characters. This is a joint work with Amir Akbary.

Luke Morgan (University of Western Australia) Nov 22, 2016
Permutation groups and graphs

The use of graphs to study permutation groups goes back to Higman who first introduced the orbital graphs, and used them to characterise the primitive groups. Since then, graph theory and permutation group theory have become intertwined, with many beautiful results. In this talk, I will discuss some problems which lie across the boundary of permutation group theory and graph theory (or at least algebraic graph theory), such as how to characterise a new class of permutation groups that includes the primitive ones - the so called semiprimitive groups.

Gabriel Verret (University of Auckland, New Zealand) Nov 29, 2016
Vertex-primitive digraphs having vertices with almost equal neighbourhoods

A permutation group G on Ω is transitive if for every $x, y \in \Omega$ there exists $g \in G$ mapping x to y. The group G is called primitive if, in addition, it preserves no nontrivial partition of Ω. Let Γ be a vertex-primitive digraph, that is, its automorphism group acts primitively on its vertex-set. It is not hard to see that, in this case, Γ cannot have two distinct vertices with equal neighbourhoods, unless Γ is in some sense trivial. I will discuss some recent results about the case when Γ has two vertices with "almost" equal neighbourhoods, and how these results were used to answer a question of Araújo and Cameron about synchronising groups. (This is joint work with Pablo Spiga.)

Spring 2016

Open problem session Jan 11, 2016

Please bring your favourite (math) problems. Anyone with a problem to share will be given about 5 minutes to present it. We will also choose most of the speakers for the rest of the semester.

Francesco Pappalardi (Università Roma Tre, Italy) Jan 25, 2016
On never primitive points on elliptic curves

The Lang-Trotter Conjecture for primitive points predicts an expression for the density of primes p for which a fixed rational point (not torsion) of a fixed elliptic curve defined on $\mathbb{Q}$ is a generator of the curve reduced modulo p. After providing the definition of such a density in terms of Galois representations associated with torsion points of the curve, we will tell the short story of the contributions to the conjecture and provide examples of families of elliptic curves for which the conjecture holds for trivial reasons. This is the notion of "never primitive point." The case of elliptic curves in complex multiplication will be discussed in greater detail. Part of the work is in collaboration of N. Jones.

Francesco Pappalardi (Università Roma Tre, Italy) Jan 27, 2016
The distribution of multiplicatively dependent vectors

Let n be a positive integer, G be a group and let $\nu = (\nu_1, \dots, \nu_n)$ be in G^n. We say that ν is a multiplicatively dependent n-tuple if there is a non-zero vector $(k_1, \dots, k_n)$ in $\mathbb{Z}^n$ for which for which $\nu_1^{k_1} \cdots \nu_n^{k_n} = 1$. Given a finite extension K of $\mathbb{Q}$, we denote by $M_{n,K}(H)$ the number of multiplicatively dependent n-tuples of algebraic integers of K^* of naive height at most H and we denote by $M^*_{n,K}(H)$ the number of multiplicatively dependent n-tuples of algebraic numbers of K^* of height at most H. In this seminar we discuss several estimates and asymptotic formulas for $M_{n,K}(H)$ and for $M^*_{n,K}(H)$ as $H \to \infty$. For each ν in $(K^*)^n$ we define m, the multiplicative rank of ν, in the following way. If ν has a coordinate which is a root of unity we put $m = 1$. Otherwise let m be the largest integer with $2 \le m \le n+1$ for which every set of $m-1$ of the coordinates of ν is a multiplicatively independent set. We also consider the sets $M_{n,K,m}(H)$ and $M^*_{n,K,m}(H)$ defined as the number of multiplicatively dependent n-tuples of multiplicative rank m whose coordinates are algebraic integers from K^*, respectively algebraic numbers from K^*, of naive height at most H and will consider similar questions for them.

Micah Milinovich (University of Mississippi) Feb 1, 2016
Fourier Analysis and the zeros of the Riemann zeta-function

I will show how the classical Beurling-Selberg extremal problem in harmonic analysis arises naturally when studying the vertical distribution of the zeros of the Riemann zeta-function and other L-functions. Using this relationship, along with techniques from Fourier analysis and reproducing kernel Hilbert spaces, we can prove the sharpest known bounds for the number of zeros in an interval on the critical line and we can also study the pair correlation of zeros. Our results on pair correlation extend earlier work of P. X. Gallagher and give some evidence for the well-known conjecture of H. L. Montgomery. This talk is based on a series of papers which are joint with E. Carneiro, V. Chandee, and F. Littmann.

Alexey Popov (Math and CS, U of Lethbridge) Feb 8, 2016
Operator algebras with reduction properties

An algebra is a vector space with a well-defined multiplication. An operator algebra is an algebra of operators acting on a Hilbert space, typically assumed closed in the norm topology. An easy example of an operator algebra is the algebra $M_n(\mathbb{C})$ of all the complex $n \times n$ matrices. In this colloquium-style talk, we will discuss operator algebras A with the following property: every A-invariant subspace is complemented by another A-invariant subspace. This property is called the Reduction property and is a kind of semisimplicity. We will discuss the connections of this property to some classical problems, such as Kadison Similarity Problem and the structure of amenable operator algebras.

Nathan Ng (Math and CS, U of Lethbridge) Feb 22, 2016
Linear combinations of zeros of L-functions

The linear independence conjecture asserts that the multiset of positive ordinates of the zeros of automorphic L-functions is linearly independent over the field of rational numbers. This deep conjecture implies that if $1/2 + i\gamma$ is a zero of the Riemann zeta function, then $1/2 + 2i\gamma$ is a not a zero of the zeta function. I will show that on the Riemann hypothesis this is true infinitely often. I will also discuss variants of this phenomenon. This is joint work with Greg Martin and Micah Milinovich.

Rob Craigen (University of Manitoba) Feb 29, 2016
Survey of negacyclic weighing matrices

A square or rectangular matrix is circulant if every row after the first is a right circular shift of its predecessor. Negacyclic matrices are defined the same way except that the first entry of each row is negated after circulating the preceding row. A partial Hadamard matrix is a rectangular $k \times n$ $(1, -1)$-matrix M satisfying $MM^T = nI$. In the summer of 2013 I hired four sharp undergraduate students to tackle a problem about circulant partial Hadamard matrices. The question of existence of certain negacyclic weighing matrices kept coming up, so we devoted some energy to exploring this largely uncultivated territory. In the end we produced, apparently for the first time, a fairly comprehensive survey of these objects, their structure, why certain classes exist and others cannot. The flavour of the existence questions for this class of weighing matrices is decidedly different from that of group-developed form, even though much of the theory is the same. We discuss some situations in which negacyclic weighing matrices naturally appear, and conclude with some tantalizing new open questions arising from the work.

Alia Hamieh (Math and CS, U of Lethbridge) Mar 7, 2016
Determining Hilbert modular forms by the central values of Rankin-Selberg convolutions

In this talk, we give a brief overview of adelic Hilbert modular forms. Then, we show that the central values of the Rankin-Selberg convolutions, $L(g \otimes f, s)$, uniquely determine an adelic Hilbert modular form g, where f varies in a carefully chosen infinite family of adelic Hilbert modular forms. We prove our results in both the level and weight aspects. This is a joint work with Naomi Tanabe.

Joy Morris (Math and CS, U of Lethbridge) Mar 14, 2016
Automorphisms of circulant graphs

Determining the full automorphism group of a graph is a hard problem with a long history. I will discuss some of the major results that involve finding graphs with a given automorphism group. I will then focus on circulant graphs, and describe some structural results and algorithms that help us determine the full automorphism group of the graph. I will also give some asymptotic results about how many circulant graphs fall into different categories.

Arnab Bose (Math and CS, U of Lethbridge) Mar 21, 2016
Investigations on some exponential congruences

Around 1981, Selfridge asked for what positive integers a and b does $2^a - 2^b$ divide $n^a - n^b$ for all $n \in \mathbb{N}$. The problem was independently solved by various people in different contexts. In this talk, we study their ideas and prove a generalization of the problem, in the elementary number theoretic sense and also in algebraic number fields. Further, we develop ideas to give a conditional resolution and generalizations to another problem by H.Ruderman which is closely related to Selfridge's problem.

Brandon Fuller (Math and CS, U of Lethbridge) Apr 4, 2016
CCA groups and graphs

An automorphism of a Cayley graph that preserves its natural edge-colouring is called colour-preserving. We study groups G with the property that every automorphism on every connected Cayley graph on G is the composition of a left-translation and a group automorphism. We call this class of groups CCA groups and we look at classifying which groups are not CCA. More precisely, we look at abelian groups, groups of odd order and direct or semidirect products of groups.

Asif Zaman (University of Toronto, Ontario) Apr 11, 2016
The least prime ideal in the Chebotarev Density Theorem

In 1944, Linnik famously showed unconditionally that the least prime in an arithmetic progression $a(modq)$ with with $(a, q) = 1$ is bounded by q^L for some absolute effective constant $L > 0$, known as "Linnik's constant". Many authors have computed explicit admissible values of L with the current world record at $L = 5$ by Xylouris (2011), refining techniques of Heath-Brown (1992). We consider a broad generalization of this problem in the Chebotarev Density Theorem (CDT), which is concerned with the splitting behaviour of prime ideals in number fields. Namely, what is the least norm of a prime ideal occurring in CDT. Papers of Lagarias-Montgomery-Odlyzko (1979) and Weiss (1983) give different unconditional field-uniform bounds but without any explicit exponents analogous to the subsequent work on Linnik's constant. I will report on our recent work establishing such explicit estimates along with some applications related to primes represented by binary integral quadratic forms and congruences for Fourier coefficients of cuspidal Hecke eigenforms. This is joint work with Jesse Thorner.

Ram Murty (Queen's University, Ontario) June 17, 2016
Twin primes

We will discuss recent progress towards the twin prime conjecture as well as highlight some recent joint work with Akshaa Vatwani the connects the parity problem with the twin prime conjecture. The talk will be accessible to a wide audience.

Tim Trudgian (Australian National University) June 28, 2016
Grosswald's conjecture on primitive roots

Very little is known about the distribution of primitive roots of a prime p. Grosswald conjectured that the least primitive root of a prime p is less than $\sqrt{p} - 2$ for all $p > 409$. While this is certainly true for all p sufficiently large, Grosswald's conjecture in still open. I shall outline some recent work which resolves the conjecture completely under the Generalised Riemann Hypothesis and which almost resolves the conjecture unconditionally.

Vijay Patankar (Jawaharlal Nehru University, India) June 28, 2016

Pairs of elliptic curves and their Frobenius fields

Given an elliptic curve E over a number field K . The Frobenius field attached to E at a prime p is the splitting field of the characteristic polynomial of the Frobenius endomorphism acting on the ℓ-adic Tate module of E (ℓ a prime different from p) over the rationals. Thus, the splitting field is either of degree 1 or degree 2 over the rationals. Let E_1 and E_2 be elliptic curves defined over a number field K, with at least one of them without complex multiplication. We prove that the set of places v of K of good reduction such that the corresponding Frobenius fields are equal has positive upper density if and only if E_1 and E_2 are isogenous over some extension of K. For an elliptic curve E defined over a number field K, we show that the set of finite places of K such that the Frobenius field at v equals a fixed imaginary quadratic field F has positive upper density if and only if E has complex multiplication by F. Time permits we will provide a sketch of a result about two dimensional ℓ-adic Galois representations that we will need using an algebraic density theorem due to Rajan.

Fall 2015

Open problem session Sept 14, 2015

Please bring your favourite (math) problems. Anyone with a problem to share will be given about 5 minutes to present it. We will also choose most of the speakers for the rest of the semester.

Amy Feaver (King's University, Alberta) Sept 21, 2015
A two-part talk on (1) Sage mathematics software and (2) multiquadratic fields

This talk will be in two parts. It will begin with a short discussion of recent developments in the Sage Mathematics Software and some of the implications these developments may have for research in number theory world-wide. The second portion of this talk will focus on the structure of multiquadratic number fields, what we do and do not know about their integral bases, and how this knowledge may extend to understanding other rings of integers.

Dave Morris (Math and CS, U of Lethbridge) Sept 28, 2015
What is a superrigid subgroup?

In combinatorial geometry (and engineering), it is important to know that certain scaffold-like geometric structures are rigid. (They will not collapse, and, in fact, have enough bracing that they cannot be deformed at all.) Replacing the geometric structure with an algebraic structure (namely, a group) leads to the following question: given a homomorphism that is defined on the elements of a subgroup, is it possible to extrapolate the homomorphism to the rest of the elements of the group? It is fairly obvious that every additive homomorphism from the group $\mathbb{Z}$ of integers to the real line $\mathbb{R}$ can be extended to a homomorphism that is defined on all of $\mathbb{R}$, and we will see some other examples.

Alexev Popov (Math and CS, U of Lethbridge) Oct 5, 2015
Every operator has almost-invariant subspaces

It a classical open problem in Operator Theory whether every bounded linear operator T on a Hilbert space H has a non-trivial invariant subspace (that is, a subspace Y of H such that TY is contained in Y; nontrivial means not $\{0\}$ and not H). This is called the Invariant Subspace Problem; it is almost 100 years old. In this talk we will show that any bounded operator on an infinite-dimensional Hilbert space admits a rank one perturbation which has an invariant subspace of infinite dimension and co-dimension. Moreover, the norm of the perturbation can be chosen as small as needed. This is a joint work with Adi Tcaciuc.

Alia Hamieh (Math and CS, U of Lethbridge) Oct 19, 2015
Special values of Rankin-Selberg L-functions

In this talk, we discuss some results on the non-vanishing in p-adic families of the central values of certain Rankin-Selberg L-functions (namely, anticyclotomic twists of L-functions) associated to automorphic forms on $GL(2)$.

Farzad Aryan (Math and CS, U of Lethbridge) Oct 26, 2015
Gaps between zeros of the Riemann zeta function

The Riemann Hypothesis predicts that all zeros of the Riemann zeta function are located on the line $\Re(s) = \frac{1}{2}$ Also, we have that the number of zeros with imaginary parts located between T and $2T$ is approximately $\frac{T}{2\pi}\log T$. Therefore the average gap is about $\frac{2\pi}{\log T}$. It has been conjectured that there are gaps that are smaller than $\frac{2\pi c}{\log T}$, for every $c > 0$. This has been proven for c slightly larger than $\frac{1}{2}$. Proving that c can be taken less than $\frac{1}{2}$ seems to be a very hard problem, despite being far from the conjecture. In this talk we discuss the connection between Chowla's conjecture on the shifted convolution sums of the Liouville's function and the size of c.

Nathan Ng (Math and CS, U of Lethbridge) Nov 2, 2015
The autocorrelation of a multiplicative function

Let h be a natural number and f an arithmetic function. The autocorrelation of f is the sum

$$C_f(x,h) = \sum_{n\leq x} f(n)f(n+h).$$

Such sums play an important role in analytic number theory. For instance, consider the classical arithmetic functions $\Lambda(n)$ (the von Mangoldt function), $\lambda(n)$ (Liouville's function), and $\tau_k(n)$ (the k-th divisor function). The sums $C_\Lambda(x,h)$, $C_\lambda(x,h)$, and $C_{\tau_k}(x,h)$ are related to the Twin Prime Conjecture, Chowla's conjecture, and to the moments of the Riemann zeta function, respectively. In this talk I will present a heuristic probabilistic method for deriving a conjecture for $C_f(x,h)$ in the case f is a multiplicative function.

Amir Akbary (Math and CS, U of Lethbridge) Nov 6, 2015
Lang-Trotter Revisited

For a prime p, let $n(p)$ be the number of solutions (x,y) of $y^2 = x^3 + ax + b$ over the finite field $\mathbb{F}_p$ and let $a(p) = p - n(p)$. In 1976, Serge Lang and Hale Trotter formulated a conjecture regarding the distribution of primes p for which $a(p) = A$ for a fixed integer A. In this talk we give an exposition of this conjecture as it is given in the introduction of a paper of Katz (N. Katz, Lang-Trotter Revisited, Bulletin of the AMS, Vol. 46, No. 3, July 2009, pp. 413–457).

Mohammad Bardestani (University of Ottawa, Ontario) Nov 23, 2015
Isotropic quadratic forms and the Borel chromatic number of quadratic graphs

For a field F and a quadratic form Q defined on an n-dimensional vector space V over F, let over F, let G_Q, called the quadratic graph associated to Q, be the graph with the vertex set V where vertices v, w in V form an edge if and only if $Q(v-w) = 1$. Quadratic graphs can be viewed as natural generalizations of the unit-distance graph featuring in the famous Hadwiger-Nelson problem. In the present talk, we will prove that for a local field F of characteristic zero, the Borel chromatic number of G_Q is infinite if and only if Q represents zero non-trivially over F.The proof employs a recent spectral bound for the Borel chromatic number of Cayley graphs, combined with an analysis of certain oscillatory integrals over local fields. As an application, we will also answer a variant of question 525 proposed in the 22nd British Combinatorics Conference 2009.

Habiba Kadiri (Math and CS, U of Lethbridge) Nov 30, 2015

Explicit bounds for $\psi(x;q,a)$

The prime number theorem in arithmetic progressions establishes that, for a and q fixed coprime integers, then $\psi(x;q,a)$ is asymptotic to $\frac{x}{\phi(q)}$ when x is large. We discuss new explicit bounds for the error term $\left|\frac{\psi(x;q,a)-\frac{x}{\phi(q)}}{\frac{x}{\phi(q)}}\right|$, which provide an extension and improvement over the previous work of Ramaré and Rumely. Such results depend on the zeros of the Dirichlet L-functions: a numerical verification of the Generalized Riemann Hypothesis up to a given height and explicit zero-free regions. We use the latest results of respectively Platt and Kadiri. In addition our method makes use of smooth weights. This is joint work with Allysa Lumley.

Joy Morris (Math and CS, U of Lethbridge) Dec 7, 2015

Colour-permuting and colour-preserving automorphisms

A Cayley graph $Cay(G;S)$ on a group G with connection set $S = S^{-1}$ is the graph whose vertices are the elements of G, with $g \sim h$ if and only if $g^{-1}h \in S$. If we assign a colour $c(s)$ to each $s \in S$ so that $c(s) = c(s^{-1})$ and $c(s) \neq c(s')$ when $s' \neq s, s^{-1}$, this is a natural (but not proper) edge-colouring of the Cayley graph. The most natural automorphisms of any Cayley graph are those that come directly from the group structure: left-multiplication by any element of G; and group automorphisms of G that fix S setwise. It is easy to see that these graph automorphisms either preserve or permute the colours in the natural edge-colouring defined above. Conversely, we can ask: if a graph automorphism preserves or permutes the colours in this natural edge-colouring, need it come from the group structure in one of these two ways? I will show that in general, the answer to this question is no. I will explore the answer to this question for a variety of families of groups and of Cayley graphs on these groups. I will touch on work by other authors that explores similar questions coming from closely-related colourings. This is based on joint work with Ademir Hujdurovič, Klavdija Kutnar, and Dave Witte Morris.

Spring 2015

Open problem session Jan 12, 2015

Please bring your favourite (math) problems. Anyone with a problem to share will be given about 5 minutes to present it. We will also choose most of the speakers for the rest of the semester.

Nathan Ng (Math and CS, U of Lethbridge) Jan 19, 2015
A subconvexity bound for modular L-functions

Let $L(s)$ be the L-function associated to a modular form of weight k for the full modular group. Using spectral theory, Anton Good proved that $L(k/2+it)?t^{\frac{1}{3}}(\log t)^{\frac{5}{6}}$. Matti Jutila discovered a simpler proof which makes use of the Voronoi summation formula, exponential integrals, and Farey fractions. We shall present Jutila's argument.

Nathan Ng (Math and CS, U of Lethbridge) Jan 26, 2015
A subconvexity bound for modular L-functions, part 2

This is a continuation of last week's talk. I will sketch Matti Jutila's proof of a subconvex bound for a modular L-function on the critical line. The main ideas are an approximate functional equation, the use of Farey fractions, Voronoi's summation formula, and exponential integral and sum estimates.

Nathan Ng (Math and CS, U of Lethbridge) Feb 9, 2015
Gaps between the zeros of the Riemann zeta function

In this talk we will show how to exhibit large and small gaps between the zeros of the Riemann zeta function, assuming the Riemann hypothesis. This is based on a technique of Montgomery and Odlyzko. The problem of finding small gaps between the zeros leads to a very interesting optimization problem.

Gabriel Verret (University of Western Australia) Feb 23, 2015
Automorphism groups of vertex transitive graphs

No abstract available.

Peter J. Cho (University of Buffalo, New York) Mar 11, 2015
Zeros of L-functions

In 20th century, one of the most striking discoveries in number theory is Montgomery's pair-correlation. It says that pair-correlation of zeros of the Riemann zeta function is the same with that of eigenvalues of unitary matrices. In 1990's, Rudnick, Katz and Sarnak studied the zeros of L-functions more systematically. Moreover, Katz and Sarnak proposed the n-level density conjecture which claims that distributions of low-lying zeros of L-functions in a family is predicted by one of compact matrix groups, which are $U(N)$, $SO(even)$, $SO(odd)$, $O(N)$, and $Sp(2N)$. At the end of the talk, I will state an n-level density theorem for some families of Artin L-functions and talk about counting number fields with local conditions. I will start with a friendly definition of L-functions and give some examples. No background or knowledge for L-functions are required for this talk.

Daniel Vallieres (Binghamton University, New York) Mar 13, 2015
Abelian Artin L-functions at zero

In the early 1970s, Harold Stark formulated a conjecture about the first non-vanishing Taylor coefficient at zero of Artin L-functions. About 10 years later, he refined his conjecture for abelian L-functions having order of vanishing one at zero, under certain hypotheses. In 1996, Karl Rubin extended this last refinement of Stark to the higher order of vanishing setting. In this expository talk for a general audience, we will give a survey of this area of research and present a more general conjecture, which we formulated in the past few years. At the end, we will present evidence for our conjecture and indicate one possible direction for further research.

Tristan Freiberg (University of Missouri) Mar 23, 2015
Square totients

A well-known conjecture asserts that there are infinitely many primes p for which $p-1$ is a perfect square. We obtain upper and lower bounds of matching order on the number of pairs of distinct primes $p, q \leq x$ for which $(p-1)(q-1)$ is a perfect square. This is joint work with Carl Pomerance (Dartmouth College).

Ram Murty (Queen's University, Ontario) May 8, 2015
Consecutive squarefull numbers

A number n is called squarefull if for every prime p dividing n, we have p^2 also dividing n. Erdos conjectured that the number of pairs of consecutive squarefull numbers $(n, n+1)$ with $n < N$ is at most $(\log N)^A$ for some $A > 0$. This conjecture is still open. We will show that the abc conjecture implies this number is at most N^ε for any $\varepsilon > 0$. We will also discuss a related conjecture of Ankeny, Artin and Chowla on fundamental units of certain real quadratic fields and discuss its connection with the Erdos conjecture. This is joint work with Kevser Aktas.

Adam Felix (KTH Royal Institute of Technology, Sweden) June 1, 2015
How close is the order of a mod p to $p-1$?

Let $a \in \mathbb{Z}\backslash\{0, \pm 1\}$, and let $f_a(p)$ denote the order of a modulo p, where $p \nmid a$ is prime. There are many results that suggest $p-1$ and $f_a(p)$ are close. For example, Artin's conjecture and Hooley's subsequent proof upon the Generalized Riemann Hypothesis. We will examine questions related to the relationship between $p-1$ and $f_a(p)$.

Darcy Best (Monash University, Australia) June 15, 2015
Finding long transversals in Latin squares

A transversal of a latin square of order n is a subset of entries picked in such a way that each row, each column and each symbol is present at most once. In many latin squares, you can find a full transversal by selecting n entries which do not duplicate any row, column or symbol. But what about when you can't find a full transversal? Brualdi has conjectured that a transversal of length n?1 is always present in any latin square. In this talk, we will discuss recent work which shows that for small orders, Brualdi's conjecture holds. Moreover, we show that his conjecture also holds for small generalized latin squares as well.

Anders Södergren (University of Copenhagen, Denmark) Aug 6, 2015
Low-lying zeros of Artin L-functions

In this talk we discuss the distribution of low-lying zeros of certain families of Artin L-functions attached to geometric parametrizations of number fields. We describe several explicit examples of such families and in each case we present the symmetry type of the distribution of low-lying zeros. This is joint work with Arul Shankar and Nicolas Templier.

Daniel Fiorilli (University of Ottawa, Ontario) Aug 6, 2015
On Vaughan's approximation

I will discuss Vaughan's approximation to the number of primes in arithmetic progressions. In particular, I will show that on average over large moduli, it is far superior to the usual approximation.

Fall 2014

Open problem session Sept 8, 2014

Please bring your favourite (math) problems. Anyone with a problem to share will be given about 5 minutes to present it. We will also choose most of the speakers for the rest of the semester.

Joy Morris (Math and CS, U of Lethbridge) Sept 15, 2014
Colour-permuting automorphisms of Cayley graphs

A Cayley graph $\mathrm{Cay}(G;S)$ has the elements of G as its vertices, with $g \sim gs$ if and only if $s \in S$. There is a natural colouring of the edges of any such graph, by assigning colour s to an edge if it came from the element s of S. For a Cayley digraph, any graph automorphism that preserves this colouring has to be a group automorphism of G. For a Cayley graph, this is not the case. I will present examples of Cayley graphs that have automorphisms that do not correspond to group automorphisms of G. I will also show that for some families of groups, such examples are not possible. I will also discuss the more general problem of automorphisms that permute the colours, rather than necessarily preserving all of them.

Farzad Aryan (Math and CS, U of Lethbridge) Sept 22, 2014
On binary and quadratic divisor problem

Let $d(n) = \sum_{d|n} 1$. This is known as the divisor function. It counts the number of divisors of an integer. Consider the following shifted convolution sum

$$\sum_{an-m=h} d(n)d(m)f(an,m),$$

where f is a smooth function which is supported on $[x,2x]\times[x,2x]$ and oscillates mildly. In 1993, Duke, Friedlander, and Iwaniec proved that

$$\sum_{an-m=h} d(n)d(m)f(an,m) = \text{Main term}(x) + O(x^{0.75}).$$

Here, we improve (unconditionally) the error term in the above formula to $O(x^{0.61})$, and conditionally, under the assumption of the Ramanujan-Petersson conjecture, to $O(x^{0.5})$. We will also give some new results on shifted convolution sums of functions coming from Fourier coefficients of modular forms.

Adam Tyler Felix (Math and CS, U of Lethbridge) Sept 29, 2014
Common divisors of the index and order of a modulo p

We study the distribution of primes for which the index and order of a modulo p have a fixed common divisor. We will also motivate this problem through previously known results related to Artin's conjecture for primitive roots.

Nathan Ng (Math and CS, U of Lethbridge) Oct 6, 2014
Inclusive prime number races

Let $\pi(x; q, a)$ denote the number of primes up to x that are congruent to $a (\mathrm{mod}\ q)$. A "prime number race", for fixed modulus q and residue classes $a_1, \dots, a_r$, investigates the system of inequalities

$$\pi(x; q, a_1) > \pi(x; q, a_2) > \cdots > \pi(x; q, a_r).$$

We expect that this system should have arbitrarily large solutions x, and moreover we expect the same to be true no matter how we permute the residue classes aj; if this is the case, the prime number race is called "inclusive". Rubinstein and Sarnak proved conditionally that every prime number race is inclusive; they assumed not only the generalized Riemann hypothesis but also a strong statement about the linear independence of the zeros of Dirichlet L-functions. We show that the same conclusion can be reached with a substantially weaker linear independence hypothesis. This is joint work with Greg Martin.

Sean Fitzpatrick (Math and CS, U of Lethbridge) Oct 20, 2014
Characters of induced representations

Let G be a compact semisimple Lie group, and let H be a closed subgroup of G. Given a linear representation $\tau : H \to \mathrm{End}(V)$ of H, one can form an associated vector bundle $\mathcal{V}_\tau : \tau \to G/H$ over the homogeneous space G/H, and define an induced representation of G on the space of L^2 sections of $\mathcal{V}_\tau$, after the method of Frobenius. Despite the resulting representation of G being infinite-dimensional, Berline and Vergne showed that it is possible to give a formula for its character. If we assume that H is a maximal torus in G, then G/H is a complex manifold, and the vector bundle $\mathcal{V}_\tau$ can be equipped with a holomorphic structure. In this case one can define the holomorphic induced representation of G by restricting to the space of holomorphic sections of $\mathcal{V}_\tau$, which is a finite-dimensional vector space. We'll show that both extremes can be viewed as special cases of a family of induced representations, whose characters can be computed as the index of a transversally elliptic operator on the homogeneous space G/H.

Kevin Henriot (University of British Columbia) Oct 27, 2014
Linear equations in dense subsets of the squares.

We discuss the solvability of certain linear equations in sparse subsets of the squares. Specifically, we investigate equations of the form

$$\lambda_1 n_1^2 + \cdots + \lambda_s n_s^2 = 0,$$

where $s \geq 7$ and the coefficients λ_i sum to zero and satisfy certain sign conditions. We show that such equations admit non-trivial solutions in any subset of $[N]$ of density $(\log N)^{-c_s}$, improving upon the previous best of $(\log \log N)^{-c}$.

Amir Akbary (Math and CS, U of Lethbridge) Nov 3, 2014
Heuristics for some conjectural constants

We describe heuristics for several well-known density conjectures in prime number theory and elliptic curves theory. In each case we show how one can arrive at explicit expressions for density constants. The conjectures include twin prime conjecture, Bateman-Horn conjecture, Artin's primitive root conjecture, and Koblitz-Zywina conjecture.

James Parks (Math and CS, U of Lethbridge) Nov 10, 2014
Averages of the number of points on elliptic curves

Let E be an elliptic curve defined over $\mathbb{Q}$. Let $M_E(N)$ be the function that counts the number of primes p of good reduction such that $\#E_(\mathbb{F}_p) = N$ where N is a fixed integer and $E_(\mathbb{F}_p)$ denotes the group of points on the elliptic curve modulo p. We consider this function on average and discuss recent results related to the constant in the asymptotic result in the average.

Manoj Kumar (Math and CS, U of Lethbridge) Nov 17, 2014
The signs in an elliptic net

Let R be an integral domain and let A be a finitely generated free abelian group. An elliptic net is a map $W\colon A \to R$ with $W(0) = 0$, and such that for all $p, q, r, s \in A$,

$$\begin{aligned} &W(p+q+s)W(p-q)W(r+s)W(r) \\ &\quad + W(q+r+s)W(q-r)W(p+s)W(p) \\ &\qquad + W(r+p+s)W(r-p)W(q+s)W(q) \\ &\quad = 0. \end{aligned}$$

In this talk we will give a formula to compute the sign of any term of an elliptic net without actually computing the value of that term.

Soroosh Yazdani (Google, Waterloo, Ontario) Nov 21, 2014
Belyi maps and Diophantine equations

In 1979 G. Belyi proved that given any smooth curve C over any number field, there is map $\beta : C \to \mathbb{P}_1$ such that β is unramified outside of three points. This is particularly striking since Belyi's theorem is not true over complex numbers, and hence it is an arithmetic result as much as it is a geometric result. In this talk I will give a brief explanation for the proof of this theorem and explain how this theorem can be used to relate arithmetic geometry problems to the ABC conjecture.

Dave Morris (Math and CS, U of Lethbridge) Dec 1, 2014
Introduction to arithmetic groups

We will discuss a few basic properties of "arithmetic groups," which are certain groups of $n \times n$ matrices with integer entries. By definition, the subject combines algebra (group theory and matrices) with number theory (the integers), but it also has connections with other areas, including the theory of periodic tilings. To learn more about these interesting groups, download a free copy of my book from http://arxiv.org/src/math/0106063/anc/

Spring 2014

Open problem session Jan 13, 2014

Please bring your favourite (math) problems. Anyone with a problem to share will be given about 5 minutes to present it. We will also choose most of the speakers for the rest of the semester.

Eric Naslund (Princeton University, New Jersey) Jan 20, 2014
A density increment approach to Roth's theorem in the primes

By combining Green and Tao's transference principle with a density increment argument, we show if A is a set of prime numbers satisfying $\sum_{a\in A}\frac{1}{a}=\infty$, then A must contain a 3 term arithmetic progression. The previous methods of Helfgott and De Roton, and the speaker, used the transference principle to move from a set of primes to a dense subset of integers by considering the L^2 and L^p-norms of a smoothed version of the indicator function of A. Instead, we work directly with the L^∞-norm, and exploit the structure of A to obtain increased density on a large subprogression when A contains no arithmetic progressions. By iterating we show that for any constant $B>0$, if A is a subset of primes contained in $\{1,\dots,N\}$ with size at least $|A|\gg_B \frac{N}{\log N(\log\log N)^B}$, then A contains a three term arithmetic progression.

Mohammadreza Jooyandeh (Australian National University) Jan 27, 2014
Recursive algorithms for generation of planar graphs

In this talk we introduce recursive algorithms for generation of three families of plane graphs. These algorithms start with small graphs and iteratively convert them to larger graphs. The families are k-angulations (plane graphs with whose faces are of size k), plane graphs with a given face size sequence and planar hypohamiltonian graphs. Hypohamiltonian graphs have the property that removing each vertex from the graph, there is a Hamiltonian cycle through all remaining vertices while the original graph does not have any such cycle. One of the problems in the literature since 1976 is to find the smallest planar hypohamiltonian graphs. The previous record by Weiner and Araya was a planar graph with 42 vertices. We improve this record by finding 25 planar hypohamiltonian graphs on 40 vertices while discovering many larger ones on 42 and 43 vertices. We also introduce a very fast method for canonical embedding and isomorphism rejection of plane graphs. Most graph generators like plantri generate graphs isomorph-free up to isomorphism of the embedding, however our method does the isomorphism checking up to the underlining graph while taking advantage of the planarity and embeddings to speed up the computation.

David Roe (University of Calgary, Alberta) Feb 3, 2014
Numerical methods in p-adic linear algebra

Standard numerical methods focus on algorithms for matrices over the real and complex numbers: finding singular value decompositions, eigenvalues and eigenvectors, QR and LU decompositions. Many of the same questions make sense for non-archimedian local fields, and some methods carry over. Moreover, the ultrametric properties of p-adic arithmetic allow for much better tracking of precision than in the real and complex cases. This is a report on early stages of joint work with Xavier Caruso, Tristan Vaccon, Jen Balakrishnan and Kiran Kedlaya.

Joy Morris (Math and CS, U of Lethbridge) Feb 10, 2014
Automorphisms of Cayley graphs that respect partitions

A Cayley graph $\Gamma = Cay(G; S)$ on a group G with connection set S, is a graph whose vertices are labelled with the elements of G, with vertices g_1 and g_2 adjacent if $g_1^{-1}g_2 \in S$. We say that an automorphism α of Γ respects the partition $\mathcal{C}$ of the edge set of Γ if for every $C \in \mathcal{C}$, we have $\alpha(C) \in \mathcal{C}$. I will discuss some obvious partitions of the edge set of a Cayley graph Γ, and find conditions under which a graph automorphism of Γ that respects these partitions and fixes a vertex, must be an automorphism of the group G.

Olivier Ramaré (CNRS and Université de Lille 1, France) Feb 24, 2014
Bilinear forms on prime numbers

This talk will retrace the main steps of the modern theory of prime numbers and in particular how the combinatorial sieve combined with the Dirichlet series theory to give birth to the modern representation of the primes via a linear combination of terms, some of which being "linear", while the other ones are "bilinear". This will lead us to the recent developments of Green and Tao, Mauduit and Rivat, Tao, Helfgott, and Bourgain, Sarnak and Ziegler.

Daniel Fiorilli (University of Michigan) Mar 3, 2014
Nuclear physics and number theory

While the two fields named in the title seem unrelated, there is a strong link between them. Indeed, random matrix theory makes predictions in both fields, and some of these predictions can be verified rigorously on the number theory side. This amazing connection came to life during a meeting between Freeman Dyson and Hugh Montgomery at the Institute for Advanced Study. Random matrices are now known to predict many statistics about zeta functions, such as moments, low-lying zeros and correlations between zeros. The goal of this talk is to discuss this connection, focusing on number theory. We will cover both basic facts about the zeta functions and recent developments in this active area of research.

Amir Akbary (Math and CS, U of Lethbridge) Mar 10, 2014
Introduction to the ABC Conjecture

We will describe the celebrated ABC conjecture, due to Oesterle and Masser, formulated in 1985. We will explain one of the motivations behind this conjecture and discuss a refinement of this conjecture put forward by Baker in 1996.

Hadi Kharaghani (Math and CS, U of Lethbridge) Mar 17, 2014
Difference matrices and applications

Let $(G, \odot)$ be a group of order g. A $(g, k; \lambda)$- difference matrix is a $k \times g\lambda$ matrix $D = (d_{ij})$ with entries from G, so that for each $1 \leq i < j \leq k$, the multiset

$$\{d_{il} \odot d_{jl}^{-1} : 1 \leq l \leq g\lambda\}$$

(the difference list) contains every element of $G\lambda$ times. A generalized Hadamard matrix $GH(g, \lambda)$ is a $(g, g\lambda; \lambda)$-difference matrix. Some interesting examples of difference matrices and generalized Hadamard matrices with emphasis on their applications will be discussed.

Ted Dobson (Mississippi State University) Mar 24, 2014
On Cayley Numbers

In 1983, Marušič posed the problem of determining which positive integers n have the property that every vertex-transitive graph of order n is isomorphic to a Cayley graph of some group. Such an integer n is called a Cayley number. Much work on this problem has been done, and, for example, it is known exactly which integers divisible by a square are Cayley numbers. These are p^2, p^3, and 12. Additionally, a fair amount is known via constructions about which square-free integers are not Cayley numbers. Much less is known about which square-free integers are Cayley numbers, and it is not even known if there is a Cayley number that is a product of five distinct primes. We answer a question posed by C. Praeger who asked if there was a Cayley number of order n where n has k distinct prime factors for every positive integer k. We construct an infinite set of distinct prime numbers S with the property that the product of any k elements of S is always a Cayley number. This is joint work with Pablo Spiga.

Allysa Lumley (Math and CS, U of Lethbridge) Mar 31, 2014
New bounds for $\psi(x; q, a)$

Let a, q be relatively prime integers. Then consider

$$\psi(x; q, a) = \sum_{\substack{n \leq x \\ n \equiv a (\bmod q}} \Lambda(n).$$

We discuss new explicit bounds for $\psi(x; q, a)$, which provide an extension and improvement over the bounds given in the previous work of Ramaré and Rumely. This article introduces two new ideas. We smooth the prime counting function and use the partial verification of GRH by Platt along with an explicit zero-free region given by Kadiri. This is joint work with Habiba Kadiri.

James Parks (Math and CS, U of Lethbridge) Apr 7, 2014
Amicable pairs and aliquot cycles on average

Let E be an elliptic curve defined over $\mathbb{Q}$. A pair (p, q) of distinct prime numbers is called an amicable pair of E if E has good reduction at p and q and $\#E_p(\mathbb{F}_p) = q$ and $\#E_q(\mathbb{F}_q) = p$. In this talk we show a non-trivial upper bound for the number of amicable pairs on average over a family of elliptic curves.

Soroosh Yazdani (Math and CS, U of Lethbridge) Apr 14, 2014

Modular curves and moduli problems

Modular curves are the parameter space of elliptic curves with certain torsion structure. In this talk, I will explain what that sentence means, and how it is related to the usual definition of modular curves in terms of quotients of the complex upper half plane with certain matrix groups.

Fall 2013

Open problem session Sept 9, 2013

Please bring your favourite (math) problems. Anyone with a problem to share will be given about 5 minutes to present it. We will also choose most of the speakers for the rest of the semester.

Farzad Aryan (Math and CS, U of Lethbridge) Sept 16, 2013
On distribution of squares modulo a composite number q

A natural number s is said to be a square modulo a composite number q if it is a square modulo each of the prime numbers dividing q. Let p be a prime number, then

$$\text{Prob}(s \text{ is a square mod } p) = p + \frac{1}{2p} \approx \frac{1}{2}.$$

Roughly speaking, the probability of a number to be a square modulo q is $\frac{1}{2^{\omega(q)}}$, where $\omega(q)$ is the number of prime divisors of q.

Fix h and let $X : \{1, 2, \ldots, q\} \to \mathbb{N}$ be a random variable, given by

$$X(i) = \#\{s \in [i, i+h] \ : \ s \text{ is a square modulo } q\}.$$

For the mean, we have $E(X) \approx \frac{h}{2^{\omega(q)}}$, and, in this talk, we show the following bound for the variance: $Var(X) \leq E(X) \approx \frac{h}{2^{\omega(q)}}$.

Nathan Ng (Math and CS, U of Lethbridge) Sept 23, 2013
Zhang's theorem on bounded gaps between primes

In Apr 2013, Yitang Zhang announced one of the great theorems in the history of number theory. He showed there exists an absolute constant C such that infinitely many consecutive primes differ by C. This theorem goes a long way towards proving the twin prime conjecture. In this talk I will give an overview of Zhang's theorem and some of the main ideas in the proof.

Nathan Ng (Math and CS, U of Lethbridge) Sept 30, 2013
Zhang's theorem on bounded gaps between primes, part 2

In this talk, I will focus on the Goldston-Pintz-Yildirim (GPY) method for detecting small gaps between primes. In particular, I will discuss the choice of weight function in their optimization argument and the role of primes in arithmetic progressions. Finally, we will consider the Motohashi-Pintz/Zhang variant of the GPY argument which yields bounded gaps between primes.

Jeff Bleaney (Math and CS, U of Lethbridge) Oct 7, 2013
Symmetries of an elliptic net

In 1948, Morgan Ward introduced the concept of an Elliptic Divisibility Sequence (EDS) as an integer sequence (W_n) which satisfies the recurrence relation

$$W_{m+n}W_{m-n}W_1^2 = W_{m+1}W_{m-1}W_n^2 - W_{n+1}W_{n-1}W_m^2,$$

and satisfies the additional property that $W_m \mid W_n$ whenever $m \mid n$. Of particular interest to Ward, were what he called symmetries of an EDS. Ward showed that if (W_n) is an EDS with $W_r = 0$, then we have $W_{r+i} = ab^iW_i$, for some a and b. In her Ph.D. thesis in 2008, Kate Stange generalized the concept of an EDS to an n-dimensional array called an Elliptic Net.

We will discuss the connections between EDS's, Elliptic Nets, and elliptic curves, and give a generalization of Ward's symmetry theorem for elliptic nets.

Adam Felix (Math and CS, U of Lethbridge) Oct 21, 2013
On the distribution of torsion points modulo primes

We will discuss a paper of Chen and Kuan, in which they study the distribution of torsion points modulo primes over several different commutative algebraic groups. They demonstrate that the average is related to some generalized divisor function for these groups.

Dave Morris (Math and CS, U of Lethbridge) Oct 28, 2013
What is a Coxeter group?

Coxeter groups arise in a wide variety of areas, so every mathematician should know some basic facts about them, including their connection to "Dynkin diagrams." Proofs about these "groups generated by reflections" mainly use group theory, geometry, and combinatorics.

Soroosh Yazdani (Math and CS, U of Lethbridge) Nov 4, 2013
Solving S-unit equations

Let S be a finite collection of prime numbers. We say a number is an S-unit if it is a product of powers of primes in S. For instance $-\frac{3}{8}$ is an example of a $\{2,3\}$-unit. Many interesting Diophantine equations are reduced to solving equations of the form $x+y=1$ with x and y both being an S-unit. Using linear forms of logarithms, we can show that there only finitely many solutions to these S-unit equations. In this talk, I will explain an algorithm (due primarily to Smart and Wildanger) on how we can actually enumerate all these solutions.

Patrick Ingram (Colorado State University) Nov 15, 2013
The arithmetic of post-critically finite morphisms

Let f be an endomorphism of N-dimensional projective space. In complex dynamics, it has been known for a century (at least when $N = 1$) that the orbits of the critical points determines much of the dynamics of f. Morphisms for which all of these critical orbits are finite (so-called PCF maps) turn out to be an important class to understand. Thurston proved, when $N = 1$, that there are no algebraic families of PCF maps, except for a small number of easy-to-understand examples. I will discuss some recent research into the arithmetic properties of these maps, as well as a partial extension of Thurston's result to arbitrary dimension.

James Parks (Math and CS, U of Lethbridge) Nov 18, 2013
Distribution conjectures for elliptic curves on average

Let E be an elliptic curve over $\mathbb{Q}$. In this talk we consider several open conjectures about the distribution of local invariants associated with the reductions of E modulo p as p varies over the primes. In order to gain evidence for the conjectures, we consider them on average over a family of elliptic curves.

Habiba Kadiri (Math and CS, U of Lethbridge) Nov 25, 2013
Zero density and primes

In this talk we present some new Chebyshev bounds for the function $\psi(x)$. In 1962, Rosser and Schoenfeld provided a method to estimate the error term in the approximation $|\psi(x)-x|$. Since then, progress on the numerical verification of the Riemann Hypothesis and widening the zero-free region have allowed to improve numerically these bounds. In this talk we present a new method by introducing a smooth weight and by using the first explicit zero density estimate for the Riemann zeta function. We also present new results for primes in short intervals, based on this zero density estimate.

Darcy Best (Math and CS, U of Lethbridge) Dec 2, 2013
Biangular lines

A set of unit vectors $V \subset \mathbb{C}^n$ is called biangular if for any $u, v \in V$, $u \neq v$,

$$|\langle u, v\rangle| \in \{0, \alpha\}$$

for some $0 < \alpha < 1$. There are well-known upper bounds on the size of these sets of vectors. We will discuss these upper bounds, and the implications when they are met, including the generation of combinatorial objects such as strongly regular graphs and association schemes.

Renate Scheidler (University of Calgary, Alberta) Dec 9, 2013
Continued fractions with bounded period length

It is well-known that the continued fraction expansion of a quadratic irrational is horizontally symmetric about its centre. However, an additional vertical symmetry is exhibited by the continued fraction expansions arising from a certain one-parameter family of positive integers known as Schinzel sleepers. This talk provides a method for generating any Schinzel sleeper and investigates their period lengths as well as both their horizontal and vertical symmetries.

This is joint work with Kell Cheng (Hongkong Institute of Education) as well as Richard Guy and Hugh Williams (University of Calgary). The talk is geared toward an audience with a background corresponding to no more than a first number theory course.

Spring 2013

Open problem session Jan 14, 2013

Please bring your favourite (math) problems. Anyone with a problem to share will be given about 5 minutes to present it. We will also choose most of the speakers for the rest of the semester.

Soroosh Yazdani (Math and CS, U of Lethbridge) Jan 21, 2013
Shimura-Taniyama conjecture / modularity theorems – an overview

Shimura-Taniyama conjecture (now known as modularity theorem) states that all rational elliptic curves are modular. Despite its technical sounding statement, this conjecture became famous due to its application to Fermat's last theorem. Thanks the work of Wiles and others, not only we know that all rational elliptic curves are modular, we also know that many other generalizations (for example, Q-curves) are also modular. However, what do we mean by "all rational elliptic curves are modular", and how would one go about proving such a statement?

In this talk I will explain what we mean by modularity of an elliptic curve using Galois representation, and provide some (a.k.a. epsilon amount) hint on how one can prove the modularity theorems.

Hadi Kharaghani (Math and CS, U of Lethbridge) Jan 28, 2013
The asymptotic existence of Hadamard matrices

A square ± 1-matrix with orthogonal rows is called a *Hadamard matrix*. It is conjectured that a Hadamard matrix of order $4n$ exists for each natural number n. A result of Seberry [1976] states that:

For any positive integer p there is a Hadamard matrix of order $2^n p$ for every $n \geq [2\log_2(p-3)]$.

Rob Craigen, while in our department in 1994, improved this result considerably by showing that:

There exists a circulant signed group Hadamard matrix of every even order n, using a suitable signed group. This in turn would imply the existence of Hadamard matrices of order $2^n p$ for every $n \geq 4[(1/6)\log_2\big((p-1)/2\big)] + 2$.

These and other asymptotic results will be discussed.

Nathan Ng (Math and CS, U of Lethbridge) Feb 4, 2013
Error terms and sums of independent random variables

The normalized error term in the prime number theorem is intimately related to the location of the zeros of the zeta function. In 1901, Von Koch proved that the Riemann hypothesis implies that this error term is less than $\log^2 x$. In 1914, Littlewood famously proved that the error term is infinitely often larger than $\log\log\log x$. Which function is closer to the truth? In important work, Montgomery suggested that the truth lies near $(\log\log\log x)^2$. His work depends on modelling the normalizing error term by a sum of independent random variables. He then derives sharp estimates for large deviations of this sum of independent random variables. I will attempt to explain the main ideas behind his conjecture.

Adam Felix (Math and CS, U of Lethbridge) Feb 11, 2013
Artin's Conjecture on primitive roots

A primitive root modulo a prime p is an integer which generates the group of non-zero residues modulo p. For primes p, we can always find a primitive root modulo p. In 1927, Artin conjectured that a density for the set of primes for which a fixed integer is a primitive root modulo p exists. Hooley showed that this is true upon the generalized Riemann hypothesis. I will give two conditional proofs of this result: Hooley's original proof and a proof which generalizes to other problems related to Artin's conjecture.

Soroosh Yazdani (Math and CS, U of Lethbridge) Feb 25, 2013
Chebyshev bias for elliptic curves

Recently, there's been a lot of talk about a result of Fiorilli, relating Chebyshev bias for elliptic curves and ranks of elliptic curves, during coffee hour. At the time of discussion all we had at our disposal was a vague abstract from a talk that Fiorilli gave at AMS in San Diego, so I had a hard time figuring out what was going on. As luck would have it, few weeks ago, I saw a talk of William Stein relating Chebyshev bias and ranks of elliptic curves, and this past week Fiorilli sent a preprint to Farzad. This talk will try to summarize all of these recent developments. In particular, I will describe what we mean by Chebyshev's bias for elliptic curves, and how this bias is related to the (analytic) rank of an elliptic curve.

Dave Morris (Math and CS, U of Lethbridge) Mar 4, 2013
Introduction to vertex-transitive graphs of prime-power order

A graph is *vertex-transitive* if its automorphism group acts transitively on the set of vertices. (In other words, every vertex looks exactly like all of the other vertices.) Such graphs can be very complicated in general, but we will use some group theory to see that they are easy to describe when the number of vertices is assumed to be prime. There are similar results when the number of vertices is the square or cube of a prime, but larger powers are harder to understand.

Farzad Aryan (Math and CS, U of Lethbridge) Mar 11, 2013

On sums and products of integers

Additive combinatorics has recently attracted a lot of attention in the mathematics world. A famous conjecture in this field, known as Erdös and Szemerédi's conjecture, concerns the sums and products of integers. It asserts the following:

Conjecture. *For any fixed $\delta > 0$ the lower bound*

$$\max\{|A+A|, |A\cdot A|\} \gg_\delta |A|^{2-\delta}$$

holds for all finite sets $A \subset \mathbb{Z}$.

Here $A+A = \{a+a' : a, a' \in A\}$ and $A\cdot A = \{aa' : a, a' \in A\}$.

Roughly speaking, the conjecture states that: For a fixed a set of integers, both the sum-set and product-set cannot be small. There are two major achievements towards this conjecture which we discuss during the talk:

(1) Chang in 2003 showed that the sum-set must be large whenever the product-set is sufficiently small. More precisely, she has shown that
$$|A+A| > 36^{-\alpha}|A|^2$$
if $|A\cdot A| < \alpha|A|$ for some constant α.

(2) The best known bound today, achieved by Solymosi, follows from his more general inequality
$$|A+A|^2|A\cdot A| \geq \frac{|A|^4}{2\log|A|}.$$
The Solymosi's result is valid for A a finite subset of the real numbers. From the inequality we have
$$\max\{|A+A|, |A\cdot A|\} \geq \frac{|A|^{4/3}}{2(\log|A|)^{1/3}}.$$

Ebrahim Ghaderpour (Math and CS, U of Lethbridge) Mar 18, 2013

The asymptotic existence of orthogonal designs

A *complex orthogonal design* of order n and type $(s_1, \ldots, s_k)$, denoted $COD(n;\ s_1, \ldots, s_k)$, is a matrix X with entries from $\{0, \epsilon_1 x_1, \ldots, \epsilon_k x_k\}$, where the x_i's are commuting variables and $\epsilon_j \in \{\pm 1, \pm i\}$ for each j, that satisfies

$$XX^* = \left(\sum_{i=1}^{k} s_i x_i^2\right) I_n,$$

where X^* denotes the conjugate transpose of X and I_n is the identity matrix of order n.

A complex orthogonal design in which $\epsilon_j \in \{\pm 1\}$ for all j is called an *orthogonal design*, denoted $OD(n;\ s_1, \ldots, s_k)$. An orthogonal design (=OD) in which there is no zero entry is called a *full* OD. Equating all variables to 1 in any full OD results in a *Hadamard* matrix.

In this seminar, we show that for any n-tuple $(s_1, \ldots, s_k)$ of positive integers, there exists an integer N such that for each $n \geq N$, there is an $OD\Big(2^n(s_1 + \cdots + s_k); 2^n s_1, \ldots, 2^n s_k\Big)$. This is a joint work with professor Hadi Kharaghani.

Amir Akbary (Math and CS, U of Lethbridge) Mar 25, 2013

Sets of multiples

For a subset S of natural numbers we consider its set of multiples $M(S)$. So

$$M(S) = \{ms;\ m \in \mathbb{N}, s \in S\}.$$

In many cases we can see that $M(S)$ has an asymptotic density $\delta(M(S))$. For example if $S = \{2, 3\}$ then $\delta(M(S)) = 2/3$.

Question. *Is it true that $\delta(M(S))$ exists for any $S \subseteq \mathbb{N}$?*

The following conjecture was formulated around 1930's.

Conjecture. *$\delta(M(S))$ exists for any $S \subseteq \mathbb{N}$.*

By 1934 the answer to the above question was known. In this talk we study this question.

Hadi Kharaghani (Math and CS, U of Lethbridge) Apr 8, 2013

The maximum determinant problem

Consider the set M_n of all matrices of order n with entries -1 and 1. The set $D_n = \{\det(A) : A \in M_n\}$ is a finite subset of integers. The maximum determinant problem deals with α_n; the largest possible value of the set D_n. The study of this (relatively old) problem has led people to some very interesting results and questions in number theory, combinatorics and statistics.

The following inequalities and the cases where equalities are attained will be discussed.

(1) For $n \equiv 0 \pmod 4$, $\alpha_n \leq n^{n/2}$. Equality occurs iff there is a $(1, -1)$-matrix H of order n with $HH^t = nI_n$.
(2) For odd n, $\alpha_n \leq \sqrt{2n-1}\,(n-1)^{(n-1)/2}$. Equality occurs iff there is a $(1, -1)$-matrix A with $AA^t = A^tA = (n-1)I_n + J_n$.
(3) For $n \equiv 2 \pmod 4$, $\alpha_n \leq (2n-2)\,(n-2)^{(n-2)/2}$. Equality occurs iff there is a $(1, -1)$-matrix B with

$$BB^t = B^tB = \begin{pmatrix} M & 0 \\ 0 & M \end{pmatrix},$$

where $M = (n-2)I_{n/2} + 2J_{n/2}$.

Joy Morris (Math and CS, U of Lethbridge) Apr 15, 2013

How big is the automorphism group of a generic circulant (di)graph?

A circulant (di)graph is a (di)graph that can be drawn with its n vertices equally spaced around a circle, in such a way that rotation by $360/n$ degrees is a symmetry. It is not hard to see that in the case of a graph, reflection is also a symmetry, so the automorphism group (the group of all of its symmetry operations) must contain the dihedral group of order $2n$.

I will present results showing that for almost all circulant (di)graphs, these are the only symmetries. I will then look at what we can say about the automorphism group of a circulant (di)graph that has more symmetry than this.

This will draw on work by Babai, Godsil, Dobson, Bhoumik, and myself.

Fall 2012

Open problem session Sept 10, 2012

Please bring your favourite (math) problems. Anyone with a problem to share will be given about 5 minutes to present it. We will also choose most of the speakers for the rest of the semester.

Joy Morris (Math and CS, U of Lethbridge) Sept 17, 2012
Calculating partition numbers

The partition number $p(n)$ is the number of ways that n can be partitioned into a sum of smaller positive integers. At the SIAM Discrete Math conference in June, I attended a plenary talk by Ken Ono of Emory on how to calculate partition numbers. This topic incorporates both combinatorics and number theory. Ken Ono was kind enough to give me a copy of his slides so that I could present this topic in our seminar, and I will be using those slides for this talk.

Amir Akbary (Math and CS, U of Lethbridge) Sept 24, 2012
On a conjecture of Erdös

Let m be an integer bigger than 1 and let $P(m)$ denote the largest prime divisor of m. In 1962, Erdös conjectured that

$$\lim_{n\to\infty} \frac{P(2^n-1)}{n} = \infty.$$

In 2000, Ram Murty and Siman Wong conditionally resolved this conjecture, under the assumption of a celebrated conjecture in number theory. In this talk I will describe their work.

Dave Morris (Math and CS, U of Lethbridge) Oct 1, 2012
Hamiltonian paths in solvable Cayley digraphs

Cayley graphs are very nice graphs that are constructed from finite groups. If the group is abelian, then it is easy to show that the graph has a hamiltonian cycle. It is conjectured that the nonabelian Cayley graphs also have hamiltonian cycles.

We will discuss a few recent results (both positive and negative) on the related problem where the graph is replaced by a directed graph, and the finite group is assumed to be solvable (which means it is not too far from being abelian).

Soroosh Yazdani (Math and CS, U of Lethbridge) Oct 15, 2012
Local Szpiro conjecture

The Szpiro conjecture is one of the big conjectures in number theory and Diophantine equations. It is equivalent to the ABC conjecture, and so it implies many interesting results. In this talk I will mention a conjecture that is motivated by the Szpiro conjecture, which seems much less strong than the Szpiro conjecture, even though it still has many interesting Diophantine applications. We will also present a few cases where we can prove this conjecture.

Nathan Ng (Math and CS, U of Lethbridge) Oct 22, 2012
Additive divisor sums

The divisor function $d(n)$ equals the number of divisors of an integer n. In this talk I will discuss what is known about additive divisor sums of the shape

$$D(N,r) = \sum_{n \leq N} d(n)d(n+r)$$

where r is a fixed positive integer. These sums were introduced by Ingham in 1926, who proved an upper bound for $D(N,r)$. This was later refined to an asymptotic formula by Estermann and over the years was further sharpened by a succession of authors, including Heath-Brown, Deshouilliers and Iwaniec, Motohashi, and Meurman. More recent evaluations of $D(N,r)$ makes use of the spectral theory of automorphic forms. I will also discuss more general additive divisor sums of the shape

$$D_k(N,r) = \sum_{n \leq N} d_k(n)d_k(n+r)$$

where k is a natural number larger than 2 and where $d_k(n)$ equals the number of ordered k-tuples $(n_1, \ldots, n_k)$ such that $n = n_1 \cdots n_k$.

Majid Shahabi (Math and CS, U of Lethbridge) Oct 29, 2012
Weil conjectures

In 1949, Weil proposed a set of conjectures about the generating functions which are derived from counting the number of points on an algebraic variety over a finite field. Solving Weil's conjectures was one of the central mathematics projects of the twentieth century. These problems were totally solved by a group of people including Dwork, Grothendieck, and Deligne.

In this talk, we present a historical background and state the assertions of Weil conjectures. We further explain some sentences about the ideas of the proofs.

Farzad Aryan (Math and CS, U of Lethbridge) Nov 5, 2012

The distribution of k-tuples of reduced residues

Let q be a natural number, and write $P = \varphi(q)/q$, that is P is the probability that a randomly chosen integer is relatively prime to q. Let

$$1 = a_1 < a_2 < \cdots < a_{\phi(q)} < q$$

be the reduced residues mod q (integers co-prime to q in increasing order). A quantity of central interest is

$$V_\gamma(q) = \sum_{i=1}^{\phi(q)} (a_{i+1} - a_i)^\gamma.$$

In 1940, Erdős conjectured that

$$V_\gamma(q) \ll qP^{1-\gamma}.$$

Let $\mathcal{D} = \{h_1, h_2, \cdots, h_s\}$ be an admissible set. We call $a+h_1, \ldots, a+h_s$ an s-tuple of reduced residues, if each of these numbers is co-prime with q. Study of s-tuples of reduced residues is an analogue to the study of s-tuples of primes. In this talk we prove estimates about the distribution of s-tuples of reduced residues and finally we prove an extension of Erdős's conjecture for s-tuples:

$$V_\gamma^{\mathcal{D}}(q) := \sum_{a_i < q} (a_{i+1} - a_i)^\gamma \ll qP^{-s(\gamma-1)},$$

where the sum runs over the integers $1 = a_1 < a_2 < \cdots < q$ for which $a_i + h_1, \ldots, a_i + h_s$ is an s-tuple of reduced residues.

Chris Godsil (University of Waterloo, Ontario) Nov 23, 2012

Continuous quantum walks on graphs

If A is the adjacency matrix of a graph X, then the matrix exponential $U(t) = \exp(itA)$ determines what physicists term a continuous quantum walk. They ask questions such as: for which graphs are there vertices a and b and a t such that $|U(t)_{a,b}| = 1$? The basic problem is to relate the physical properties of the system with properties of the underlying graphs, and to study this we make use of results from the theory of graph spectra, number theory, ergodic theory.... My talk will present some of the progress on this topic.

Heinz Bauschke (University of British Columbia – Okanagan) Nov 30, 2012

An Invitation to projection models

Feasibility problems, i.e., finding a solution satisfying certain constraints, are common in mathematics and the natural sciences. If the contraints have simple projectors (nearest point mappings), then one popular approach to these problems is to use the projectors in some algorithmic fashion to approximate a solution. In this talk, I will survey three methods (alternating projections, Dykstra, and Douglas-Rachford), and comment on recent advances and remaining challenges.

Mark Thom (Math and CS, U of Lethbridge) Dec 3, 2012

Squarefree values of trinomial discriminants

The discriminant of a trinomial of the form $x^n \pm x^m \pm 1$ has the form $\pm n^n \pm (n-m)^{n-m} m^m$ when n and m are co-prime. We determine necessary and sufficient conditions for identifying primes whose squares never divide the discriminants arising from coprime pairs (n, m). These conditions are adapted into an exhaustive search method, which we use to corroborate a heuristic estimate of the density of all such primes among the odd primes. The same results are used to produce a heuristic estimate of the density of squarefree values of these discriminants. We'll also look at an unlikely seeming family of divisors of the discriminants, arising from an elementary identity on them. This is joint work with David Boyd and Greg Martin.

Spring 2012

Open problem session Jan 16, 2012

Please bring your favourite (math) problems to share with everyone.

Habiba Kadiri (Math and CS, U of Lethbridge) Jan 23, 2012

Zero density estimates for the zeros of the Riemann zeta function

An important tool in the analytic investigation of the distribution of primes consists in estimates for the density of zeros of the Riemann zeta function in the critical strip $0 < x < 1$.

We denote $N(a, T)$ the number of such zeros in the region $\left\{ a < x < 1 \mid 0 < y < T \right\}$. It is expected that the zeros close to the 1-line are rare (and thus that $N(a, T)$ decreases with a). Great efforts have been made to establish asymptotic results of the form

$$N(a, T) \ll T^{c(a)(1-a)} (\log T)^A,$$

where $c(a)$ and A are positive. However, there are very few explicit bounds for $N(a, T)$.

In this talk, we will present the following result together with the ideas for its proof:

$$N(a, T) < c_1(a)T + c_2(a) \log T - c_3(a),$$

where each c_i is explicit and positive.

Brandon Fodden (Math and CS, U of Lethbridge) Jan 30, 2012

Hilbert's Tenth Problem

Hilbert's Tenth Problem asks for an algorithm which can determine if an arbitrary Diophantine equation (with integral coefficients) has solutions. In 1970 Yuri Matiyasevich, building on the work of Martin Davis, Julia Robinson and Hilary Putnam, showed that no such algorithm may exist. In this talk, we give an outline of a proof of this, and discuss some applications and related problems. No specialist knowledge is assumed and everyone is welcome.

PDF slides of the talk are available at

http://www.cs.uleth.ca/~nathanng/Fodden-hilbert10.pdf

Nathan Ng (Math and CS, U of Lethbridge) Feb 6, 2012

At least one-third of the zeros of the Riemann zeta function are on the half line

In 1942 Selberg proved that a positive proportion of the zeros of the Riemann zeta function lie on the half line. Unfortunately, he never determined a numerical value for this proportion. By a different method Levinson proved in 1974 that the proportion is at least one-third. In this talk I will explain Levinson's proof and I will also briefly discuss Conrey's improvement of Levinson's result to four-tenths.

Amir Akbary (Math and CS, U of Lethbridge) Feb 13, 2012
Maass forms

This is an introductory talk on Maass forms for $\mathrm{SL}(2,\mathbb{Z})$. These objects were first studied by H. Maass in 1949. They appeared as non-holomorphic analogues of modular forms. Maass called them waveforms. We follow the presentation given in Sections 1.6 and 1.9 of Bump's book (Automorphic Forms and Representations)

Yuri Matiyasevich (Steklov Institute, Russia) Feb 27, 2012
New conjectures about zeros of Riemann's zeta function

In http://logic.pdmi.ras.ru/~yumat/personaljournal/artlessmethod/artlessmethod.php the speaker described a surprising method for (approximate) calculation of the zeros of Riemann's zeta function using terms of the divergent Dirichlet series. In the talk this method will be presented together with some heuristic "hints" explaining why the divergence of the series doesn't spoil its use. Several conjectures about the zeros of Riemann's zeta function will be stated including supposed new relationship between them and the prime numbers.

Ted Dobson (Mississippi State University) Feb 29, 2012
Groups that are transitive on all partitions of a finite set

Let $\ell_1,\dots,\ell_r$ be positive integers whose sum is n. Let $K_1,\dots,K_r$ be subsets of the n-element set $[n]=\{1,\dots,n\}$ such that these sets form a partition P of $[n]$ and $|K_i|=\ell_i$. We say that $[\ell_1,\dots,\ell_r]$ is the *shape* of P. Let $\mathcal{P}$ be the set of all partitions of $[n]$ with shape $[\ell_1,\dots,\ell_r]$. We determine all subgroups of S_n that are transitive on $\mathcal{P}$ for every possible shape $[\ell_1,\dots,\ell_r]$, as well as determine all subgroups of S_n that are transitive on the set of all ordered partitions of every possible shape. As an application, we determine which Johnson graphs are isomorphic to Cayley graphs. This is joint work with Aleksander Malnič.

Ce Bian (University of Calgary, Alberta) Mar 5, 2012
Two approaches to compute GL(3) automorphic forms

In this talk we present methods using the functional equation and Voronoi summation formula to compute the Casimir eigenvalues and Hecke eigenvalues of certain automorphic forms on GL(3).

Timothy Trudgian (Math and CS, U of Lethbridge) Mar 12, 2012
Some mathematics in voting

Many countries employ different voting systems, each with its own advantages and disadvantages. In Australia the 'preferential' voting system is used: candidates are numbered 1 through to n. One disadvantage is a theoretical occurence of non-monotonicity: essentially candidates can be ranked more highly and yet they, almost paradoxically, perform more poorly. The debate about the likelihood of such a paradox has influenced recent decisions (notably in the UK) about whether a particular voting system should be adopted. I will try to sketch a mathematical approach to this problem.

Joy Morris (Math and CS, U of Lethbridge) Mar 19, 2012
The probabilistic method

Paul Erdös is well-known for the number and breadth of his publications. His most significant contributions to combinatorics involved using the "probabilistic method:" proving that various objects must exist by developing a probability model and proving that the probability of finding such an object is strictly greater than 0. I will introduce the probabilistic method, and work through examples of several theorems that can be proved using this method.

Soroosh Yazdani (Math and CS, U of Lethbridge) Mar 26, 2012
Death of synthetic geometry

Since antiquity people have been intrigued by problems like the "problems of Appolonius:" construct a circle tangent to three given circles. This specific problem can be solved using compass and straight edge. Jacob Steiner in 1848 pointed out that when the circles are replaced by arbitrary conics, these problems become more involved. For one thing it should take 5 conics, rather than 3, to determine the unknown conic. Furthermore, the five conic rarely determine a single conic, which raises the question, known as the Steiner problem, of how many conics are tangent to 5 given conics. Steiner conjectured that there are $6^5 = 7776$ conics, but did not elaborate much on this conjecture. This was proved by Johann Bischoff in 1859, but it was soon realized that this is not the right answer to the question.

In this talk I will explain how do we get this answer, why this is not the right answer, how to get the right answer, and why this is an example of a problem responsible for killing synthetic geometry, and for that matter, what do I mean by synthetic geometry.

Dave Morris (Math and CS, U of Lethbridge) Apr 2, 2012
Strictly convex norms on amenable groups

It is obvious that the usual Euclidean norm is strictly convex, by which we mean that, for all x and all nonzero y, either $\|x + y\| > \|x\|$, or $\|x - y\| > \|x\|$. We will discuss the existence of such a norm on an abstract (countable) group G. A sufficient condition is the existence of a faithful action of G by orientation-preserving homeomorphisms of the real line. No examples are known to show that this is not a necessary condition, and we will combine some elementary measure theory and dynamics with the theory of orderable groups to show that the condition is indeed necessary if G is amenable. This is joint work with Peter Linnell of Virginia Tech.

Michael Coons (University of Waterloo, Ontario) Apr 10, 2012

Diophantine approximation of Mahler numbers

Let $F(x) \in Z[[x]]$ be a Mahler function; that is, there exist positive integers $k \geq 2$ and $d \geq 1$ and polynomials $a_0(x), \ldots, a_d(x) \in \mathbb{Z}[x]$ with $a_0(x)a_d(x) \neq 0$ such that

$$\sum_{i=0}^{d} a_i(x) F\left(x^{k^i}\right) = 0.$$

Let ξ be a real number. The irrationality exponent $\mu(\xi)$ of ξ is defined as the supremum of the set of real numbers μ such that the inequality $|\xi p/q| < q^{-\mu}$ has infinitely many solutions $(p, q) \in \mathbb{Z} \times \mathbb{N}$. Last year (in a talk at the University of Lethbridge), I showed that the sum of the reciprocals of the Fermat numbers (which is a special value of a Mahler function) has irrationality exponent 2 and I conjectured that all reasonable special values of Mahler functions should have finite irrationality exponent. In this talk, I will present some of the history of Mahler functions and Diophantine approximation with a view towards the proof of the above-mentioned conjecture.

Paul Buckingham (University of Alberta) Apr 16, 2012

p-adic L-functions, and derivatives of Artin L-functions at $s = 0$

p-adic L-functions are traditionally obtained from the more classical Artin L-functions by interpolating their values at negative integers. Iwasawa gave an alternative construction which, surprisingly, involves only values at $s = 0$. We will discuss a relatively new object defined in terms of derivatives at $s = 0$, instead of simply values, which appears to extend Iwasawa's construction to a potentially new kind of p-adic L-function. The talk will assume no prior knowledge of p-adic numbers.

Fall 2011

Open problem session Sept 14, 2011

Please bring your favourite (math) problems to share with everyone.

Soroosh Yazdani (Math and CS, U of Lethbridge) Sept 21, 2011
From Pythagoras to Beal?

In this talk I will look at some of Diophantine equations of the form $x^p + y^q = z^r$. The oldest of this equation studied is probably when $p = q = r = 2$ (Pythagorean triples), and probably the most famous one is when $p = q = r > 2$ (Fermat's last theorem). However, many other variations exist, and in this talk I will present what is known about them, and what is believed to be true.

Joy Morris (Math and CS, U of Lethbridge) Sept 28, 2011
Generalised n-gons with symmetry conditions

A generalised n-gon is an incidence structure whose bipartite incidence graph has diameter n and girth $2n$. Many of the known examples of generalised n-gons are highly symmetric, and in fact arise naturally from particular group actions.

I will give an overview of some of the things that are known about symmetries of generalised n-gons that we hope are leading toward classification of these objects, or at least to understanding the symmetry that they can have. My contributions to this problem are based on joint work with John Bamberg, Michael Giudici, Gordon Royle and Pablo Spiga of the University of Western Australia, done during my study leave.

Nathan Ng (Math and CS, U of Lethbridge) Oct 5, 2011
What is a modular form?

Modular forms play an important role in many branches of mathematics including number theory, arithmetic geometry, representation theory, and even theoretical physics. In this talk I will give a general introduction to modular forms and I will explain some of their fundamental properties.

Nathan Ng (Math and CS, U of Lethbridge) Oct 12, 2011
Simple zeros of modular L-functions

An old problem in analytic number theory is to show that an L-function possess simple zeros. Thanks to work of Levinson and Bauer, it is known that any degree one L-function has many simple zeros. For degree two L-functions there are fewer results known. Recently, the speaker and Milinovich have established a number of results concerning simple zeros of modular L-functions.

Timothy Trudgian (Math and CS, U of Lethbridge) Oct 19, 2011
One way to improve Ingham's theorem

One can conjecture the size of a certain arithmetic function: such a conjecture often implies the Riemann hypothesis and, courtesy of Ingham's theorem, that there are infinitely many zeroes the imaginary parts of which are linearly dependent. This is indeed bitter-sweet since, if one were keen to place a wager, one might venture to say that no zeroes are linearly dependent. Very little work has been done to find, computationally, 'near-zero' linear combinations of zeroes. The topic of this paper is to discuss what has been done by Bateman and co. in 'Linear relations connecting the imaginary parts of the zeros of the zeta function'.

Hadi Kharaghani (Math and CS, U of Lethbridge) Oct 26, 2011
Mutually unbiased Hadamard matrices

Two unit Hadamard matrices H,K of order n are called unbiased, if $HK^* = \sqrt{n}L$, where L is a unit Hadamard matrix. Time permitting, I will do all or part of the following:

- If there are m mutually unbiased unit (real) Hadamard matrices of order n, then $m \leq n$ ($m \leq n/2$).
- The above upper bound is sharp for n a prime power.
- Discuss the literature for composite orders n.
- Talk about mutually unbiased real Hadamard matrices and their applications to association schemes.

Nathan Ng (Math and CS, U of Lethbridge) Nov 2, 2011
A theorem of Frobenius

Consider the irreducible polynomial $f(x) = x^3 - x - 1$. Let p be a prime and consider this as a polynomial over the finite field of p elements. Over this field the polynomial is either irreducible, splits into three linear factors, or splits into a linear factor and a quadratic factor. Frobenius proved a theorem which asserts that these 3 cases occur with frequencies: 1/3, 1/6, and 1/2. Why do these fractions occur? The answer is related to the fact that the Galois group of f is the symmetric group of 3 letters. Moreover, he considered how an irreducible polynomial factors when reduced modulo p. In this talk I will explain Frobenius' theorem. This seminar will be accessible to undergraduate students who have taken Math 3400 (Group and Rings).

Timothy Trudgian (Math and CS, U of Lethbridge) Nov 9, 2011
Dirichlet's theorem and an application to the zeta-function

Suppose one has managed to bound a certain complex-valued function, $f(z)$ say, by another function $g(z)$. How could one show that the bound $g(z)$ is 'as good as it gets'? The study of so-called Omega-theorems is designed to answer this question. Dirichlet's theorem (which is not much more complicated than the statement that if $k+1$ students need to sit on k chairs then at least two of them must sit in the same chair) provides a good insight into Omega-theorems: in particular one may use Dirichlet's theorem to show that some bounds for the growth of the zeta-function are the best possible.

Soroosh Yazdani (Math and CS, U of Lethbridge) Nov 16, 2011
Introduction to elliptic curves

In this talk we give a brief introduction to elliptic curves. We start by describing what they are, where they came from, and why number theorists are obsessed by them.

Amir Akbary (Math and CS, U of Lethbridge) Nov 23, 2011
On a theorem of Jordan

We give an exposition of a paper of Jean-Pierre Serre with the same title (Bulletin of AMS, Volume 40 (2003), 429–440). Its abstract reads as follows: "The theorem of Jordan which I want to discuss here dates from 1872. It is an elementary result on finite groups of permutations. I shall first present its translations in Number Theory and Topology."

Dave Morris (Math and CS, U of Lethbridge) Nov 30, 2011
Hamiltonian checkerboards

Place a checker on some square of an m-by-n rectangular checkerboard. Asking whether the checker can tour the board, visiting all of the squares without repeats, is the same as asking whether a certain graph has a hamiltonian path (or hamiltonian cycle). The question becomes more interesting if we allow the checker to step off the edge of the board. This modification leads to numerous open problems, and also to connections with ideas from elementary topology and group theory. Some of the problems may be easy, but many have resisted attack for 30 years. No advanced mathematical training will be needed to understand most of this talk.

Dave Morris (Math and CS, U of Lethbridge) Dec 7, 2011
How to make infinitely large numbers from two-player games

We will talk about certain strategy games, in which the moves alternate between two players. Chess, checkers, and Go are some of the games we could discuss, but, to keep things simple, we will stick to easier examples. John H. Conway discovered that analyzing who will win from a given starting position has some very interesting consequences. In particular, we will see how to add two games (or subtract them, or multiply them), and we will encounter numbers that are infinitely large. No advanced mathematical training will be needed to understand most of this talk, but it would be helpful to have heard of "Dedekind cuts".

The main talk will be preceded by a short explanation of "Zero-Knowledge Proofs." These allow you to convince someone you know how to prove a theorem, without giving them any information at all about the proof (except how long it is).

Fall 2010

Tim Trudgian (Math and CS, U of Lethbridge) Sept 29, 2010
Gram's Law and the zeroes of the Riemann zeta-function (I)

That all the complex zeroes of the zeta-function lie on the critical line is the Riemann Hypothesis. Regrettably, the margin for this abstract is too narrow to write down a proof. The first 15 zeroes on the critical line were found by Gram in 1903. As a general rule of thumb, he proposed what is now called 'Gram's Law', a phenomenon by the use of which one can locate zeroes on the critical line. All subsequent searches for zeroes on the critical line use this method, in some form or another. In this seminar I shall summarise the theory one requires to state Gram's Law, as well as providing motivation for why it might be true significantly often.

Tim Trudgian (Math and CS, U of Lethbridge) Oct 6, 2010
Gram's Law and the zeroes of the Riemann zeta-function (II)

With Gram's Law clearly defined, I shall develop the necessary theory to see whether it fails or holds in a positive proportion of cases. Several versions of Gram's Law hold and fail at this frequency, and this was my doctoral research at Oxford. Motivation from random-matrix theory will perhaps indicate the true rate of success and failure of Gram's Law.

Nathan Ng (Math and CS, U of Lethbridge) Oct 27, 2010
Nonzero values of Dirichlet L-functions in vertical arithmetic progressions

An open question in analytic number theory is:

How do the zeros of a Dirichlet L-function behave in the critical strip?

One might wonder whether the zeros bunch up or are they very well-spaced.

In particular, is it possible for the zeros to lie in an arithmetic progression?

In joint work with Greg Martin, we show that many terms of an arithmetic progression are not zeros of a fixed Dirichlet L-function.

Amir Akbary (Math and CS, U of Lethbridge) Nov 24, 2010
Uniform distribution of zeros of the Riemann zeta function

We explain the Weyl criterion for the uniform distribution mod 1 of a sequence of real numbers. As an application of this criterion we describe a theorem of Hlawka on the uniform distribution mod 1 of the imaginary parts of the zeros of the Riemann zeta function.

Dave Morris (Math and CS, U of Lethbridge) Dec 8, 2010
Reconstruction from vertex-switching

The Reconstruction Conjecture is a famous unsolved problem in graph theory. We will discuss a related problem that was partially solved by Richard Stanley in 1985. He used the Radon Transform, which is a technique that originated in analysis, and is the mathematical basis of modern CAT scans (used in medical diagnostics).

Spring 2010

Nathan Ng (Math and CS, U of Lethbridge) Feb 24, 2010
Linear combinations of the zeros of the zeta function

The linear independence conjecture asserts that the imaginary ordinates of the zeros of the zeta function are linearly independent over the rationals. This conjecture has played an important role in several classical problems in analytic number theory including the Mertens conjecture and the Shanks-Renyi prime number race game. I will discuss the history of this conjecture and some preliminary results concerning linear combinations of the zeros of zeta function. This is joint work with Greg Martin.

Vorrapan Chandee (Stanford University, California) Mar 4, 2010
On the correlation of shifted values of the Riemann zeta function.

In 2007, assuming the Riemann Hypothesis (RH), Soundararajan proved that the $2k$-th moments of the Riemann zeta function on the critical line is bounded by $T(\log T)^{k^2+\epsilon}$ for every k positive real number and every $\epsilon > 0$. In this talk I will generalize his methods to find upper bounds for shifted moments. Also I will sketch the proof how we derive their lower bounds and conjecture asymptotic formulas based on Random matrix model, which is analogous to Keating and Snaith's work. These upper and lower bounds suggest that the correlation of $|\zeta(1/2+it+i\alpha_1)|$ and $|\zeta(1/2+it+i\alpha_2)|$ transition at $|\alpha_1-\alpha_2|$ is around $1/\log T$. In particular these distribution appear independent when $|\alpha_1-\alpha_2|$ is much larger than $1/\log T$.

Micah Milinovich (University of Mississippi) Mar 17, 2010
Central values of derivatives of Dirichlet L-functions

It is believed (a conjecture usually attributed to S. Chowla) that no primitive Dirichlet L-function vanishes at the center of the critical strip $s = 1/2$. This problem is still open. The best partial is due to H. Iwaniec and P. Sarnak who have shown that at least a third of the Dirichlet L-functions, to a large modulus q, do not vanish at the central point. I will describe how to modify their method and show that, for k and q large, almost all of the values of the k-th derivatives of primitive Dirichlet L-functions (mod q) are nonzero at $s = 1/2$. Our result compliments earlier work of P. Michel and J. VanderKam whoconsidered a similar problem. This is joint work with Hung M. Bui.

Habiba Kadiri (Math and CS, U of Lethbridge) Mar 31, 2010
Explicit bounds for some prime counting functions.

A prime counting function assigns a weight to each prime number. For example $\pi(x)$ counts exactly the number of prime numbers less than an arbitrarily large number x. It was conjectured by Gauss that $\pi(x)$ is of the size $\dfrac{x}{\log x}$ as x grows larger. In 1859, Riemann proposed a formula relating prime counting functions to the zeros of a complex function (now called the Riemann Zeta function). This innovative approach allowed Hadamard and de la Vallée Poussin to establish the Prime Number Theorem:

$$\pi(x) \sim \frac{x}{\log x}.$$

An explicit bound for this error term has been successively investigated by Rosser, Schoenfeld, and more recently by Dusart. I will start the talk by explaining their method and I will then present a new approach investigated last summer together with Laura Faber, Allysa Lumley and Nathan Ng.

Habiba Kadiri (Math and CS, U of Lethbridge) Apr 7, 2010
Explicit bounds for some prime counting functions (II)

This talk is a continuation of last week's talk. I will explain how to obtain lower and upper bounds for the prime counting function $\psi(x)$. The proof uses smooth functions and the theory of Mellin transforms. We will also see how the previous method of Rosser and Schoenfeld is reinterpreted through this method.

Fall 2009

Dragos Ghioca (Math and CS, U of Lethbridge) Sept 30, 2009
Arithmetic dynamics

Starting from a fundamental question regarding roots of unity we present a generalization of the classical Manin-Mumford conjecture in the context of algebraic dynamics.

Brandon Fodden (Math and CS, U of Lethbridge) Oct 16, 2009
An explicit inequality equivalence of the generalized Riemann hypothesis for a member of the Selberg class

Given a member F of the Selberg class, we find a property P of the natural numbers such that the generalized Riemann hypothesis holds for F if and only if P holds for all natural numbers. P is given as an explicit inequality. If one can show that P is a decidable property, then the generalized Riemann hypothesis for F is equivalent to the unsolvability of a particular Diophantine equation. We discuss variants of P for which proving decidability is more practical. Finally, we apply this result to L-functions related to elliptic curves.

Amir Akbary (Math and CS, U of Lethbridge) Oct 28, 2009
Analytic problems for elliptic curves (I): Titchmarsh Divisor Problem

Titchmarsh Divisor Problem concerns the asymptotic behavior of the sum (on primes up to x) of the number of divisors of shifted primes. In 1930 Titchmarsh studied this problem and conjectured an asymptotic formula for such a sum. In 1961 Linnik proved that Titchmarsh's conjecture is true.

In this talk we will review the results given in the original paper of Titchmarsh. Our goal here is to describe an analogue of the Titchmarsh Divisor Problem in the context of elliptic curves.

Amir Akbary (Math and CS, U of Lethbridge) Nov 4, 2009
Analytic problems for elliptic curves (II): an elliptic analogue of the Titchmarsh Divisor Problem

We continue our discussion on the Titchmarsh Divisor Problem. Recall that this problem concerns the asymptotic behavior of the sum

$$\sum_{\substack{p\leq x\\ p \text{ prime}}} \tau(p-1)$$

as $x \to \infty$, where $\tau(p-1)$ is the number of divisors of $p-1$.

Our goal is to describe an analogue of this problem in the context of elliptic curves.

Nathan Ng (Math and CS, U of Lethbridge) Nov 18, 2009
A brief history of the Riemann Hypothesis

In 1859, Riemann introduced the zeta function to the theory of prime numbers. Riemann proved some basic properties regarding the behaviour of this function: functional equation, approximate functional equation, number of zeros in a box, and explicit formula. Moreover, he introduced a profound conjecture, the Riemann hypothesis, which concerns the location of zeros of the zeta function. In this talk I will discuss Riemann's conjecture and it's great influence on analytic number theory.

Howard Cheng (Math and CS, U of Lethbridge) Nov 27, 2009
Time- and space-efficient computation of hypergeometric constants

Hypergeometric series are infinite series of the form

$$\sum_{n=0}^{\infty} a(n) \prod_{i=0}^{n-1} \frac{p(i)}{q(i)}$$

where a, p, and q are polynomials with integer coefficients. Many elementary functions evaluated at rational points may be approximated to high precision (millions of digits) by using hypergeometric series with a technique commonly known as "binary splitting." Furthermore, well-known constants such as π and $\zeta(3)$ can also be evaluated in this manner.

Although the binary splitting method is relatively efficient in terms of time, it is not optimal in terms of the amount of space (memory) used. In this talk, we look at the development of an algorithm that is space-efficient—it uses only $O(N)$ extra space where N is the number of digits desired. Its time complexity is the same as binary splitting but is faster in practice. Elementary properties of integer factorization and prime numbers are used to obtain the resulting algorithm. To the best of my knowledge, this is also the fastest algorithm for this type of calculations.

Dave Morris (Math and CS, U of Lethbridge) Dec 2, 2009
Some arithmetic groups that cannot act on the line

It is known that finite-index subgroups of the arithmetic group $SL(3, \mathbb{Z})$ have no interesting actions on the real line. This naturally led to the conjecture that most other arithmetic groups (of higher real rank) also cannot act on the line (except by linear-fractional transformations). This problem remains open, but my joint work with Lucy Lifschitz (University of Oklahoma) and Vladimir Chernousov (University of Alberta) has verified the conjecture for many examples. The proofs are based on the fact, proved by D. Carter, G. Keller, and E. Paige, that if A is the ring of integers of an algebraic number field, and A has infinitely many units, then every element of $SL(2, A)$ is a product of a bounded number of elementary matrices.

Spring 2009

Habiba Kadiri (Math and CS, U of Lethbridge) Jan 14, 2009
The Ihara Zeta function of graphs

In this talk, I will give an introduction to the Ihara Zeta function of graphs, which has analogous behavior to the Riemann Zeta function. For example, we will discuss its analytical properties, the explicit formula, the Riemann Hypothesis and the Graph Prime Number Theorem.

This talk is accessible to students.

Habiba Kadiri (Math and CS, U of Lethbridge) Jan 21, 2009
About the distribution of the eigenvalues of Ramanujan's graphs

In the last lecture, we discovered the notion of arithmetic for graphs and how the Ihara Zeta function was used to count the number of paths and prime paths of arbitrarily large length. This type of relation is analogous to the relation between the distribution of prime numbers and the location of the zeros of the Riemann Zeta function.

This lecture is a follow up to the previous lecture. I will focus on some particular regular graphs, called Ramanujan graphs. These graphs appear in various domains of mathematics and computer science. I will discuss the distribution of the eigenvalues for Ramanujan graphs, the Riemann Hypothesis for graphs and compare it to the case of the classical Riemann Zeta function. If time permits, I will also discuss the problem of the distribution of the spacings of the zeros.

Amir Akbary (Math and CS, U of Lethbridge) Feb 11, 2009
Ramanujan graphs

A Ramanujan graph is a connected regular graph whose non-trivial eigenvalues are relatively small in absolute value. This talk introduces these graphs and describes some basic constructions of them.

The talk will be accessible to people familiar with basic elements of graph theory.

Amir Akbary and Dave Morris (Math and CS, U of Lethbridge) Feb 25, 2009
Expander graphs

This talk will introduce the class of expander graphs, and describe some of their basic properties. We will start the seminar with some applications of Ramanujan graphs, which are a special case.

The talk will be accessible to people familiar with basic elements of graph theory.

Dave Morris (Math and CS, U of Lethbridge) Mar 4, 2009
More on expander graphs

This talk will have three parts: a proof that random k-regular graphs are very likely to be expanders, a discussion of the eigenvalues of the adjacency matrix of an expander graph, and a brief explanation of Margulis' explicit construction of expander graphs.

Kaneenika Sinha (University of Alberta) Mar 18, 2009
A trace formula for Hecke operators on spaces of newforms

Fourier coefficients of some appropriately chosen modular forms can be interpreted as eigenvalues of Hecke operators. We derive a trace formula for Hecke operators acting on spaces of newforms of given level and weight. This explicit formula can be applied to study the distribution of Fourier coefficients of newforms. We will also derive arithmetic information about newparts of Jacobians of modular forms.

Behruz Tayfeh-Rezaie (Institute for Research in Fundamental Science, Iran) Apr 8, 2009
On the sum of Laplacian eigenvalues of a graph

A. E. Brouwer conjectured that the sum of k largest Laplacian eigenvalues of G is at most $e + \binom{k+1}{2}$, where e is the number of edges of G. We prove this conjecture for $k = 2$. We also show that if G is a tree, then the sum of k largest Laplacian eigenvalues of G is at most $e + 2k - 1$.

This is a joint work with W. H. Haemers and A. Mohammadian.

Fabien Pazuki (U of Lethbridge, U of Paris 7, and U of Bordeaux 1, France) Aug 19, 2009
Bounds on torsion for abelian varieties and reduction properties

Let k be a number field and A/k be an abelian variety. The Mordell-Weil theorem implies that there are only finitely many torsion points defined over k, and finding a uniform upper bound on this number is still an open question for abelian varieties of dimension $g > 1$. We will see how properties of reduction of the variety are linked with getting good upper bounds on the cardinality of the torsion subgroup. We will try to avoid technicality.

Fabien Pazuki (U of Lethbridge, U of Paris 7, and U of Bordeaux 1, France) Aug 26, 2009
Bounds on torsion and reduction properties (II). The height theory strikes back.

We will focus on the height theory in this second talk. We will study a conjecture formulated by Lang and Silverman, predicting a precise lower bound to the canonical height on an abelian variety. The goal is to understand the link between these height inequalities and uniform bounds on the number of torsion points. We will briefly recall the key facts from the first talk, present the conjecture and the known results.

Fall 2008

Brandon Fodden (Math and CS, U of Lethbridge) Sept 10, 2008
A lower bound for fractional moments of certain L-functions

We extend the method of Heath-Brown to find a lower bound for the fractional moments of a certain class of L-functions.

Dragos Ghioca (Math and CS, U of Lethbridge) Sept 17, 2008
Algebraic dynamics

The classical Mordell-Lang conjecture (proven by Faltings and Vojta) describes the intersection between a finitely generated subgroup of a semiabelian variety defined over the field of complex numbers with a subvariety V of G. We may view this subgroup of G as the image of 0 under the action of a finitely generated semigroup S of automorphisms of G (each automorphism being a translation). We present extensions of the Mordell-Lang conjecture in which S is any finitely generated semigroup of endomorphisms of G.

Amir Akbary (Math and CS, U of Lethbridge) Sept 24, 2008
Rankin-Selberg Convolutions

We describe how the study of the analytic properties of the convolution of the Dirichlet series leads to the results on the size of the coefficients of the Dirichlet series.

Nathan Ng (Math and CS, U of Lethbridge) Oct 1, 2008
Non-vanishing of L-functions and application to a Fermat equation

In recent years, a popular research topic in analytic number theory has the been the non-vanishing of L-functions. In this talk I will discuss some non-vanishing results which imply the Fermat equation $A^4 + B^2 = C^p$ for p a prime larger than 5 has no non-trivial solutions.

Nathan Ng (Math and CS, U of Lethbridge) Oct 22, 2008
The Mobius function summed over short intervals

The Central Limit Theorem in probability determines that a sum of independent identically distributed random variables is normally distributed. A number theoretic model for a sequence of such random variables is the Mobius function. In this talk we discuss the distribution of the sum of the Mobius function in short and long intervals. We will see that in short intervals the Mobius function behaves like a sum of independent random variables. However, over longer intervals its behaviour depends on the zeros of the zeta function.

Dave Morris (Math and CS, U of Lethbridge) Oct 29, 2008
Introduction to Ratner's Theorems on unipotent flows (I)

Unipotent flows are very well-behaved dynamical systems. In particular, Marina Ratner has shown that every orbit is uniformly distributed (on some invariant submanifold). The first talk will present some important number-theoretic consequences of this theorem, and the second talk will explain a few of the ideas of the proof.

Dave Morris (Math and CS, U of Lethbridge) Nov 5, 2008
Introduction to Ratner's Theorems on unipotent flows (II)

Unipotent flows are very well-behaved dynamical systems. In particular, Marina Ratner has shown that every orbit is uniformly distributed (on some invariant submanifold). The first talk will present some important number-theoretic consequences of this theorem, and the second talk will explain a few of the ideas of the proof.

Chantal David (Concordia University, Quebec) Nov 10, 2008
Almost prime orders of elliptic curves over finite fields

Let E be an elliptic curve over the rationals. A conjecture of Neal Koblitz predicts an exact asymptotic for the number of primes p such that the order of E over the finite field with p elements is prime. This conjecture is still open. Using sieve techniques, one can find a lot of primes p such that the order $p+1-a_p(E)$ is almost prime. The best result that one may hope to achieve by sieve techniques was obtained by Iwaniec and Jimenez Urroz for complex multiplication curves using Chen's sieve. They showed that there are infinitely many primes p such that $p+1-a_p(E) = P_2$, where $n = P_k$ means that the integer n has at most k prime factors. For elliptic curves without complex multiplication, it is not known how to apply the switching principle of Chen's sieve to get such a result.

For curves without complex multiplication, we show that there are many primes p such that $p+1-a_p(E) = P_8$ with an explicit lower bound (in terms of the constant $C(E)$ of Koblitz's conjecture), using Greaves' sieve and under the GRH. This improves previous work of Steuding and Weng. One can also show that there are many primes such that $p+1-a_p(E)$ has at most 6 *distinct* prime factors, but still cannot improve the number of (not necessarily distinct) primes from 8 to 6. This surprising result is related to the difficulty of sieving square-free numbers in the sequence $p+1-a_p(E)$.

This is joint work with Jie Wu (CNRS, Institut Elie-Cartan, Nancy).

Harald Helfgott (University of Bristol, England) Nov 21, 2008
Escape and incidence: their role in growth in groups

There is, so far, one tool that geometric group theory (largely on infinite groups) and recent work on non-commutative group combinatorics (largely on finite groups) have in common: the idea of escape.

After a brief discussion of what escape is and how it can be used, we shall pass to the possibility of restating much of "additive combinatorics" as the combinatorics of an abstract projective plane. There is a basic statement in the latter that does not seem to have a clear analogue in classical additive combinatorics; we shall see how the main idea of the proof is, again, escape.

Hadi Kharaghani (Math and CS, U of Lethbridge) Nov 26, 2008
On mutually unbiased Hadamard matrices

Two Hadamard matrices H and K of order n are called *unbiased* if $HK^t = \sqrt{n}L$, where L is a Hadamard matrix of order n. Mutually unbiased Hadamard matrices have applications in quantum measurement, quantum cryptography and design theory. I will try to give a simple survey talk on the the existence, structure and applications of these matrices.

This talk will be accessible to the senior undergraduate mathematics students.

Pablo Spiga (University of Padova, Italy) Dec 3, 2008
Synchronization and homomorphisms

An automaton is a machine which can be in any of a set of internal states which cannot be directly observed. A synchronizing automaton is an automaton admitting a sequence of transitions which take the automaton from any state into a known state. In this talk we present some recent connections between synchronizing automatons, permutation groups and graph homomorphisms. All relevant definitions would be given during the talk.

Spring 2008

Dragos Ghioca (Math and CS, U of Lethbridge) Jan10, 2008
Skolem-Mahler-Lech theorem

We present an old result for linear recurrence sequences whose proof relies on p-adic analysis. Based on it we derive an interesting result for automorphisms of the affine space.

Nathan Ng (Math and CS, U of Lethbridge) Jan 24, 2008
Lower bounds for moments of L-functions

Hardy and Littlewood initiated the study of high moments of the Riemann zeta function. They were initially interested in this problem because of its connection to the Lindelof hypothesis. In recent years, the moments of central values of families of L-functions have attracted much attention. In this talk I will explain a recent method of Rudnick and Soundararajan which establishes lower bounds for moments of L-functions of the correct order or magnitude.

Amir Akbary (Math and CS, U of Lethbridge) Jan 31, 2008
On the reduction mod p of a rational point of an elliptic curve

Let E be an elliptic curve over $\mathbb{Q}$. For any prime p of good reduction, let E_p be the elliptic curve over the finite field $\mathbf{F}_p$ obtained by reducing E modulo p. We investigate that for a point of infinite order in the Mordell group $E(\mathbb{Q})$, how the order of the reduction of this point mod p varies as p goes to infinity. We study this problem by comparison with reduction of integers mod p.

Nathan Ng (Math and CS, U of Lethbridge) Feb 7, 2008
Upper bounds for moments of the Riemann zeta function

I will explain a recent method of Soundararajan that proves an upper bound for moments of the Riemann zeta function which is nearly as sharp as the expected order of magnitude. This technique assumes the Riemann hypothesis and relies on obtaining an upper bound for the frequency of values for which the zeta function is large on the critical line.

John Irving (Saint Mary's University, Nova Scotia) Feb 14, 2008
Lattice paths under a shifting boundary

The generalized ballot theorem gives a well-known formula for the number of lattice paths in the first quadrant lying weakly under the line $x = ay$, wherea is an arbitrary positive integer. While there is almost certainly no simple formula for the number of paths under an arbitrary piecewise linear boundary, we show that nice enumerative results are available if we allow for cyclic shifts of such a general boundaries. A refinement of this result allows for the counting of paths with a specified number of corners, and we also examine paths dominated by periodic boundaries. This is joint work with A. Rattan.

Nathan Ng (Math and CS, U of Lethbridge) Feb 28, 2008
Upper bounds of the Riemann zeta function

Hadamard and Weierstrass proved a product formula for entire functions of order one. This factorization theorem leads to a formula for the logarithmic derivative of the zeta function in terms of the zeros of the zeta function. I will explain how such formulae can be applied to obtain upper bounds for the Riemann zeta function on the critical line. This talk is based on recent work of Soundararajan.

Matthew Greenberg (University of Calgary, Alberta) Mar 13, 2008
Modular forms, Stark units and Heegner points

In this talk, we will discuss constructions and conjectures concerning units in rings of algebraic integers and algebraic points on elliptic curves over number fields. Modular forms, in various guises, are the key ingredients in all known systematic constructions of such objects.

Brandon Fodden (Math and CS, U of Lethbridge) Mar 20, 2008
Fractional moments of the Riemann zeta function

We discuss the Heath-Brown method to find upper and lower bounds for the fractional moment of the Riemann zeta function for s with real part 1/2.

Hadi Kharaghani (Math and CS, U of Lethbridge) Mar 27, 2008
The energy of matrices

Let M be an m by n matrix , $m \leq n$. Let λ_i, $i = 1, 2, \ldots, m$ be the eigenvalues of the matrix MM^t. Motivated by an application in theoretical chemistry, Gutman defined the energy of M to be the sum of the square roots of λ_i's. The $(0, 1)$-matrices attaining maximum energy will be discussed.

Habiba Kadiri (Math and CS, U of Lethbridge) Apr 3, 2008
A bound for the least prime ideal in the Chebotarev density problem.

A classical theorem due to Linnik gives a bound for the least prime number in an arithmetic progression. Lagarias, Montgomery and Odlyzko gave a generalization of this result to any number field. Their proof relies on some results about the distribution of the zeros of the Dedekind Zeta function (zero free regions, Deuring Heilbronn phenomenon). In this talk, I will present some new results about these zeros. As a consequence, we are able to prove an effective version of the theorem of Lagarias et al.

Harald Helfgott (University of Bristol, England) Apr 17, 2008
Growth in SL_3

Let K be $\mathbb{R}$, $\mathbb{C}$ or a $\mathbb{Z}/p\mathbb{Z}$. Let $G = SL_2(K)$. Not long ago, I proved the following theorem: for every subset A of G that is not contained in a proper subgroup, the set AAA is much larger than A. A generalization to groups of higher rank was desired by many, but seemed hard to obtain. I have obtained a generalization to $SL_3(K)$. The role of both linearity and the group structure of G should now be clearer than they were at first. Bourgain, Gamburd and Sarnak derived various consequences on expander graphs from my SL_2 result; analogous consequences should follow in the case of SL_3.

Nathan Jones (Centre de Recherches Mathématiques, Montreal, Quebec) May 9, 2008
A refined version of the Lang-Trotter conjecture

Let E be an elliptic curve defined over the rational numbers and r a fixed integer. Using a probabilistic model consistent with the Chebotarev density theorem for the division fields of E and the Sato-Tate distribution, Lang and Trotter conjectured an asymptotic formula for the number of primes up to x which have Frobenius trace equal to r. However, when one sums the main term in their asymptotic over r in a fixed residue class modulo q, one does not recover the main term in the Chebotarev theorem for the q-th division field, but rather $8/\pi$ times the main term.

In this talk, I will state a refinement of the Lang-Trotter conjecture and demonstrate consistency of this refinement with the Chebotarev Theorem for a fixed division field. This is based on joint work with S. Baier.

Fall 2007

Brandon Fodden (Math and CS, U of Lethbridge) Sept 12, 2007
Some unprovable statements in number theory

We will discuss some number theoretic statements which are unprovable with respect to either Peano arithmetic or the ZFC axioms of set theory. We will cover Goodstein's theorem as well as the connection that Diophantine equations have with the consistency of formalized systems.

Brandon Fodden (Math and CS, U of Lethbridge) Sept 26, 2007
Diophantine equations and the generalized Riemann hypothesis

We show that the statement "for all number fields K, the generalized Riemann hypothesis for K holds" is equivalent to a statement of the form "for all natural numbers n, property P holds" where P is a decidable property of the natural numbers (that is, there is an algorithm which will tell if P holds for an arbitrary natural number in finitely many steps). This in turn implies that the original statement is equivalent to the unsolvability of a particular Diophantine equation in the integers.

Dragos Ghioca (Math and CS, U of Lethbridge) Oct 10, 2007
Polynomial dynamics in number theory

We study orbits of complex polynomials from the point of view of arithmetic geometry. In particular we show that if two nonlinear complex polynomials have orbits with infinite intersection, then the polynomials have a common iterate.

Nathan Ng (Math and CS, U of Lethbridge) Oct 26, 2007
Chebyshev's Bias, Galois groups, and L-functions

Chebyshev observed the strange phenomenon that there appear to be more primes congruent to three modulo four than to one modulo four. This is counterintuitive since one expects that there are an equal number of primes congruent to three modulo four than to one modulo four. In this talk, I will explain this phenomenon known as "Chebyshev's bias" and I will discuss generalizations. For example, consider the polynomial $x^3 - x - 1$. If we consider this polynomial modulo p a prime, this polynomial is either irreducible, splits into a linear factor and a quadratic factor, or splits into three linear factors. I will explain which of these cases occurs the most frequently and I will explain why the "bias" arises.

Habiba Kadiri (Math and CS, U of Lethbridge) Nov 7, 2007
About Vinogradov's bound for the three primes Goldbach's conjecture

Can any odd number greater than 5 be written as a sum of 3 primes? In 1922, Hardy and Littlewood were the first to give a substantial answer to this question: using their Circle Method, they proved that, under the condition of the Generalized Riemann Hypothesis, it was true for sufficiently large integers.

Fifteen years later, Vinogradov removed completely this hypothesis. His theorem remains one of the strongest results in the direction of Goldbach's conjecture. In this lecture, we will go through Vinogradov's proof, and understand how the distribution of the zeros of the Dirichlet L-functions enter into play.

Kerri Webb (Math and CS, U of Lethbridge) Nov 21, 2007
Lattice path bijections

Two opponents play $2n$ head to head games, and each player wins a total of n games. In how many ways can this be done, if the second player never has more wins than her opponent?

This puzzle can be solved with lattice paths: paths in the plane from the point $(0, 0)$ to (n, n), where each step in the path is in the direction $(1, 0)$ or $(0, 1)$. We survey enumeration results for various modifications of lattice paths. Classical bijections and a search for a new bijection are also discussed.

Radan Kucera (Masaryk University, Czech Republic) Nov 28, 2007
On circular units and the class group of an abelian field

The aim of this talk is to show that circular units can be used to study the class group of an abelian field. At the beginning we recall the definition and basic properties of the group of circular units of an abelian number field (explicit generators, finite index in the full group of units, Sinnott's formula containing the class number).

Then we show a concrete application: having a compositum K of real quadratic fields unramified at 2, we derive a lower bound for the divisibility of the class number of K by a power of 2.

We also explain that circular units can be used to obtain an information concerning the Galois module structure of the class group: For an abelian field K and a prime p, two Galois modules appear here naturally, namely the p-th part of the group of all units modulo the subgroup of circular units and the p-th part of the class group. Thaine's theorem states that any annihilator of the former module is an annihilator of the latter one, provided p is odd and relatively prime to the degree of the field.

Finally a joint result with C. Greither concerning the p-th part of the class group of cyclic fields of p-power degree will be explained.

Amir Akbary (Math and CS, U of Lethbridge) Dec 5, 2007
Sharp upper bounds for divisor sums

We describe an algorithm that provides explicit upper bounds for a certain arithmetic function (which will be defined in the talk). We use this algorithm to establish some explicit upper bounds for the sum of divisors function.

This is a joint work with Zachary Friggstad (University of Alberta) and Robert Juricevic (University of Waterloo).