The Mathematical Interests of Peter Borwein
May 12 - May 16, 2008

Speakers
Times and Rooms
Titles and Abstracts

Richard Askey, University of Wisconsin-Madison

Time: Tuesday, May 13th, 11:30 - 12:00
Room: ASB 10900

Title: Inequalities and special functions

Abstract: Some known and some open inequalities which involve special functions will be discussed.

*****

Bruce Aubertin, Langara College

Time: Friday, May 16th, 4:15 - 4:45
Room: ASB 10900

Title: Algebraic numbers and harmonic analysis

Abstract: Cantor's ternary set $C(3) = \left\{ \sum_1^\infty \epsilon_n 3^{-n} : \epsilon_n = 0 \text{ or } 1 \right\}$ is a set of uniqueness for trigonometric series, meaning that if a series $\sum_{-\infty}^{\infty} a_n e^{inx}$ converges to 0 everywhere outside $C(3)$ then it must be the zero series with $a_n \equiv 0$. It is not just size that determines this property of the set; in fact the Salem-Zygmund theorem tells us that if $\theta > 2$, then the Cantor set $C(\theta) = \left\{ \sum_1^\infty \epsilon_n \theta^{-n} : \epsilon_n = 0 \text{ or } 1 \right\}$ is a set of uniqueness if and only if θ is

a Pisot number (an algebraic integer greater than 1 all of whose conjugates lie inside the disk $|z| < 1$). The analogue of this result for groups of p-adic integers is well-known. But what about the square-wave case of Walsh series on the unit interval? The natural home of the Walsh functions is the dyadic group (the group of integers of the 2-series field), so we look at the group of integers of a p-series field. The sets $C(\theta)$ turn out to be all sets of uniqueness, and they need to be enlarged a little to see an interplay with algebraic numbers . We find that the enlarged set $E(\theta)$ is a set of uniqueness if and only if θ is a Pisot or Salem element of the field. (To come full circle (or rather back to the circle), we still dont know if the ternary set is a set of uniqueness for Walsh series!)

*****

David H. Bailey, Lawrence Berkeley National Laboratory

Time: Tuesday, May 13th, 9:00-10:00
Room: ASB 10900

Title: High-Performance Computing and Peter Borwein

Abstract: Peter Borwein's research career has touched on many of the most important themes of modern computing, including computational complexity, highly parallel computing, numerical analysis, high-accuracy computing, numerical integration, fast Fourier transforms, computational algebra, computational linear algebra and linear relation detection. This talk will describe how these seemingly different threads of research all connect together, and how they have led to unanticipated new developments that are only now being fully plumbed.

*****

Arthur Baragar, University of Nevada, Las Vegas

Time: Friday, May 16th, 11:30 - 12:00
Room: ASB 10900

Title: Ruler and compass constructions

Abstract: "It is impossible to trisect an arbitrary angle."
"It is impossible to solve an arbitrary quintic."

So mathematicians have claimed, with confidence, for 170 years. Often omitted from these provocative statements are the qualifying phrases "using a straightedge and compass," and "using radicals." The cumbersome term "straightedge" is crucial, since with a ruler and compass one can, in fact, trisect an arbitrary angle. This was known to Archimedes. In this talk, we will show that there also exist quintics that are not solvable using radicals, but that are solvable using a ruler and compass.

*****

Mark Bauer, University of Calgary

Time: Monday, May 12th, 4:30 - 5:00
Room: ASB 10900

Title: The Trials and Tribulations of Cubic Function Fields in Characteristic Three

Abstract: Much of our knowledge and insight into function fields (from a computational perspective) comes from extending what has been learned in the number field case to this new setting. While this can work in positive characteristic, things tend to go awry when the characteristic of the field divides the degree of the extension. The simplest example of this is elliptic and hyperelliptic function fields in characteristic two. In this situation, while many things become more complicated, they are still manageable enough because they are relatively well behaved (it helps that they are Galois extensions). By doing something as innocuous as looking at cubic function fields in characteristic three, even calculating the most mundane invariant can become problematic.

In this talk, we will highlight some of the challenges that await the unwary researcher who mistakenly treads into this area. Some successes, and setbacks, will be discussed.

This is joint work with Jonathan Webster.

*****

Heinz Bauschke, University of British Columbia, Okanagan

Time: Friday, May 16th, 12:00 - 12:30
Room: ASB 10900

Title: 8 Queens, Sudoku and Projection Methods

Abstract: I will report on the unreasonable effectiveness of a projection method, and on corresponding results and open problems.

Based on joint works with Patrick Combettes (Paris VI) and Russell Luke (Delaware), and with Jason Schaad (UBC Okanagan).

*****

Jason Bell, Simon Fraser University

Time: Monday, May 12th, 3:15 - 3:45
Room: ASB 10900

Title: Integer factorial ratios

Abstract: Using the fact that $\binom{2n}{n}$ is an integer for all $n \geq 0$, one can get a very good estimate for the function $\pi(x)$, the number of primes less than or equal to x. Using a slightly more complicated factorial ratio, Chebyshev showed $.92x/\log x \leq \pi(x) \leq 1.11x/\log x$. More generally, Erdős showed there exists a sequence of factorial ratios from which the prime number theorem can be deduced using Chebyshev's methods (he did not, however, produce such a sequence). We consider the question of when a factorial ratio of the form

$$\frac{\prod(a_i n)!}{\prod(b_j n)!}$$

is an integer for all $n \geq 0$, and give necessary conditions for this to hold. This proves a conjecture of Borisov and has applications to the classification of cyclic quotient singularities. This is joint work with Jonathan Bober.

*****

Adrian Belshaw, Simon Fraser University

Time: Tuesday, May 13th, 4:45 - 5:15
Room: ASB 10908

Title: The Distribution of the Primes

Abstract: We define normality of a sequnce of integers $\{a_n\}$ modulo an integer q. The definition ensures that if α is normal to a base b, then the sequence $\{[\alpha b^n]\}$ is normal modulo b.

If α is normal to a base b we can fully determine the modular normality of the sequence $\{[\alpha b^n]\}$. It turns out that this sequence is simply normal modulo every integer. On the other hand, it is normal modulo q if and only if q divides the base b.

Our proof of these two facts invokes some elementary graph theory, and makes use of some slightly less elementary properties of Markov chains.

*****

David Borwein, University of Western Ontario

Time: Wednesday, May 14th, 10:45 - 11:15
Room: ASB 10900

Title: Surprising Sinc Sums and Integrals

Abstract: This talk is based on material in a paper to appear shortly in MAA Monthly with the above title, co-authored with Robert Baillie and Jonathan M. Borwein, in which we show that a variety of trigonometric sums have unexpected closed forms by relating them to cognate integrals. For example, for $N = 1, 2, 3, 4, 5,$ and 6, (but not 7 or 8), we have

$$\frac{1}{2} + \sum_{n=1}^{\infty} \operatorname{sinc}^N(n) = \int_0^{\infty} \operatorname{sinc}^N(x)\, dx = r_N \pi,$$

where $\operatorname{sinc}(x) := \sin(x)/x$ and r_N is an effectively computable rational number, in particular, $r_1 = r_2 = 1/2$. In some natural cases ostensible identities fail only for very large N. For example, if $p_0 = 2$ and p_k is the kth odd prime, then

$$\frac{1}{2} + \sum_{n=1}^{\infty} \prod_{k=0}^{N} \operatorname{sinc}\left(\frac{n}{p_k}\right) = \int_0^{\infty} \prod_{k=0}^{N} \operatorname{sinc}\left(\frac{x}{p_k}\right)\, dx$$

holds until N is about 10^{176} and fails thereafter with error less than one part in a googolplex.

These and many of the other identities in the paper were first suggested by experimentation with *Mathematica* and *Maple*, and subsequently proved by means of Fourier analytic techniques.

*****

Jonathan Borwein, Dalhousie University

Time: Wednesday, May 14th, 4:15 - 5:15
Room: ASB 10900

Title: Peter Borwein revisited
Abstract: I'll be giving a talk full of anecdotes, pictures, and a bit of math.

*****

Nils Bruin, Simon Fraser University

Time: Tuesday, May 13, 3:30 - 4:00
Room: ASB 10900

Title: Local-to-global obstructions on curves
Abstract: I will give a brief survey of some of the phenomena one encounters when one tries to develop a general method to decide, given a curve, if it has any rational points.

*****

Imin Chen, Simon Fraser University

Time: Thursday, May 15, 2:30 - 3:00
Room: ASB 10900

Title: Quartic Q-derived polynomials with distinct roots
Abstract: We will discuss the problem of quartic Q-derived polynomials with distinct roots which is equivalent to the problem of finding the Q-rational points on a certain surface. We study some features of the geometry of this surface through a related cubic surface.

*****

Michael Coons, Simon Fraser University

Time: Thursday, May 15th, 3:45 - 4:15
Room: ASB 10908

Title: Sums of Completely Multiplicative Signature Functions

Abstract: This talk will focus on functions $f : \mathbb{N} \to \{1, -1\}$ that are completely multiplicative. In particular we will study their summatory functions, $\sum_{n \leq x} f(n)$. Related examples and conjectures will be discussed. (This is joint work with Peter Borwein and Stephen Choi.)

*****

Richard Crandall, Apple, Inc.

Time: Wednesday, May 14th, 1:15 - 2:15
Room: ASB 10900
Title: The partition function of number theory: A computational perspective

Abstract: The celebrated partition function $p(n)$ that counts partitions of n remains—even after 2 centuries—shrouded in mystery. For example, it remains unknown whether the parities $p(n)$ mod 2 are "random." Moreover, $p(n)$ is difficult to compute for very large n. But there are new, fast algorithms that lessen the effort. Some such algorithms have been implemented to answer certain statistical questions about the elusive $p(n)$.

*****

Annie Cuyt, University of Antwerpen

Time: Thursday, May 15th, 1:15 - 2:15
Room: ASB 10900

Title: Continued fractions for Special functions: Handbook and Software

Abstract: Special functions are pervasive in all fields of science. The most well-known application areas are in physics, engineering, chemistry, computer science and statistics. Because of their importance, several books and a large collection of papers have been devoted to the numerical computation of these functions. But up to this date, even environments such as Maple,

Mathematica, MATLAB and libraries such as IMSL, CERN and NAG offer no routines for the reliable evaluation of special functions. Here the notion reliable indicates that, together with the function evaluation a guaranteed upper bound on the total error or, equivalently, an enclosure for the exact result, is computed. We point out how limit-periodic continued fraction representations of these functions can be helpful in this respect. The newly developed (and implemented) scalable precision technique is mainly based on the use of sharpened a priori truncation error and round-off error upper bounds for real continued fraction representations of special functions of a real variable. The implementation is reliable in the sense that it returns a sharp interval enclosure for the requested function evaluation, at the same cost as the evaluation.

*****

Vahid Dabbaghian, Simon Fraser University

Time: Thursday, May 15th, 4:15- 4:45
Room: ASB 10900

Title: The Impact of Social Interactions on the Spread of HIV Infection among Injection Drug Users: A Cellular Automaton Model

Abstract: Injection drug users (IDU) who share needles are at high risk for contracting human immunodeficiency virus (HIV). Social and behavioral dynamics that lead to needle sharing can impact HIV transmission. In this talk I will describe a cellular automaton which is constructed to model a hypothetical HIV epidemic in an IDU community, in the presence of social influences that promote or discourage unsafe injection practices. Social influences are tracked using a social counter associated with each individual. Peer influence discouraging needle sharing shows a nonlinear response in exerting a strong impact on needle-sharing behaviour among IDU. Values below the phase transition curve we produced show an effect similar to herd immunity, as the epidemic for parameters in this region is eventually driven to extinctio.

This is a joint work with Peter Borwein, Krisztina Vasarhelyi, Alexander Rutherford and Natasha Richardson.

*****

Karl Dilcher, Dalhousie University

Time: Wednesday, May 14th, 3:00 - 3:30
Room: ASB 10900

Title: Stern polynomials and continued fractions

Abstract: We derive new identities for a polynomial analogue of the Stern sequence and define two subsequences of these polynomials. We obtain various properties for these two interrelated subsequences which have 0-1 coefficients and can be seen as extensions or analogues of the Fibonacci numbers. We also define two analytic functions as limits of these sequences. As an application we obtain evaluations of certain finite and infinite continued fractions whose partial quotients are doubly exponential. Finally we prove transcendence results for some of the infinite continued fractions. (Joint work with K.B. Stolarsky).

*****

Tamás Erdélyi, Texas A&M University

Time: Monday, May 12th, 1:30 - 2:30
Room: ASB 10900

Title: A few highlights of Peter Borwein's work with me

Abstract: I met Peter Borwein first more than 22 years ago in the Alfred Haar Memorial Conference held in Budapest, Hungary, in August 1985. In fact, my very first published paper appeared in the Conference Proceedings of this meeting, and was dealing with an extension of a Markov-type inequality of Peter for constrained polynomials. Proving a conjecture of Szabados, Peter established the right Markov-type inequality for all real algebraic polynomials of degree n with at least $n - k$ real zeros outside $(-1, 1)$. I recall that answering Peters friendly question what have you done? I told him my result in broken English. Not only did Peter understand my statement immediately but he replied it was expected. However, Peter seemed to like the fact that an undergraduate student extended his result to all real algebraic polynomials of degree n with at least $n-k$ zeros outside the open unit disk of the complex plane. Since then Peter published at least one paper with me in almost every year and it is not easy for me to select some of those I consider to be Peters best results with me.

*****

Greg Fee, Simon Fraser University

Time: Thursday, May 15th, 3:45 - 4:15
Room: ASB 10900

Title: Zeros and poles of Pade Approximates to the symmetric Zeta function.

Abstract: We compute Pade Approximates to Riemann's symmetric Zeta function. Next we calculate the zeros and poles of these rational functions. Lastly we attempt to fit these to algebraic curves.

*****

Michael Filaseta, University of South Carolina

Time: Friday, May 16th, 2:30 - 3:00
Room: ASB 10900

Title: Miscellaneous problems on the factorization of $0,1$-polynomials

Abstract: The speaker will discuss different problems and related results associated with the factorization, over the rationals, of polynomials all of whose coefficients are 0 and 1. In the way of examples, we mention the following questions: (i) Are almost all $0,1$-polynomials irreducible? (ii) Can a $0,1$-polynomial be divisible by the square of a non-constant non-cyclotomic polynomial? (iii) What can one say about the factorization of $1+x^{a_1}+x^{a_2}+\cdots+x^{a_n}$ if $\{a_j\}$ is an infinite sequence of positive integers that increases sufficiently fast? (iv) Is it possible to construct an infinite set S of positive integers such that $1+\sum_{t\in T} x^t$ is irreducible for all non-empty finite subsets T os S? These and a variety of other questions will be addressed.

*****

John Friedlander, University of Toronto

Time: Friday, May 16th, 9:00-10:00
Room: ASB 10900

Title: Selberg and the Sieve: A Positive Approach

Abstract: We survey the contributions of Atle Selberg to Sieve Methods. The talk is intended to be accessible to a general mathematical audience.

*****

John J.F. Fournier, University of British Columbia

Time: Tuesday, May 13th, 3:00 - 3:30
Room: ASB 10908

Title: Paley's Theorem for Hankel Matrices via the Schur Test
Abstract: Paley's theorem for lacunary coefficients of H^1-functions is equivalent to a statement about lacunary Hankel matrices acting on ℓ^2 of the nonnegative integers. That statement reduces easily to the case where the entries in the matrix are all nonnegative. So it must be provable by the Schur test. We give such a proof, with an interesting pattern in the vector used in the test. This is joint work with Bradley G. Wagner.

*****

Frank Garvan, University of Florida

Time: Wednesday, May 14th, 2:30 - 3:00
Room: ASB 10900

Title: Congruences for the rank and crank of partitions
Abstract: In 2000, Ken Ono proved that for each prime $t > 3$ there are infinitely many partition congruences $p(An + B) \equiv 0 \pmod{t}$. In 2005, Karl Mahlburg proved the analog for the crank of partitions, and recently Ken Ono and Kathrin Bringmann proved the analog for the rank of partitions using the theory of weak Maass forms. We describe a more elementary approach to these congruences that comes from a PDE found by the speaker and Oliver Atkin that connects the generating functions for the rank and crank moments. We examine the problem of finding explicit congruences. The first explicit nontrivial rank congruence was found by Atkin and Hussain in 1958. Part of the talk describes recent joint work with Kathrin Bringmann and Karl Mahlburg.

*****

Mark Giesbrecht, University of Waterloo

Time: Wednesday, May 14th, 10:15 - 10:45
Room: ASB 10900

Title: Detecting perfect powers of lacunary polynomials

Abstract: When computing with polynomials having only a few non-zero coefficients, we want algorithms whose speed is proportional only to their compact size — the number and length of non-zero coefficients, and the logarithm of their degree — and not proportional to their possibly huge degree. Many problems associated with lacunary polynomials have been proven computationally intractable, such as determining squarefreeness and computing GCDs. It is therefore heartening that we can now provide an algorithm for determining if a lacunary polynomial is a perfect power, which runs in time polynomial in its compact size. To accomplish this we employ a randomized evaluation scheme and prove its effectiveness with a character sum argument. The algorithm is shown to be fast both in theory and practice.

*****

Luis Goddyn, Simon Fraser University

Time: Wednesday, May 14th, 3:45 - 4:15
Room: ASB 10908

Title: Two Lower Bounds for Subset Sums

Abstract: I present two recent lower bounds in additive number theory. First, let A be a finite subset of an abelian group G, and let $\sum(A)$ be the set of group elements representable as a sum of a subset of A. Then

$$|\sum(A)| \geq |H| + 1/64\, |A - H|^2 .$$

Here H is the stabilizer of $\sum(A)$. This implies a result of Erdös/Heilbronn, and improves a difficult theorem of Van Vu regarding the integers modulo n.

Second, let $\mathcal{A} = (A_1, A_2, \ldots A_n)$ be a sequence of finite subsets of G, and let $\sum_k(\mathcal{A})$ denote the set of group elements representable as a sum of k elements taken from distinct sets in $\mathcal{A}$. We prove the following generalization of Kneser's addition theorem.

$$|\sum_k(\mathcal{A})| \geq |H| \left(1 - k + \sum_Q \min\{k, r(\mathcal{A}, Q)\}\right) .$$

Here H is the stabilizer of $\sum_k(\mathcal{A})$, and Q runs over the H-cosets of G, and $r(\mathcal{A}, Q)$ counts the sets in $\mathcal{A}$ which intersect Q. This bound is a very special case of a little-known conjecture of Schrijver/Seymour regarding group-weighted matroids. Our bound implies a several results and conjectures by Cao, Gao, Grynkiewicz, Hamidoune, and Bollobás/Leader, mostly in the spirit of the following classic of Erdös/Ginsberg/Ziv: *Every set of* $2n-1$ *integers, contains an* n*-subset which sums to* 0 *modulo* n.

These are joint works with Matt DeVos, Bojan Mohar, and Robert Šámal.

*****

Ron Graham, University of California, San Diego

Time: Friday, May 16th, 1:15-2:15
Room: ASB 10900

Title: Iterated Partitions of Triangles

Abstract: There are many ways in which one can subdivide a triangle into smaller triangles. However, the limiting behavior when various methods of partitioning are iterated can be quite different. In this talk, we will describe some recent results for this problem, which include a few facts that we can prove, and a large set of conjectures arising from computational experiments that we cannot (yet) prove.

*****

Jens Happe, MDA Corporation

Time: Thursday, May 15th, 4:15 - 4:45
Room: ASB 10908

Title: On the relationship between the nonreal zeros and the Fourier Critical Points of real polynomials

Abstract: Geometry of Polynomials is a field notorious for its simple-sounding conjectures, some of which may even have simple and elegant solutions, that nonetheless have remained open for decades (Sheil-Small). Some famous examples include the Ilieff-Sendov conjecture and the Hawaii Conjecture. This talk outlines a conclusive treatment of an even older, admittedly nebulous conjecture posed by Gauss in 1833 and re-stated by Pólya in 1930:

Given a polynomial p of degree n with real coefficients, consider the sequence $(\operatorname{sgn} p(x), \operatorname{sgn} p'(x), \ldots, \operatorname{sgn} p^{(n)}(x))$ $(x \in \mathbb{R})$, and determine the points x at which sign changes of the form $+-+ \to +++$ or $-+- \to ---$ occur anywhere within this sequence (these are called the Fourier Critical Points), and the total number k of such occurrences. It is easy to show that k is equal to the number of conjugate pairs of nonreal zeros of p; Gauss' conjecture states that there exists a unique mapping between *specific* pairs of zeros and *specific* Fourier critical points.

We answer this conjecture by constructing, given a polynomial p and an argument parameter $c \in (0, \pi)$, a unique mapping from a partition of (pairs of) nonreal zeros to sets of Fourier Critical Points. The construction is geometric and offers a nice graphical visualization in the complex plane. We further characterize the cases in which single pairs are mapped to single critical points. Even in those cases, however, the dependency on the parameter c cannot be removed in general. We provide an example of a polynomial where two different values of c give rise to two different mappings.

The talk covers M.Sc. work done with Peter Borwein in 1994/5 but also gives an overview of more recent development in the field.

*****

Kevin Hare, University of Waterloo

Time: Monday, May 12th, 9:15-10:15
Room: ASB 10900

Title: A history of, and recent results on Beta-expansion.

Abstract: That base 10 number system has not always enjoyed the popularity that it does today. Though out history, many different bases systems have been used. (Examples include 5, 8, 10, 12, 20, 60.) More recently [Rényi, 1957] started investigations into the case when the base is a non-integer real number. We say that x has a beta-expansion with base β and digits S if $x = \sum_{i \geq N} a_i \beta^{-i}$ with the $a_i \in S$. Numerous results on these beta-expansions have been developed. This talk will give a history of these beta-expansions, and some of the results on them. Recent work and some open problems about beta-expansions will also been presented.

*****

Warren Hare, Simon Fraser University

Time: Thursday, May 15th, 4:45 - 5:15
Room: ASB 10900

Title: Mathematical Challenges and Aides to Tuning Models to Complex Social Systems

Abstract: Complex social systems are any system that is governed at least partially by social dynamics. In developing mathematical models of complex social systems, one is often left with a incomplete picture of the system being modelled. In particular most models contain parameters that are unmeasurable by standard data collection techniques. (For example, the societal ratio to which one values family-time over increased income.)

Determining best approximations for these parameters is typically done by a system of trial and error, seeking a combination of parameters that result in the model fitting a known data set. In this talk we discuss how using derivative free optimization can automate this process and vastly improve over all fit. An example model regarding Home and Community Care in British Columbia is given.

*****

Brett Hemenway, University of California, Los Angeles

Time: Tuesday, May 13th, 4:15 - 4:45
Room: ASB 10908

Title: Locally-Decodable Codes based on Hidden Chinese Remaindering

Abstract: Using techniques from the field of Private Information Retrieval we show how to construct an error correcting code which is locally-decodable in the computationally bounded channel model. Our code has constant information rate, and can recover from constant error rate, but what distinguishes it from existing error correcting codes is its local-decodability property. Specifically, we can recover any bit of the plaintext by reading only a small portion of the (corrupted) codeword. We achieve this by working in the computationally bounded channel model, where we view the channel as an adversary who can corrupt bits of the codeword, but is limited to "feasible" computation. By working in this restricted model, we are able to use standard cryptographic protocols, which, combined with the well-known Chinese

Remainder Error Correcting Code, allows us to create a locally-decodable code which is much more efficient than all existing codes in the unbounded channel model.

Efficient locally-decodable codes are highly desirable for encoding large pieces of data of which only small portions are accessed at a given time. For example any kind of database. In the unbounded channel model, the best known locally-decodable codes have codewords that grow almost exponentially in the size of the plaintext. Our code, by making use of standard cryptographic hardness assumptions, achieves codewords that are only a constant times larger than the plaintext.

*****

Colin Ingalls, University of New Brunswick

Time: Friday, May 16th, 10:15 - 10:45
Room: ASB 10900

Title: Noncommutative Surfaces
Abstract: We present some examples of noncommutative algebraic surfaces and discuss their birational classification.

*****

Matt Klassen, DigiPen Institute of Technology

Time: Thursday, May 15th, 11:30 - 12:00
Room: ASB 10908

Title: Generalized Van der Monde Determinants, Interpolation, and Splines
Abstract: To solve for the interpolating polynomial in the standard monomial basis, one writes down a linear system whose determinant is Van der Monde and is thus computable with the well-known product formula. The analogous linear system for the Hermite interpolation problem is also easily solvable but the coefficient matrix does not have a Van der Monde determinant. We show that there is, however, a similar product formula for this determinant which generalizes the Van der Monde case. We also show how these determinants arise in computing coefficients for the basis change between various polynomial spline bases.

*****

George Labahn, University of Waterloo

Time: Monday, May 12th, 10:30 - 11:00
Room: ASB 10900

Title: Recent Developments in Order Bases

Abstract: Order bases provides a mechanism for describing all the solutions of certain rational approximation problems (as a module). They are used for various Padé approximation problems, for inversion formulae for structured matrices, for guessing recurrence formulae and for finding matrix normal forms (for example, Popov forms). There are a number of fast algorithms to compute such bases. In this talk we will describe some recent developments for the use of and also the computation of order bases.

*****

Petr Lisoněk, Simon Fraser University

Time: Thursday, May 15th, 10:45 - 11:15
Room: ASB 10900

Title: On zeros of Kloosterman sums

Abstract: For $q = p^m$ and $a \in \mathbb{F}_q$ we define the Kloosterman sum $K(a) = 1 + \sum_{x \in \mathbb{F}_q^*} \omega^{\mathrm{Tr}\left(x^{-1}+ax\right)}$ where $\omega = e^{2\pi i/p}$. Kloosterman sums find applications in areas such as crosscorrelation of sequences or construction of bent functions. One problem of particular interest is to find $a \in \mathbb{F}_q$ for which $K(a) = 0$. We discuss some computational methods for this goal when $p = 2, 3$. These methods are based on the association of Kloosterman sums with the number of $\mathbb{F}_q$-rational points on certain elliptic curves.

*****

Friedrich Littmann, North Dakota State University

Time: Tuesday, May 13th, 10:15 - 10:45
Room: ASB 10908

Title: Approximation of functions that are analytic in a strip

Abstract: Let $f : \mathbb{R} \to \mathbb{R}$. The topic of this talk is approximation of f by an entire function G of fixed exponential type such that $G \geq f$ on $\mathbb{R}$. We will present a construction that starts with an identity $1 = F(x)\mathcal{L}[g](x)$ where $\mathcal{L}$ denotes the two-sided Laplace transform. With a suitable interpretation of $f(D)$ with $D = d/dx$ an interpolation to f is defined via

$$G_F(x) = F(x)\mathcal{L}[f(D)g](x).$$

Different choices of F in this formula give different approximations to f. The method is illustrated by considering $f(x) = \cosh(ax)^{-1}$. As an application, approximation theorems for functions that are analytic and bounded in a horizontal strip of height $2a$ are obtained.

*****

Doron Lubinsky, Georgia Institute of Technology

Time: Monday, May 12th, 11:45 - 12:15
Room: ASB 10900

Title: On the q disease on the unit circle

Abstract: Peter Borwein often uses different aspects of $q-$series in his research. Peter and his collaborators have investigated the irrationality of various types of $q-$series, and established and applied various $q-$series identities. Peter has also been interested in a problem of Erdős and Szekeres about the size of

$$\frac{1}{2\pi}\int_{|q|=1}\left|\prod_{j-1}^{n}(1-q^{\alpha_j})\right||dq|,$$

where the $\{\alpha_j\}$ are positive integers. This can be thought of as a problem about q series for the exotic case of q on the unit circle.

We review some problems about q-series for q on the unit circle, such as
(I) The role of the partial theta function

$$h_q(z) = \sum_{j=0}^{\infty} q^{\frac{j(j-1)}{2}} z^j$$

in resolving the Baker-Gammel-Wills Conjecture for Padé approximants.
(II) The growth of the q Pochhammer symbol

$$\prod_{j-1}^{n}\left(1-q^j\right)$$

for q on the unit circle;
(III) The definition of q exponential and $q-$gamma functions for q on the unit circle.

*****

Greg Martin, University of British Columbia

Time: Thursday, May 15th, 3:00 - 3:30
Room: ASB 10908

Title: Absolutely abnormal numbers

Abstract: Almost all real numbers are absolutely normal - that is, the digits in their decimal-like expansion to any base occur in all possible configurations with the expected frequencies. However, not one explicit example of an absolutely normal number is known. In this talk we investigate the opposite extreme, numbers that are normal to no base whatsoever, and we describe a construction of uncountably many explicit (irrational) examples of these absolutely abnormal numbers.

*****

Idris Mercer, York University

Time: Thursday, May 15th, 4:45 - 5:15
Room: ASB 10908

Title: The cosine problem

Abstract: The "cosine problem" of Chowla is a fifty-year-old problem lying on the border between number theory and classical analysis, and is far from completely solved. In this talk, we describe some partial results and discuss a variety of tools that have been used to attack the cosine problem. Of particular interest to us is the (perhaps under explored) question of the finiteness of the problem.

*****

Victor Moll, Tulane University

Time: Monday, May 12th, 2:45 - 3:15
Room: ASB 10900

Title: 2-adic valuations of a sequence arising from a rational integral
Abstract: In the study of the rational integral

$$N_{0,4}(a;m) := \int_0^\infty \frac{dx}{(x^4+2ax^2+1)^{m+1}}$$

we found the sequence

$$d_l(m) := 2^{-2m} \sum_{k=l}^{m} 2^k \binom{2m-2k}{m-k} \binom{m+k}{k} \binom{k}{l}.$$

We present a binary tree that describes the 2-adic valuation of $\{d_l(m) : 0 \leq l \leq m\}$. This lead us to consider the arithmetical properties of Stirling numbers of the second kind. We discuss a conjecture on the structure of their 2-adic valuation.

Joint work with T. Amdeberhan, D. Manna and X. Sun.

*****

Michael Monagan, Simon Fraser University

Time: Thursday, May 15th, 12:00 - 12:30
Room: ASB 10908

Title: How fast can we multiply and divide sparse polynomials?
Abstract: Most of today's computer algebra systems use either a sparse distributed data representation for multivariate polynomials or a sparse recursive representation. For example Magma, Maple, Mathematica, and Singular use distributed representations as their primary representation. Macsyma, REDUCE, and TRIP use recursive representations. In 1984 David Stoutemyer suggested "recursive dense" as an alternative and showed that it was the best overall across the Derive test suite. Of the newer systems, only Pari uses recursive dense.

In 2003, Richard Fateman compared the speed of polynomial multiplication in many computer algebra systems. He found that Pari was clearly the fastest system on his benchmarks. His own implementation of recursive dense came in second. So is recursive dense best?

In this talk we take another look at the sparse distributed representation with terms sorted in a monomial ordering. Our algorithms for polynomial multiplication and division use an auxiliary data structure, a "chained heap of pointers". Using a heap for polynomial arithmetic was first suggested by Stephen Johnson in 1974 and used in the Altran system. But the idea seems to have been lost.

Let $h = fg$ where the number of terms in f, g, and h are $\# \ f$, $\# \ g$, and $\# \ h$. The heap gives us the following:

- It reduces the number of monomial comparisons to $O(\#f\#g \log \min(\#f, \#g))$.
- For dense polynomials, chaining reduces this to $O(\#f\#g)$.
- By using $O(1)$ registers for bignum arithmetic, multiplication can be done so that the terms of the product fg are output sequentially with no garbage created.
- The size of the heap is $O(\min(\#f, \#g))$ which fits in the cache.
- For polynomials with integer coefficients, the heap enables multivariate pseudo-division - our division code is as fast as multiplication.

In the talk I would like to first show how Maple, Singular, TRIP and Pari represent polynomials. Second I will show how pointer heaps work for multiplying and dividing polynomials. Third, some benchmarks, comparing Maple, Magma, Singular, Trip, and Pari. The benchmarks suggest pointer heaps are really really good. Fourth, I will show some of the other "necessary optimizations" needed to get high performance. The most important one is to encode monomials into a single word.

This is joint work with Roman Pearce at Simon Fraser University.

*****

Michael J. Mossinghoff, Davidson College

Time: Tuesday, May 13th, 1:15 - 2:15
Room: ASB 10900

Title: Peter Borwein, Plane Geometry, Polynomials, and Polygons

Abstract: Peter Borwein has long been involved with research on polynomials in number theory and analysis, in particular, on polynomials with restricted coefficients and prescribed factors. However, some of his earliest work treated some problems in combinatorial geometry involving arrangements of lines and points in the plane. We describe a sampling of his work in these fields, first in geometry, then on polynomials, and then we describe a problem that brings together both of these interests: For a fixed positive integer n, how many different convex polygons with n sides and unit diameter have maximal perimeter? This problem, which dates to a question of Karl Reinhardt in 1922, can be recast as a problem about polynomials with restricted coefficients and prescribed vanishing. We describe this connection, and discuss some recent results obtained both on this problem and on related questions.

*****

Nathan Ng, University of Ottawa

Time: Friday, May 16th, 10:45 - 11:15
Room: ASB 10900

Title: The distribution of the Mobius function in short intervals

Abstract: In this talk we study the distribution of the Mobius function in a short interval $[x, x+h]$ with x less than N. We give an argument which suggests that the distribution is approximately normal with mean 0 and variance $6h/\pi^2$. This argument is based on Montgomery and Soundararajan's work on primes in short intervals.

*****

Bruce Richmond, University of Waterloo

Time: Tuesday, May 13th, 10:45 - 11:15
Room: ASB 10900

Title: On the maximum of the Stirling numbers

Abstract: Say an integer n is *exceptional* if the maximum Stirling number of the second kind $S(n,k)$ occurs for two (of necessity consecutive) values of k. We with Graeme Kemkes and Donatella Merlini have shown that the number of exceptional integers less than or equal to x is $O\left(x^{1/2+\epsilon}\right)$ for any $\epsilon > 0$. We derive a similar result for partitions of n into exactly k parts $p(n,k)$. The estimates of Bombieri and Pila for lattice points on convex curves and the asymptotic behaviour of $S(n,k)$ and $p(n,k)$ are required.

*****

Sinai Robins, Nanyang Technological University

Time: Monday, May 12th, 12:15 - 12:45
Room: ASB 10900

Title: New measures of discrete volumes for polytopes whose vertices have arbitrary real coordinates

Abstract: We extend many theorems from the context of solid angle sums over polytopes with rational vertices to the context of solid angle sums over polytopes with real vertices. Moreover, we consider any real dilation parameter, as opposed to the traditional integer dilation parameters. One of the main results is an extension of I.G. Macdonald's solid angle quasi-polynomial for rational polytopes to a real analytic function of the dilation parameter, for any convex polytope with vertices that have arbitrary real coordinates. This is joint with David DeSario.

*****

Renate Scheidler, University of Calgary

Time: Monday, May 12th, 4:00 - 4:30
Room: ASB 10900

Title: Construction of all cubic function fields of a given discriminant

Abstract: For any odd prime power $q \equiv -1 \pmod 3$ and any squarefree polynomial D in $\mathbb{F}_q[t]$ of even degree, we present an algorithm for generating all cubic function fields of discriminant D. In the case where the leading coefficient of D is not a square in $\mathbb{F}_q$, i.e. D is the discriminant of an unusual hyperelliptic function field, we make use of the infrastructure of the associated dual real hyperelliptic function field of discriminant $-3D$. This technique was first proposed by D. Shanks for cubic number fields in an unpublished manuscript from the 1970s.

*****

Chris Sinclair, University of Colorado

Time: Tuesday, May 13th, 4:15 - 4:45
Room: ASB 10900

Title: Repulsion between imaginary quadratic numbers on the unit circle
Abstract: Let K be a fixed imaginary quadratic extension of Q. We prove that the algebraic numbers in K on the unit circle are equidistributed. Generalizations of this fact will be presented. This is joint (ongoing) work with Kathleen Petersen.

*****

Chris Smyth, Edinburgh University

Time: Wednesday, May 14th, 11:30 - 12:00
Room: ASB 10900

Title: Lehmer's problem for integer symmetric matrices
Abstract: In joint work with James McKee, we show that the Mahler measure of an integer symmetric matrix is either 1 or at least Lehmer's number 1.176... . We exhibit all the extremal matrices.

*****

Cam Stewart, University of Waterloo

Time: Thurdsay, May 15th, 9:00-10:00
Room: ASB 10900

Title: Neighbouring Powers

Abstract: Let m and n be coprime integers with $n > m > 1$. How close can the nth power of a positive integer and the mth power of a positive integer be to each other without being zero? It follows from work of Baker, Sprindzuk and Schmidt that the difference between them tends to infinity as the size of the powers tends to infinity. In this talk we shall discuss some recent work with F.Beukers where we study bounds on how quickly the difference tends to infinity.

*****

Agnes Szanto, North Carolina State University

Time: Monday, May 12th, 11:00 - 11:30
Room: ASB 10900

Title: Moment matrices, trace matrices and the radical of ideals

Abstract: Let I be an ideal in $C[x_1, \ldots, x_m]$ generated by polynomials $f_1, \ldots, f_s$, and assume that the factor algebra $A = C[x_1, \ldots, x_m]/I$ is finite dimensional over the complex field C. In this talk we give a simple algorithm to compute matrices of traces of A with respect to some basis of A. Matrices of traces play an important role in real and complex algebraic geometry: for example their rank is equal to the number of distinct complex roots of I, and their signature is equal to the number of real roots of I. Previous methods computing matrices of traces include the use of Newton Sums, residues or the computation of high powers of multiplication matrices of I.

We propose a method using linear algebra on the Sylvester matrix of $f_1, \ldots, f_s$ and a polynomial F to compute matrices of traces for A. Here F is a generalization of the Jacobian of a well-constrained system, i.e. when $s = m$. These matrices of traces in turn allow us to compute a system of multiplication matrices of the radical ideal of I, such that these multiplication matrices are simultaneously diagonalizable with eigenvalues which are the coordinates of the distinct complex roots.

This is a joint work with Itniut Janovitz Freireich, Lajos Ronyai and Bernard Mourrain.

*****

Sziklai, Peter, Eotvos University

Time: Friday, May 16th, 3:00 - 3:30
Room: ASB 10900

Title: An extreme polynomial with two variables

Abstract: For every positive integer n, Peter Borwein, T. Erdélyi and G. Kós [1] constructed a polynomial $q(x)$ such that $\deg q < c\sqrt{n}$ and $q(0) > |q(1)| + |q(2)| + \ldots + |q(n)|$. This tool has been applied to answer some questions about polyonomials with restricted coefficients and to provide lower bounds on the solutions of the Prouhet-Tarry-Escott problem. Krasikov and Roditty also used this tool for reconstruction of sequences from subsequences [2].

Here we present a generalization with two variables. For an arbitrary nonempty set $H \subset \{1, 2, \ldots, n\}2$ of lattice points, we prove that there exists a point $(a, b) \in H$ and a polynomial $q(x, y)$ such that $\deg q < cn^{2/3}$ and

$$q(a, b) > \sum_{(x,y)\in H\setminus\{(a,b)\}} |q(x, y)|.$$

This polynomial has applications in reconstruction of matrices from its submatrices of a given size [3].

This is a joint work with Géza Kós and Péter Ligeti.

References

[1] P. Borwein, T. Erdélyi, G. Kós, *Littlewood-Type Problems on* $[0, 1]$. Proc. London Math. Soc. **79** No. 1 (1999), 22–46.

[2] I. Krasikov, Y. Roditty, *On a reconstruction problem for sequences.* J. Combin. Theory Ser. A **77** No. 2 (1997), 344–348.

[3] G. Kós, P. Ligeti, P. Sziklai: *Matrix reconstruction from submatrices* Mathematics of Computation, submitted in 2008

*****

Jeffrey Vaaler, University of Texas

Time: Wednesday, May 14th, 12:00 - 12:30
Room: ASB 10900

Title: A Banach space determined by the Weil height

Abstract: Let $\overline{\mathbb{Q}}^{\times}$ denote the multiplicative group of nonzero algebraic numbers. Write $\mathrm{Tor}\{\overline{\mathbb{Q}}^{\times}\}$ for its torsion subgroup, and $\mathcal{G} = \overline{\mathbb{Q}}^{\times}/\mathrm{Tor}\{\overline{\mathbb{Q}}^{\times}\}$ for the quotient group. The absolute logarithmic Weil height is well defined on $\mathcal{G}$ and induces a metric topology in this group. We show that the completion of this metric space is a Banach space over the field $\mathbb{R}$ of real numbers. We further show that this Banach space is isometrically isomorphic to a co-dimension one subspace of $L^1(Y, \mathcal{B}, \lambda)$, where Y is a certain totally disconnected, locally compact space, $\mathcal{B}$ is the σ-algebra of Borel subsets of Y , and λ is a certain measure satisfying an invariance property with respect to the absolute Galois group $\mathrm{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})$. Some applications and related open problems will also be discussed.

Joint work with Daniel Allcock.

*****

Alexa van der Waal, Simon Fraser Univesrity

Time: Tuesday, May 13th, 4:45 - 5:15
Room: ASB 10900

Title: Priority based allocation of police resources to crime related investigations.

Abstract: This talk considers a model that theoretically studies the allocation of police resources to the investigation of two kinds of crimes. A priority scheme is taken such that the resources are used to investigate one of the crime types first. The remainder is then used for the investigation of the other crimes. Restrictions on some model parameters are determined analytically, in order to achieve a “real life” equilibrium.

*****

Joris Van Deun University of Antwerpen

Time: Friday, May 16th, 3:45 - 4:15
Room: ASB 10900

Title: The Riemann zeta function and asymptotics for Stieltjes fractions

Abstract: We study the asymptotic behaviour of the coefficients in the continued fractions corresponding to Stieltjes transforms of weight functions on a finite interval. It is shown that, in general, the coefficients with odd and even index converge to a different limit. For a specific class of weights a detailed asymptotic expansion of the coefficients is obtained. Some examples serve as illustration and an application to continued fraction expansions for the Riemann ζ function is given.

*****

Hugh Williams, University of Calgary

Time: Wednesday, May 14th, 9:00-10:00
Room: ASB 10900

Title: Primality Proving, Polynomials and Sieving

Abstract: The problem of establishing with full mathematical rigour that a given integer is a prime is called the problem of primality proving. The recent proof by Agrawal, Kayal and Saxena that primality proving of N can be done in deterministic polynomial time has stimulated a lot of research into just how efficiently we could expect to do this. However, proving an integer N, suspected of being a prime, to actually be one is much more time-consuming than employing probabilistic tests that can at best determine only that N behaves in certain respects like a prime. Because of this, despite their lack of rigour, these probabilistic tests are used by the cryptographic community to identify primes. In this talk I show how some probabilistic tests for primality (including the well-known Miller-Rabin test) can be converted to algorithms for primality proving. In order to use these techniques we need to compute certain pseudopowers.

Suppose r and p are primes such that $r \,|p-1$. Let $f(x) = xra$ be a polynomial over the integers such that $(r, a) = 1$ and $f(x) \equiv 0 \pmod{q}$ is solvable for $q = r^2$ (r^3 in the case of $r = 2$) and all primes $q \leq p$ such that $r \,|q-1$. We denote the least positive value of a which is not divisible by any

prime les than p and is not a perfect rth power by $M_{p,r}$ and we call $M_{p,r}$ a pseudo rth power.

The process of finding these numbers has always involved the use of a device called a number sieve. This machine detects pseudopowers simply by searching through all integers up to a certain, pre-selected bound. While this approach may sound naive, it is in fact possible through a judicious exploitation of parallelism to make these devices execute at a very rapid rate; indeed, the use of these machines is the fastest method known for finding pseudopowers.

Assuming reasonable heuristics (which have been confirmed for numbers to 2^{80}), pseudosquares can be used to provide a deterministic primality test in time $O((\log N)^{3+o(1)})$, which some believe might be best possible. While the case of $r = 3$ seems to lead to a more efficient primality testing algorithm than $r = 2$, we argue that extending to any $r > 3$ does not appear to lead to any further improvements.

*****

Soroosh Yazdani, University of Berkeley

Time: Thursday, May 15th, 10:15 - 10:45
Room: ASB 10900

Title: On maximality of Certain Littlewood Polynomials

Abstract: In the paper [1] it was proved that Fekete polynomials satisfy a certain extremal property amongst all Littlewood polynomials of odd degree. Specifically for an odd integer n, if $f(x) = \sum_{i=1}^{n-1} a_i x^i$ with $a_i = \pm 1$ and $a_1 = 1$, and we have $\max_{\zeta^n=1} |f(\zeta)| \leq \sqrt{n}$, then $a_i = \left(\frac{i}{n}\right)$ for all i.

In this talk we focus on the same problem when n is even. Computer calculation suggests that in this case $\max_{\zeta^n=1} |f(\zeta)| \leq \sqrt{n+1}$, with equality being achieved only if $n + 1$ is a power of a prime integer. We study some of the properties that such polynomials must satisfy.

This is joint work with K. Hare.

References

[1] P. Borwein, K. K. Choi, and S. Yazdani, *Extremal Property of Fekete Polynomials*, Proc. Amer. Math. Soc. **129**, (2001) 19–27

*****

Ping Zhou, St. Francis Xavier University

Time: Tuesday, May 13th, 2:30 - 3:00
Room: ASB 10908

Title: Padé Approximants Associate with Functional Equations

Abstract: The method to explicitly construct Padé approximants to some functions by using functional equations and the residue theorem, developed by Peter Borwein, will be introduced. Then we will discuss the applications of this method in explicit constructions of multivariate pad approximants to some multivariate functions which satisfy some functional equations.

*****

S. P. Zhou, Institute of Mathematics, Zhejiang Sci-Tech University

Time: Tuesday, May 13th, 12:00 - 12:30
Room: ASB 10900

Title: Convergence Problems of Some Fourier Series

Abstract: It is well known that Fourier analysis plays an important role in pure mathematics and has many important applications in science and technology. Convergence problems of Fourier (trigonometric) series are very fundamental to establish a solid basis for Fourier analysis.

After a brief review of the history of convergence problems of Fourier (trigonometric) series, we will discuss our very recent development: the ultimate condition to generalize monotonicity for the uniform convergence of some trigonometric series.