TALK INFORMATION FOR FIELDS–IRMACS WORKSHOP: DISCOVERY AND EXPERIMENTATION IN NUMBER THEORY

1. Plenary speakers

Speaker: David H. Bailey, *Lawrence Berkeley National Lab*

Title: High-Precision Arithmetic and Experimental Mathematics

Abstract: One technique employed in the emerging "experimental" methodology of mathematical research is to compute some mathematical object to high precision, then to utilize techniques such as the PSLQ integer relation to identify the constant as an expression involving well-known mathematical constants. In the past two or thee years, this methodology has been applied with striking success to the age-old problem of evaluating integrals. In particular, hundreds of integrals, many of them arising in applied disciplines such as mathematical physics and mathematical biology, have been computed to high precision, identified numerically, then proven by formal means. These include some problems that have resisted solution for many years. (joint work with Jonathan M. Borwein)

Note: Attending at IRMACS.

Speaker: Dan Bernstein, *University of Illinois at Chicago*

Title: Addition laws on elliptic curves

Abstract: TBA

Note: Attending at Toronto.

Speaker: Jonathan M. Borwein, *University of Newcastle*

Title: Exploratory Experimentation and Computation

Abstract: The mathematical research community is facing a great challenge to re–evaluate the role of proof in light of the growing power of current computer systems, of modern mathematical computing packages, and of the growing capacity to data-mine on the Internet. Add to that the enormous complexity of many modern capstone results such as the Poincaré conjecture, Fermat's last theorem, and the Classification of finite simple groups. As the need and prospects for inductive mathematics blossom, the requirement to ensure the role of proof is properly founded remains undiminished.

I shall look at the philosophical context and then offer five bench-marking examples of the opportunities and challenges we face, along with some interactive demonstrations.

Note: Attending at IRMACS.

Speaker: Michael Filaseta, *University of South Carolina*

Title: Open Problems on Covering Systems

Abstract: There has been several recent papers on covering systems of the integers. In this talk, I will survey a variety of results associated with covering systems of the integers with some emphasis on what we don't know. As an example, one topic to be surveyed is that of Sierpiński numbers, positive odd integers

Date: September 22–26, 2009.

k with the property that $k \cdot 2^n + 1$ is composite for all positive integers n. We will, for example, consider a still open problem posed by P. Erdős to determine whether every such positive integer k can be obtained from an appropriate covering system of the integers. Formulating this more accurately leads to yet other interesting questions.

Note: Attending at Fields.

SPEAKER: Jeff Lagarias, *University of Michigan*

TITLE: Ternary Expansions of Powers of 2

ABSTRACT: P. Erdős raised the question whether there are infinitely many integers n such that the ternary expansion of $2n$ omits the digit 2. We discuss this question, and generalize it to viewing $\{2n : n \geq 1\}$ as a special case of an orbit of a dynamical system acting on the real numbers, and of a second dynamical system acting on the 3–adic integers. The set of orbits having infinitely many elements with the property above should be "small". This leads to new questions about the sizes of intersections of multiplicative translates of 3–adic Cantor sets, which are investigated experimentally. The latter reports on joint work with an REU student, Will Abram (U. Chicago).

Note: Attending at Fields

SPEAKER: Hendrik Lenstra, *Mathematisch Instituut, Universiteit Leiden*

TITLE: Profinite Fibonacci numbers

ABSTRACT: Profinite numbers form an important technical tool in several parts of algebraic number theory and arithmetic geometry. While many of their properties resemble those of their nearest cousins, the rings of p–adic numbers, which occupy a similar position at the cross–roads of number theory and topological algebra, there are also a number of fascinating differences. The lecture will present an experimental and informal approach to profinite numbers, using Fibonacci numbers and their power series developments to illustrate some of their surprising features.

Note: Attending at Fields.

SPEAKER: Greg Martin, *University of British Columbia*

TITLE: The ABCDEs of collaborating with your computer

ABSTRACT: Even we practitioners of pure mathematics find ourselves using the computational power of modern computers and software increasingly in our working lives. As this workshop proclaims, Experimentation and Discovery are now more possible than ever, and the extent of raw Computation continues to expand; however, these computational systems can also act as Backup researchers for us and even as new ways to Access the mathematical literature. In this talk, I'll lead a guided tour of some aspects of my past research that employed each of these five benefits of our mathematical technology.

Note: Attending at IRMACS

SPEAKER: Michael Mossinghoff, *Davidson College*

TITLE: Wieferich Madness

ABSTRACT: A Barker sequence is a finite sequence of integers $\{a_i\}$, each ± 1, for which every sum $\sum_i a_i a_{i+k}$ with $k \neq 0$ is -1, 0, or 1. It is unknown if any Barker sequences exist with length $n > 13$, although a number of necessary conditions on their existence have been established, so restrictive in fact that no value of $n > 13$ was even known that satisfied all of the requirements. We describe a large computational investigation that significantly improves the best known lower bound on the length of a long Barker sequence. The computation

involves a large search for Wieferich prime pairs (q, p), which are defined by the property that $q^{p-1} \equiv 1 \bmod p^2$. We also describe some connections with other open problems in number theory, combinatorics, and analysis.

Note: Attending at IRMACS.

SPEAKER: Ram Murty, *Queen's University*

TITLE: Ramanujan and the Zeta Function

ABSTRACT: Ramanujan stated several interesting formulas for $\zeta(2k+1)$ which involve (what are now called) Eichler integrals. There are some interesting features of these formulas which we will explore in this talk. The most notable is the appearance of a polynomial which we call the Ramanujan polynomial. We present some numerical evidence that seems to suggest that the non-real zeros of this polynomial lie on the unit circle.

Note: Attending at Fields.

SPEAKER: Chris Sinclair, *University of Oregon*

TITLE: Patterns and Periodicity in a Family of Resultants

ABSTRACT: Given a monic polynomial with integer coefficients, F, we may create a new monic polynomial with integer coefficients, F_m, by raising all of the roots of F to the power m. In 1979, Edward Dobrowolski showed that, if p is a prime and N is the degree of F, then p^N divides the resultant of F and F_p. He then used this result to give the best known asymptotic lower bound for the Mahler measure of a non-cyclotomic integer polynomial as a function of the degree (Lehmer's conjecture asserts the existence of a constant for this quantity–Dobrowolski's lower bound is a very very slowly decaying function of the degree). Two colleagues, Kevin Hare and David McKinnon, and myself considered divisibility results similar to Dobrowolski's among resultants of the form $\mathrm{Res}(F_m, F_n)$. Considering this as a function of m and n, striking patterns emerge. I will discuss these patterns, as well as give a sketch of the derivation of Dobrowolski's lower bound.

Note: Attending at IRMACS.

SPEAKER: Cam Stewart, *University of Waterloo*

TITLE: Neighbouring Powers

ABSTRACT: Let m and n be coprime positive integers larger than 1. In this talk we shall discuss the problem of determining how small the difference of an m–th power of a positive integer and the n–th power of a positive integer can be without being 0. (joint work with F. Beukers and W. van der Bilt)

Note: Attending at Fields

SPEAKER: Karen Yeats, *Simon Fraser University*

TITLE: Patterns in Feynman periods

ABSTRACT: Massless scalar Feynman integrals in 4 dimensions give number theoretically interesting values, multiple zeta values in known examples. However a systematic understanding is lacking. Mathematicians tackle this problem both from the top down and from the bottom up. My tastes and those of the conference favor the latter.

Calculating such Feynman integrals, even numerically, is difficult. None-the-less the available data is full of unexplained patterns. I will explain the set-up and some recent results with Francis Brown.

Note: Attending at IRMACS.

2. Invited Talks (Fields)

Speaker: Andrew Bremner, *Arizona State University*

Title: Rational points on $y^2 = x^n + k$

Abstract: Some parameterizations of points on the title curve are given (joint work with Maciej Ulas).

Speaker: Timothy Caley, *University of Waterloo*

Title: The Prouhet–Tarry–Escott Problem over the Gaussian Integers

Abstract: The Prouhet–Tarry–Escott (PTE) Problem is a classical number theoretic problem which asks for integer solutions to sums of equal powers. Solutions to the PTE problem give improved bounds for the "Easier" Waring problem, but they are very difficult to find using conventional methods. In 2003, P. Borwein et al. described and implemented a computational method to find solutions to the PTE problem. The PTE problem over the Gaussian integers and other unique factorization domains will be discussed, including generalizations of results from the literature and the above method of Borwein et al. Finally, there will be a statement of open questions relating to the PTE problem.

Speaker: Marc Chamberland, *Grinnell College*

Title: Beautiful Sums: from Ramanujan to Apery

Abstract: Beautiful sums, both finite and infinite, have long been witnessed in number theory. This talk shows how computer algebra systems can used to discover and occasionally prove results for various sums. This includes generalizing equations due to Ramanujan and Apery, sums of squares motivated by geometry, combinatorial identities arising from matrix factorization, and BBP infinite series.

Speaker: Morley Davidson, *Kent State University*

Title: From covering congruences to Rubik's Cube: a distributed computing experiment

Abstract: This talk will summarize results from a computational group theory experiment carried out with Joseph Miller and Bruce Norskog which was initially sparked by this number-theoretic notion. Efficient semi-rectangular coverings of certain stabilizer subgroups are constructed, thereby bringing the Toronto-born, two-step endgame approach of Zborowski and Bruchem more in line with human memory and time limitations. As an illustration we consider the so-called superflip, one of the relatively few permutations known to require 20 moves to solve; a 22-move solution is given based on a popular five-step stabilizer chain with ZB endgame.

Speaker: Bart de Smit, *Universiteit Leiden*

Title: Searching for ABC triples

Abstract: The ABC conjecture is an asymptotic statement about the quality of so-called ABC triples. For over 25 years computational techniques have been developed and applied to generate ABC triples of high quality. We report on some recent efforts involving thousands of volunteers through abcathome.com.

SPEAKER: Karl Dilcher, *Dalhousie University*

TITLE: Mod p^3 analogues of theorems of Gauss and Jacobi on binomial coefficients

ABSTRACT: The theorem of Gauss that gives a modulo p evaluation of a certain central binomial coefficient has been extended modulo p^2 by Chowla, Dwork, and Evans. In this talk we extend it further to a congruence modulo p^3. We derive a similar extension of a theorem of Jacobi. In the process we prove congruences to arbitrarly high powers of p for certain quotients resembling binomial coefficients and related to the p-adic gamma function. These congruences are of a very simple form and involve Catalan numbers as coefficients. As another consequence we obtain complete p-adic expansions for certain Jacobi sums. (Joint work with John B. Cosgrave)

SPEAKER: David Freeman, *Centrum Wiskunde & Informatica, Netherlands*

TITLE: Pairing–friendly hyperelliptic curves and Weil restriction

ABSTRACT: A "pairing–friendly curve" is a curve C over a finite field F_q such that (a) the Jacobian of C has a subgroup of large prime order r, and (b) the r–th roots of unity are contained in an extension field F_{q^k} for some small value of k.

Pairing–friendly curves have found many uses in cryptography. For such applications one wants to control the extension degree k, known as the "embedding degree," while keeping the field size q as small as possible relative to the subgroup size r.

We describe a construction of pairing-friendly genus 2 curves that, for certain embedding degrees k, achieves the smallest known ratio $\log q/\log r$ for simple, non–supersingular abelian surfaces. The proof that these curves have the desired properties relates them to Weil restrictions of elliptic curves.

We also describe some experimental results suggesting that our construction fails in certain cases. Finding alternative constructions for these cases is an open problem. (This is joint work with Takakazu Satoh of Tokyo Institute of Technology)

SPEAKER: Patrick Ingram, *University of Waterloo*

TITLE: Periodic points for polynomials over number fields

ABSTRACT: Let c be a complex number, and let $f(z) = z^2+c$. A point of period N for this function is simply a complex number z such that $f^N(z) = z$, and $f^m(z) \neq z$ for $m < N$ (where f^m denotes the m-fold iterate of f with itself). A conjecture of Poonen postulates that there are no pairs of rational numbers z and c such that z is a point of period $N > 3$ for f. We will present the results come computations (conducted jointly with Benjamin Hutz) which support this conjecture, and a similar conjecture over quadratic extensions of $\mathbb{Q}$.

SPEAKER: Tanje Lange, *Technische Universiteit Eindhoven*

TITLE: Edwards curves for ECM

ABSTRACT: This covers joint work with D.J. Bernstein, Peter Birkner and Christiane Peters.

SPEAKER: James McKee, *Royal Holloway, University of London*

TITLE: Computing totally positive algebraic integers of small trace

ABSTRACT: We construct minimal polynomials of totally real algebraic integers of small absolute trace by consideration of their reductions modulo auxiliary polynomials. Many new examples of such polynomials of minimal absolute trace (for given degree) are found. As one application, we produce a new record bound for the Schur-Siegel-Smyth trace problem.

SPEAKER: Hugh Montgomery, *University of Michigan*

TITLE: Moments of generating functions

ABSTRACT: Let $s(n)$ denote the sum of the binary digits of n, and set

$$F_J(\alpha) = \sum_{0 \le n < 2^J} (-1)^{s(n)} e(n\alpha) = \prod_{j=0}^{J-1} (1 - e(2^j \alpha)) .$$

Properties of this generating function play an important role in the recent work of Mauduit and Rivat in which it was shown that $s(p)$ is odd for asymptotically half the primes. (This settles a question posted by A. O. Gelfond in 1968.) In particular, estimates for the L^1 and L^∞ norms are required. We show that if k is a positive integer, then $\int_0^1 |F_J(\alpha)|^{2k}\, d\alpha$ satisfies a linear recurrence of order at most k.

We also consider moments of the Rudin–Shapiro polynomials on the unit circle.

SPEAKER: Georges Rhin, *Université de Metz*

TITLE: On the totally real algebraic integers with diameter less than 4

ABSTRACT: The diameter of a totally real algebraic integer α of degree d with conjugates $\alpha_1 < \alpha_2 < \ldots < \alpha_d$ is $\mathrm{diam}(\alpha) = \alpha_d - \alpha_1$. For all positive integers k, n $\mathrm{diam}(2\cos(2k\pi/n))$ is less than 4. R. M. Robinson has computed, modulo integer translations, all the totally real algebraic integers α with $\mathrm{diam}(\alpha) < 4$ for $d \le 6$. We have done the computations for all $d \le 13$. We used a large family of explicit auxiliary functions related to generalised integer transfinite diameter of real intervals. They give good bounds for the coefficients of the minimal polynomial of α. The search for the degree 13 took 365 days of CPU time on a 2.8 Ghz PC. (Joint work with Valérie Flammang and Qiang Wu)

SPEAKER: Igor Schparlinski, *Macquarie University*

TITLE: Possible Group Structures of Elliptic Curves

ABSTRACT: It is well know that the set $E(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points on any elliptic curve over finite field $\mathbb{F}_q$ for an abelian group of rank at most 2, that is, $E(\mathbb{F}_q) \cong \mathbb{Z}_n \times \mathbb{Z}_{nk}$ for some integers k and n. For a fixed q, possible values of n and k described by simple inequalities and divisibility conditions. We study the dual and appratently new question of counting $(n, k) \in [1, N] \times [1, K]$ such that $\mathbb{Z}_n \times \mathbb{Z}_{nk} \cong E(\mathbb{F}_q)$ for some q and E. (Joint work with Francesco Pappalardi and Bill Banks)

SPEAKER: Chris Smyth, *University of Edinburgh*

TITLE: Intersecting plane curves with the Euclidean algorithm

ABSTRACT: We show that, with the help of the Euclidean algorithm for polynomials, the problem of finding the intersection points of two algebraic plane curves can be reduced to the case of intersecting lines, giving an algorithm for finding these intersection points, with multiplicities. It also yields a simple proof of Bézout's theorem, giving the total number of such points. (Joint work with Jan Hilmar)

SPEAKER: Graeme Taylor, *University of Edinburgh*

TITLE: Integer Matrices with Constrained Eigenvalues

ABSTRACT: Lehmer's Problem on the Mahler measure of integer polynomials motivates the study of "cyclotomic" matrices - those with all eigenvalues in the interval $[-2, 2]$. For the rational integer case, such matrices have been completely classified, via the study of charged signed graphs. I will discuss this result, as well as my own generalizations to cyclotomic matrices/graphs over rings of integers of imaginary quadratic extensions.

SPEAKER: Michael Yampolsky, *University of Toronto*

TITLE: Diophantine conditions and computability in polynomial dynamics

ABSTRACT: TBA

SPEAKER: Soroosh Yazdani, *McMaster University*

TITLE: On Szpiro's Conjecture

ABSTRACT: In this talk we present some computations related to Szpiro's conjecture and some conjectures that are motivated by Szpiro's conjecture.

3. Invited Talks (IRMACS)

SPEAKER: Shabnam Akhtari, *Queen's University*

TITLE: Integral Points on Elliptic Curves

ABSTRACT: I will describe a general method for finding integral points on elliptic curves. The method is a classic one due to Mordell. We will see that the problem of finding integral points on an elliptic curve can be reduced to the problem of finding integral solutions (x, y) to an equation of the following shape:

$$F(x, y) = m,$$

here $F(x, y)$ is a quartic binary form and m is an integer. Then I will show some results on representation of integers by quartic binary forms.

SPEAKER: Andrew Arnold, *Simon Fraser University*

TITLE: Computing Cyclotomic Polynomials of Large Height

ABSTRACT: TBA

SPEAKER: Imin Chen, *Simon Fraser University*

TITLE: On the equation $x^2 + y^6 = z^p$

ABSTRACT: The modular method has been successfully applied to tackle a number of classes of ternary diophantine equations of the form $Ax^a + By^b = Cz^c$. A recent development in the method has been the use of $\mathbb{Q}$-curves instead of elliptic curves over $\mathbb{Q}$. This was first introduced by Ellenberg to tackle the equations $x^2 + y^4 = z^p$ and has since been used to obtain results for several new families of generalized Fermat equations. We show how the modular method can be used to resolve the family of equations $x^2 + y^6 = z^p$. A new feature which arises for this equation is the use of the multi-Frey technique of Siksek in a situation which involves $\mathbb{Q}$-curves. The results require extensive use of MAGMA. (Joint work with Michael Bennett)

SPEAKER: Sander Dahmen, *University of British Columbia and Simon Fraser University*

TITLE: TBA

ABSTRACT: TBA

SPEAKER: Daniel Fiorilli, *Université de Montréal*

TITLE: Computations in prime number races using asymptotic formulae

ABSTRACT: The computational aspect of prime number races was put forward by the work of Rubinstein and Sarnak on "Chebyshev's bias." For the first time they were able to compute explicitly some densities, which

we will define during the talk. For instance, they were able to conclude that the inequality $\mathrm{Li}(x) > \pi(x)$ is true for 99.999973..% of the values of x on the logarithmic scale. However, computations of this kind are very tedious as they involve indefinite integrals of infinite products of Bessel functions. We will outline how we can use asymptotic formulae to get such explicit values with much less effort, but with the cost of an error term. We will also show how such explicit formulae can make great predictions about these values. (joint work with Greg Martin)

SPEAKER: Ron Ferguson, *IRMACS*

TITLE: TBA

ABSTRACT: TBA

SPEAKER: Richard Guy, *University of Calgary*

TITLE: $2 + 2$ is not equal to $2x2$

ABSTRACT: A few answers, and lots of questions, about adding and multiplying divisibility sequences.

SPEAKER: Matt Klassen, *DigiPen Institute of Technology*

TITLE: Non–associative loops on real loci of Fermat curves of odd degree

ABSTRACT: We investigate a class of nonassociative loops whose points are the real loci of the equations $x^n + y^n = 1$ for odd integers $n > 3$. The loop operation is analogous to the chord-tangent group law on the elliptic curve $x^3 + y^3 = 1$, with identity being the point at infinity $(1, -1, 0)$. We show that these loops have finite subgroups (associative subloops) of orders 2, 3, 4, 5 and 6. We illustrate the loop operation with a graphical program written in python and SAGE. We conclude with various open questions.

SPEAKER: Matilde Lalin, *University of Alberta*

TITLE: Higher Mahler measures

ABSTRACT: The classical Mahler measure of an n–variable polynomial P is the integral of $\log|P|$ over the n–dimensional unit torus T^n with the Haar measure. We consider, more generally, the integral of $\log^k|P|$. Specific examples yield special values of zeta functions, Dirichlet L–series, and polylogarithms. This is a joint work with N. Kurokawa and H. Ochiai.

SPEAKER: Nathan Ng, *University of Lethbridge*

TITLE: Effective Chebotarev and Computation

ABSTRACT: In this talk we will describe the role of computation in several results which are related to effective versions of Chebotarev's Density Theorem. Let L/K be a normal extension of number fields with Galois group G. The first theorem concerns an effective bound for the least prime ideal whose Frobenius equals a given conjugacy class C of G and the second concerns prime number races between two conjugacy classes C_1 and C_2 of G.

SPEAKER: Charles Samuels, *University of British Columbia*

TITLE: Reducing the ultrametric Mahler measure to a finite search

ABSTRACT: Recent work of Dubickas and Smyth examines a metric version of Mahler's measure, denoted M_1. It is natural to consider a non–Archimedean analog M_∞, which, in some ways, is much simpler. We show that M_∞ can be reduced to a search through a finite set. We provide an example where this result allows us to compute its value.