Computational and Diophantine Number Theory
Théorie des nombres computationnelle et diophantienne
(Org: **Michael Bennett** (University of British Columbia), **Keith Johnson** (Dalhousie University) and/et **Gary Walsh** (University of Ottawa / Université d'Ottawa))

MARK BAUER, University of Calgary

ADELA GHERGA, The University of British Columbia
Implementing Algorithms to Compute Elliptic Curves Over $\mathbb{Q}$

Let $S = \{p_1, \ldots, p_k\}$ be a set of rational primes and consider the set of all elliptic curves over $\mathbb{Q}$ having good reduction outside S and bounded conductor N. Currently, using modular forms, all such curves have been determined for $N \leq 390000$, the bulk of this work being attributed to Cremona.

Early attempts to tabulate all such curves often relied on reducing the problem to one of solving a number of certain integral binary forms called Thue-Mahler equations. These are Diophantine equations of the form

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

where

$$F(x, y) = f_0 x^n + f_1 x^{n-1} y + \cdots + f_{n-1} x y^{n-1} + f_n y^n$$

is a given binary form of degree at least 3 and u is an S-unit. A theorem of Bennett-Rechnitzer show that the problem of computing all elliptic curves over $\mathbb{Q}$ of conductor N reduces to solving a number of Thue-Mahler equations. To compute all such equations, there exists a practical method of Tzanakis-de Weger using bounds for linear forms in p-adic logarithms and various reduction techniques. In this talk, we describe our implementation of this method and discuss the key steps in used in our algorithm.

MIKE JACOBSON, University of Calgary
Statistical Analysis of Aliquot Sequences

Let $s(n) = \sigma(n) - n$ denote the proper sum of divisors function. 1n his 1976 M.Sc. thesis, Stan Devitt presented theoretical and numerical evidence, using a "new method of factoring called POLLARD-RHO", that the average order of $s(n)/n$ in successive iterations of $s(n)$ (Aliquot sequences) is greater than 1. These results seemingly lent support to the Guy/Selfridge Conjecture that there exist unbounded Aliquot sequences.

In this talk, we describe our on-going efforts to extend and update Devitt's computations, by considering the more-appropriate geometric mean of $s(n)/n$ as opposed to the arithmetic mean considered by Devitt, and by using modern factoring algorithms.

This is joint work with K. Chum, R. Guy, and A. Mosunov.

LIN JIU, Dalhousie University
Matrix Representations for Bernoulli and Euler Polynomials

Abstract. Probabilistic interpretations of Bernoulli and Euler polynomials recognize them as moments of certain random variables. Classical results on continued fractions identify moment and generalized Motzkin number, whose combinatorial interpretation is weighted lattice path. This allows us to derive the matrix representations for Bernoulli and Euler polynomials. This is joint work with Diane Shi.

CLAUDE LEVESQUE, U. Laval
Solving some cyclotomic binary forms

This is a joint work with Étienne Fouvry and Michel Waldschmidt. A cyclotomic binary form $\Phi_n(X,Y)$ is the homogenized version of the cyclotomic polynomial $\Phi_n(X)$ of degree $\phi(n)$. We look for the solutions of the Diophantine equation $\Phi_n(X,Y) = m$, where m is an integer > 0.

RENATE SCHEIDLER, University of Calgary
Dan Shanks' CUFFQI Algorithm Resurrected

In 1925, William E. H. Berwick designed an approach for enumerating all cubic fields $\mathbb{K}$ of a given fixed discriminant Δ via suitable integers, which he termed "quadratic generators", in the quadratic resolvent field $\mathbb{Q}(\sqrt{-3\Delta})$ of $\mathbb{K}$. When Δ is fundamental, he showed in particular that every cubic field $\mathbb{K}$ of discriminant Δ has a generating polynomial of the form $f_\lambda(x) = x^3 - 3(\lambda\overline{\lambda})^{1/3}x + (\lambda + \overline{\lambda}) \in \mathbb{Z}[x]$ where $(\lambda) = \mathfrak{a}^3$ and $\mathfrak{a}$ is an ideal in the maximal order of $\mathbb{Q}(\sqrt{-3\Delta})$.

Unfortunately, the Berwick construction can produce generating polynomials with very large coefficients. For example, if $\Delta < 0$ and λ is the fundamental unit of $\mathbb{Q}(\sqrt{-3\Delta})$, then $f_\lambda(x) = x^3 \pm 3x + T$ where $T \approx \exp(\sqrt{-3\Delta})$. In 1987, Daniel Shanks devised an ingenious algorithm for finding quadratic generators λ whose norm and trace in $\mathbb{Q}(\sqrt{-3\Delta})$ are both small, utilizing the infrastructure of $\mathbb{Q}(\sqrt{-3\Delta})$ when $\Delta < 0$. Shanks called his method "CUbic Fields From Quadratic Infrastructure, or CUFFQI (pronounced "cuff-key") for short. Although implemented in 1990 by Gilbert Fung as part of his PhD thesis, the CUFFQI algorithm was never published. In this talk, we present a modern version of this algorithm.

FRANCOIS SEGUIN, Queen's University
A lower bound for the two-variable Artin Conjecture

In 1927, Artin conjectured that any integer other than -1 or a perfect square generates the multiplicative group $\mathbb{Z}/p\mathbb{Z}^\times$ for infinitely many primes p. In a 2000 article, Moree and Stevenhagen considered a two-variable version of this problem, and proved a positive density result conditionally to the generalized Riemann Hypothesis by adapting a 1967 proof by Hooley for the original conjecture. During this talk, we present an unconditional lower bound for this two-variable problem obtained through the study of binary recurrence sequences. This is joint work with Ram Murty and Cameron Stewart.

SAMIR SIKSEK, University of Warwick
Which numbers are sums of seven cubes?

In 1851, Carl Jacobi made the experimental observation that all integers are sums of seven non-negative cubes, with precisely 17 exceptions, the largest of which is 454. Building on previous work by Maillet, Landau, Dickson, Linnik, Watson, Bombieri, Ramare, Elkies and many others, we complete the proof of Jacobi's observation.

ASMITA SODHI, Dalhousie University
Integer-Valued Polynomials over Matrix Rings

Bhargava's p-orderings and p-sequences have been helpful tools in the study of integer-valued polynomials over subsets of $\mathbb{Z}$ and arbitrary Dedekind domains, and similar useful definitions exist of ν-orderings and ν-sequences in the case of certain noncommutative rings. In a 2015 paper by Evrard and Johnson, these ν-sequences are used to construct a regular p-local basis for the rational integer-valued polynomials over the ring of 2×2 integer matrices $M_2(\mathbb{Z})$. In this talk we will show how the construction used there extends nicely to $M_n(\mathbb{Z})$ where n is prime, as well as discuss some interesting issues which arise in the case where n is composite.

COLIN WEIR, Tutte Institute
Diophantine equations counting supersingular hyperelliptic curves

One way to generalize the notion of a supersingular elliptic curve to curves with higher genus is to consider an invariant called the a-number. For example, curves with the a-number 0 have ordinary Jacobians, and those with a-number equal to their genus have Jacobians isomorphic to a product of supersingular elliptic curves. In this talk we will show how the number of hyperelliptic curves with a given a-number is related to the number of low height solutions to a family of Diophantine equations over $\mathbb{F}_q[x]$. In the case of characteristic 3, we are able to prove exact formulas for the number of such solutions and find, among other things, that precisely $1/q$ hyperelliptic curves are not ordinary (when counted in a certain way). This is joint work with Derek Garton and Jeff Thunder.

HUGH WILIAMS, University of Calgary

Some Remarks Concerning Voronoi's Continued Fraction Algorithm

Abstract. In 1896 G. Voronoi presented an algorithm for determining the fundamental unit(s) of the maximal order of a cubic number field. His procedure is an extension of the well-known simple continued fraction algorithm used to find the fundamental unit of a real quadratic field. This latter process requires that we only perform rational arithmetic and also provides simple bounds on the numbers it produces while executing. Unfortunately, Voronoi's process possesses neither of these computationally desirable features. In this talk we will discuss how Voronoi's algorithm can be modified to provide both of these properties in the case of a cubic field with negative discriminant. This is joint work with Sam Hambleton (Quensland) and Renate Scheidler (Calgary).

PAUL YOUNG, College of Charleston

2-adic properties of generalized Fibonacci sequences

Let T_n denote the generalized Fibonacci number of order k defined by the recurrence $T_n = T_{n-1} + T_{n-2} + \cdots + T_{n-k}$ for $n \geq k$, with initial conditions $T_0 = 0$ and $T_i = 1$ for $1 \leq i < k$. Motivated by some recent conjectures of Lengyel and Marques, we establish the 2-adic valuation of T_n, settling one conjecture affirmatively and one negatively. We discuss the computational issues that arise and applications to Diophantine equations involving (T_n) and $(T_n \pm 1)$.