Experimental Methods in Number Theory
Méthodes expérimentales en théorie des nombres
(Org: **Karl Dilcher** (Dalhousie), **Michael Jacobson** (Calgary) and/et **Renate Scheidler** (Calgary))

JEAN-FRANCOIS BIASSE, University of Calgary
Sieving methods for ideal class group and unit group computation

The purpose of this talk is to give an overview of the impact of sieving methods on the computation of the ideal class group and the unit group of a number field.

Class group and unit group computation are essential tasks in computational number theory. In particular, they occur in the resolution of Diophantine equations and in the test of many unproven number theoretic conjectures.

Class group and unit group computation for number fields of small degree can be speeded up greatly by the use of sieving algorithms. We will describe how sieving methods originally developped for factoring large numbers can be adapted for our purposes and report experiments showing that this provides a significant speed-up.

MICHAEL FILASETA, University of South Carolina
Problems connected to the factorization of $f(x)x^n + g(x)$

There are a variety of topics that have connections to the factorization of $f(x)x^n + g(x)$. These include a generalization of Sierpiński numbers to polynomials, a problem of Turán to show polynomials in $\mathbb{Z}[x]$ are always near irreducible polynomials, estimating the largest absolute value for a root of a given non-cyclotomic polynomial, the element with smallest norm in a principal ideal in $\mathbb{Z}[x]$, the Prouhet-Tarry-Escott problem, and a question involving a special sequence of Newman polynomials. We discuss these connections to the extent that time permits. This talk will focus on work of Schinzel as well as multiple joint research projects of the speaker with E. Dobrowolski, M. Mossinghoff, C. Nicol, M. Robinson and F. Wheeler, and with my former students P. Banerjee, C. Finch, I. Solan and A. Vincent, and with my current student J. Harrington.

DANIEL FIORILLI, University of Michigan
Dirichlet L-functions at the central point

In this talk I will describe recent results on the non-vanishing of Dirichlet L-functions at the central point, using probabilistic ideas. Chowla conjectured that Dirichlet L-functions never vanish at the central point; this is widely believed to be true. I will sketch how one can use conjectures coming from probabilistic arguments to tackle this problem.

KEVIN HARE, University of Waterloo
Representation of integers base d with digits $0, 1, \cdots, q-1$

Let d and q be positive integers, and consider representing a positive integer n with base d and digits $0, 1, \cdots, q-1$. Clearly if $q < d$, then not all positive integers can be represented. If $q = d$, every positive integer can be represented in exactly one way. If $q > d$, then there may be mutliple ways of representing the integer n. For example, if $d = 2$ and $q = 3$ we might represent 6 as $110 = 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$ as well as $102 = 1 \cdot 2^2 + 0 \cdot 2^1 + 2 \cdot 2^0$. (This list is not complete.) Let $f_{d,q}(n)$ be the number of representations of n with base d and digits $0, 1, \cdots, q-1$. In this talk we will look at the asymptotics of $f_{d,q}(n)$ as $n \to \infty$. This depends in a rather strange way on the Generalized Thue-Morse sequence. Many of the results are computationally/experimentally true, although no proofs are known.

JOSHUA HOLDEN, Rose-Hulman Institute of Technology
Counting solutions to exponential congruences using p-adic methods

Congruences involving exponential functions are common in modern cryptography and have also come up in questions of pure number theory and in electrical engineering. These functions include the well-known discrete exponentiation map, the self-power map, the discrete Lambert map, and exponential Welch permutations. The number of solutions to such congruences depends, of course, on the range of inputs involved. In some cases we have been able to count the number of solutions exactly, and if the modulus is a prime power, we have found that p-adic methods are very helpful in this. In other cases, the number of solutions can only be estimated. In these cases, experimental observations and heuristics inspired by theory are among the main tools. Some of this is joint work with Margaret Robinson.

JOHN JONES, Arizona State University
The tame-wild principle

We consider relationships between discriminants of number fields contained in a given Galois extension. When the "tame-wild principle" holds, then one only needs to check what happens under the assumption of tame ramification, which is much simpler to deal with than wild ramification. We will describe the theory with applications to the construction of complete tables of number fields.

DAVID KRUMM, University of Georgia
Quadratic points on dynamical modular curves

This talk will be an overview of an ongoing project in arithmetic dynamics being developed jointly with John Doyle and Xander Faber. A recent algorithm for computing elements of bounded height in number fields was applied to the problem of finding preperiodic points for quadratic polynomials over number fields. Following extensive computations of preperiodic structures over quadratic fields we asked various questions suggested by the data. By using new techniques for studying quadratic points on algebraic curves we are now answering these questions and proving earlier conjectures.

MICHAEL MOSSINGHOFF, Davidson College
Barker sequences, Wieferich pairs, and Compute Canada

A *Barker sequence* is a finite sequence of integers, each ± 1, whose off-peak aperiodic autocorrelations are all at most 1 in absolute value. Very few Barker sequences are known, and it has long been conjectured that no additional ones exist. Many arithmetic restrictions have been established that severely limit the allowable lengths of Barker sequences, so severely that no permissible lengths were even known. Using computational resources of Compute Canada, we identify the smallest plausible value for the length of a new Barker sequence, and we compute a number of permissible lengths up to a sizable bound. This work involves a substantial search for Wieferich prime pairs (q, p), which are defined by the property that $q^{p-1} \equiv 1 \bmod p^2$. This is joint work with Peter Borwein.

TATIANA HESSAMI PILEHROOD, Dalhousie University
Modulo p structures of multiple harmonic sums.

We will discuss arithmetic properties and possible relations for finite multiple harmonic sums (MHS) modulo a prime which are defined as partial sums of multiple zeta values. The theory of MHS modulo a prime bears many similarities with the theory of multiple zeta values. It turns out that the MHS modulo a prime often can be expressed in terms of Bernoulli numbers. We will describe sets of generators for the MHS of small weights and give a refinement of results due to Hoffman and Zhao for the MHS in weight 7 and 9 modulo a prime. This is joint work with Khodabakhsh Hessami Pilehrood and Roberto Tauraso.

MICHAEL RUBINSTEIN, University of Waterloo
Elliptic curves with positive rank and the Riemann zeta function

I will describe some experiments and computations that indicate that in order for an elliptic curve to acquire large rank r and have relatively small conductor, its L-function, normalized so that the critical line is $\mathrm{Re}(s) = 1$, should behave like $1/\zeta(s)^r$. I will also describe other features of L-functions where the zeta function on the one line plays a prominent role.

ANDREW SHALLUE, Illinois Wesleyan University
Constructing a 10 billion factor Carmichael number

A Carmichael number is a pseudoprime n that passes the base a Fermat primality test for all a coprime to n. With programming help from Steven Hayman, I have constructed a Carmichael number with 10 billion prime factors and almost 300 billion decimal digits. This was made possible by a new algorithm for dense instances of the subset-product problem, an algorithm inspired by the Kuperberg Sieve from the theory of quantum algorithms.

JONATHAN SORENSON, Butler University
Approximately Counting Semismooth Integers

An integer n is (y, z)-semismooth if $n = pm$ where m is an integer with all prime divisors $\leq y$ and p is 1 or a prime $\leq z$. Large quantities of semismooth integers are utilized in modern integer factoring algorithms, such as the number field sieve, that incorporate the so-called *large prime* variant. Thus, it is useful for factoring practitioners to be able to estimate the value of $\Psi(x, y, z)$, the number of (y, z)-semismooth integers up to x, so that they can better set algorithm parameters and minimize running times, which could be weeks or months on a cluster supercomputer. In this talk, we explore several algorithms to approximate $\Psi(x, y, z)$ using a generalization of Buchstab's identity with numeric integration.

EDLYN TESKE, University of Waterloo
Solving the ECDLP using Semaev Polynomials, Weil Descent, and Groebner basis methods – an experimental study

At EUROCRYPT 2012, Petit and Quisquater suggested that there may be a subexponential time algorithm for the Elliptic Curve Discrete Logarithm Problem (ECDLP) in characteristic two fields. This algorithm uses Semaev polynomials and Weil Descent to create a system of polynomial equations that subsequently is to be solved. Its analysis is based on unproven heuristic assumptions on the performance of Groebner basis methods in this particular setting. While the subexponential behaviour would manifest itself only far beyond the cryptographically interesting range, this result, if correct, would still be extremely remarkable. We examined some aspects of the Petit-Quisquater assumptions experimentally. This is joint work with Michael Shantz.

HUGH WILLIAMS, University of Calgary
Linear Divisibility Sequences of Order Six

A sequence of rational integers is said to be a divisibility sequence if the mth term always divides the nth term whenever m divides n. If the divisibility sequence also satisfies a linear recurrence relation, it is said to be a linear divisibility sequence of order k, where k is the degree of its characteristic polynomial. The best-known example of a linear divisibility sequence of order 2 is the Lucas sequence, one particular instance of which is the famous Fibonacci sequence. Indeed, it was through experimenting with the Fibonacci numbers that Lucas discovered the properties of the more general Lucas sequence. It was these properties that he utilized in developing his various primality tests. While much has been learned recently about linear divisibility sequences of order 4 (see Williams and Guy 2011, 2012), there is very little known about linear divisibility sequences of order 6. In the Online Encyclopedia of Integer Sequences, there are only 5 such sequences listed. In this paper we mention these sequences and produce some results concerning their generalizations.