Computational Number Theory
Théorie des nombres computationnelle
(Org: **Mark Bauer** (Calgary) and/et **Mike Bennett** (UBC))

PAUL BUCKINGHAM, University of Alberta
Implementing Zagier's inductive procedure for constructing higher K-groups of number fields

When numerically testing a certain p-adic Beilinson conjecture for number fields, one would like to be able to compare Borel regulators with p-adic regulators, as they are expected to give the same rational number on dividing by the appropriate L-value or p-adic L-value. We describe how one can implement Zagier's inductive procedure for computing higher algebraic K-groups in order to test this conjecture for K_5 and K_9, corresponding to L-function values at 3 and 5 respectively. This is joint work with Amnon Besser, Rob de Jeu and Xavier-Francois Roblot.

SANDER DAHMEN, Max-Planck-Institut für Mathematik
Elliptic curves of high rank

We discuss the construction of infinite families with many parameters of elliptic curves over number fields of high rank.

FELIX FONTEIN, University of Calgary / PIMS
Rigorous Computation of Fundamental Units in Number Fields

In this talk, we will discuss currently available rigorous methods for computation of fundamental units in an algebraic number field, as well as methods which verify that a given set of units is a set of fundamental units. By rigorous, we mean that the result of the computation is unconditionally correct, i.e. does not depend on any kind of unproven hypothesis. We will present results on the theoretical runtime complexity of such methods as well as their behaviour in practice.

EYAL GOREN, McGill University
The computational complexity of generating genus 2 curves suitable for cryptography

In his 2010 Leiden Thesis, M. Streng had determined the computational complexity of generating genus 2 curves suitable for cryptography. I will quickly recall a method of generating such curves and talk about one of the key elements in Streng's analysis, which is a recent theorem of K. Lauter (Microsoft Research) and myself.

MATT GREENBERG, University of Calgary
On the computation of algebraic modular forms

In the 1990s, Gross introduced the study of algebraic modular forms — automorphic forms on reductive groups G with the property that all arithmetic subgroups of $G(\mathbb{Q})$ are finite. In this talk I will discuss the computability of such forms for various groups G.

PATRICK INGRAM, University of Waterloo
Post-critically finite polynomials

In classical holomorphic dynamics, rational self-maps of the Riemann sphere whose critical points all have finite forward orbit under iteration are known as post-critically finite (PCF) maps. A deep result of Thurston shows that if one excludes examples arising from endomorphisms of elliptic curves, then PCF maps are in some sense sparse, living in a countable union of zero-dimensional subvarieties of the appropriate moduli space (a result offering dubious comfort to number theorists, who tend to work over countable fields). We show that if one restricts attention to polynomials, then the set of PCF points in moduli space is actually a set of algebraic points of bounded height. This allows us to give an elementary proof of the appropriate part of Thurston's result, but it also provides an effective means of listing all PCF polynomials of a given degree, with coefficients of bounded algebraic degree (up to the appropriate sense of equivalence).

MATILDE LALIN, Universite de Montreal
Higher Mahler measure and Lehmer's question

The k-higher Mahler measure of a nonzero polynomial P is the integral of $\log^k |P|$ on the unit circle. I will discuss Lehmer's question for $k > 1$ and show some interesting formulae for 2- and 3-higher Mahler measure of cyclotomic polynomials. This is joint work with Kaneenika Sinha.

MATTHEW MUSSON, University of Calgary
A Second Look at the GHS Attack on the Elliptic Curve Discrete Log Problem

We take a second look at the GHS Attack on the ECDLP. This time we relax the conditions of Hess' theorem in its analysis and find more curves appearing in the Weil Restriction. Relaxing the conditions of Hess' theorem benefits us especially in the case where curves are defined over $\mathbb{F}_{2^n}$ where $n = 2p, 3p$ or $4p$ for some prime p such that $2^n > 2^{160}$. In particular, we classify all curves appearing via the GHS attack over $\mathbb{F}_{q^2}$ and determine the full security impact on the fields $\mathbb{F}_{q^3}$ and $\mathbb{F}_{q^4}$. Our analysis suggests that the fields $\mathbb{F}_{q^4}$ are bad for elliptic curve cryptography - the first such fields - and should never be used in cryptographic protocols. We then turn our attention to fields of the form $\mathbb{F}_{q^5}$ and discuss the security impact of our findings, focusing on the curves found in the Oakley Key Determination Protocol. Lastly, we discuss ongoing research and open problems concerning this attack.

MATHEW ROGERS, University of Illinois
Computational proofs of Mahler measure identities

I will show how to use the WZ and PSLQ algorithms to prove identities involving Mahler measures. Some of these identities were previously proved with algebraic K-theory. I will also mention connections to elliptic dilogarithms, and the conjectures of Bloch and Grayson.

RENATE SCHEIDLER, University of Calgary
The ℓ-Rank Structure of a Global Function Field

For any prime ℓ, it is possible to construct global function fields whose Jacobians, when viewed as finite Abeian groups, have high ℓ-rank by moving to a sufficiently large constant field extension. Previously, Bauer, Jacobson, Lee and the speaker provided two main results in this context: an upper bound on the size of the field of definition of the ℓ-torsion $\mathcal{J}[\ell]$ of the Jacobian $\mathcal{J}$, and a lower bound on the increase in the base field size that guarantees a strict increase in ℓ-rank. In this talk, we provide improvements to both these results, and demonstrate that our techniques have the potential to yield the entire "ℓ-rank structure" of a function field. In other words, we can deduce the ℓ-rank over any intermediate field of the field of definition of $\mathcal{J}[\ell]$, including base fields that might be too large to be handled directly by computer algebra packages.

This is joint work with L. Berger, J.L. Hoelscher, Y. Lee, and J. Paulhus.

KATHERINE STANGE, Simon Fraser U / Pacific Institute for the Mathematical Sciences, U of British Columbia
Elliptic divisibility sequences and elliptic nets in computation

Evaluate the sequence of division polynomials at a fixed point on a fixed elliptic curve, and one obtains an elliptic divisibility sequence. These can be generalised to higher rank "elliptic nets" associated to an elliptic curve and an n-tuple of points. In fact, the collection of elliptic nets is in bijection with the collection of tuples $(E, P_1, \ldots, P_n)$ where E is an elliptic curve and the P_i are points on the curve. Taking elliptic nets as an alternate model of elliptic curves, we can see some of the usual quantities associated to a curve arising directly from the net. For example, we can compute Weil and Tate pairings, reduction modulo p (including information about bad reduction), the canonical height, etc. We will also see some problems for elliptic nets which are equivalent to the elliptic curve discrete logarithm problem (this portion is joint work with Kristin Lauter).

HUGH WILLIAMS, University of Calgary

A Problem Concerning Divisibility Sequences

The best known example of a linear divisibility sequence is the Lucas sequence, which is of considerable importance in computational number theory. One particular instance of this sequence is the well-known Fibonacci sequence. One way to generalize the Lucas sequence is to consider linear divisibility sequences which have a characteristic polynomial of even degree 2k, and distinct zeros with the property that k pairs of these zeros have the same integral product. The case where k is 1 is, of course, the Lucas sequence. In this talk I will discuss the case where k is 2. This deceptively simple sounding investigation results in some rather difficult problems.