Computational Number Theory
Théorie algorithmique des nombres

(Org: **Kevin Hare** (Waterloo) and/et **Patrick Ingram** (Colorado State University))

JEAN-FRANÇOIS BIASSE, University of South Florida
Quantum algorithms for number theory and their relevance to cryptography

I will report on recent results about quantum algorithms for solving computational problems in number theory.

In a recent work in collaboration with Fang Song, I presented the first quantum polynomial time algorithm for computing the S-unit group of a number field for a given set of prime ideals S. This algorithm works for arbitrary classes of number fields, even with large degree. It implies polynomial time algorithms for computing the ideal class group, solving the so-called "Principal Ideal Problem" (PIP), computing ray class groups and solving some norm equations. I will discuss the relevance of the efficient PIP resolution method for cryptography.

In collaboration with David Jao and Anirudh Sankar, I also described a quantum algorithm which finds an isogeny between two given supersingular curves over a finite field. In some cases, this algorithm runs in subexponential time. This can be used to attack quantum-safe cryptographic schemes relying on the hardness of finding an isogeny between two given supersingular curves.

DANIELLE COX, Mount Saint Vincent University
A Problem on Generating Sets Containing Fibonacci Numbers

The following problem was posed at the Sixteenth International Conference on Fibonacci Numbers and Their Applications:

Let S be the set generated by these rules: Let $1 \in S$ and if $x \in S$, then $2x \in S$ and $1 - x \in S$; so that S grows in generations:

$$\text{gen}(1) = \{1\}, \text{gen}(2) = \{0, 2\}, \text{gen}(3) = \{-1, 4\} \ldots$$

Prove or disprove that each generation contains at least one Fibonacci number or its negative.

In this talk we will discuss the solution using techniques involving the dragon curve, binary sequences and trees.

This is joint work with Karyn McLellan (Mt. St. Vincent University)

CLIFTON CUNNINGHAM, University of Calgary
Lifts of Hilbert modular forms and applications to a conjecture of Gross

This talk concerns two approaches to automorphic representations of general spin groups. First, we review a conjecture of Gross which, given an abelian variety over $\mathbb{Q}$ with trivial endomorphism algebra, predicts the weight and level of an automorphic representation of $\mathrm{GSpin}_{2n+1}(\mathbb{A}_\mathbb{Q})$ with matching L-function. Second, we review a lifting procedure which produces automorphic representations of $\mathrm{GSpin}_{2n+1}(\mathbb{A}_\mathbb{Q})$ from certain Hilbert modular forms over degree n extensions of $\mathbb{Q}$. We then present examples, identified through computational experimentation, of Hilbert modular forms which produce automorphic representations of $\mathrm{GSpin}_{2n+1}(\mathbb{A}_\mathbb{Q})$ coming from certain abelian varieties, as predicted by Gross. Joint with Lassina Dembélé.

EVA CURRY, Acadia University
Computational Complexity of Addition with Multidimensional Digit Representations

Vectors with integer entries, like integers, can be represented with a digit representation with a base (radix) matrix and a finite set of digit vectors. Standard algorithms for multi-digit addition can then be extended to new addition algorithms for vectors, beyond the standard component-wise addition. Digit representations for integers, including the base-10 Hindu-Arabic numeration system and binary representations, were major advances in mathematics, enabling efficient computations, with numerous important consequences. We ask whether digit representations for vectors can yield further advances in computational efficiency.

Some surprising results occur in the multidimensional setting: addition may be of quadratic rather than linear complexity ($O(n^2)$ instead of $O(n)$, where n is the length of input), and for some addition tables, the standard multidigit addition algorithm may not terminate. Workarounds exist in some cases, making use of an idea similar to the two's complement algorithm for subtraction in one dimension. This talk will briefly review the construction of multidimensional radix representations, will summarize the work recently completed in the Master's thesis of M. ALmutairi, and will present some variations of the addition algorithm that may simplify multidigit addition in the multidimensional setting.

AURORE GUILLEVIC, University of Calgary and PIMS-CNRS
Computing discrete logarithms in non-prime finite fields

Computing discrete logarithms in finite fields is a main concern in cryptography. The best algorithms known are the Number Field Sieve and its variants in medium- and large-characteristic fields (e.g. $GF(p^2)$, $GF(p^{12})$); the Function Field Sieve and the Quasi Polynomial-time Algorithm in small characteristic finite fields (e.g. $GF(2^{4404})$). The last step a.k.a. the initial splitting step of the NFS and FFS algorithms computes a smooth decomposition of a given target. While new improvements have been made to reduce the complexity of the dominating relation collection and linear algebra steps of NFS and FFS, resulting in a smaller database of known logarithms of small elements, the target is still any large element of the finite field, so that finding a smooth enough decomposition over the database becomes harder.

Our present method applies to any finite field of composite extension degree. It exploits the available subfields with a cheap (polynomial-time) linear algebra step, resulting in a much more smooth decomposition of the target. This leads to a new trade-off in the asymptotic complexity of the initial splitting step: it is improved by a factor 2 in the exponent with FFS and $2^{1/3}$ in the exponent with NFS, for any finite field of even extension degree, and with a much smaller smoothness bound. In medium and large characteristic, it can be combined with Pomerance's Early Abort strategy. In small characteristic, it replaces the Waterloo algorithm of Blake, Fuji-Hara, Mullin and Vanstone. Moreover it reduces the width and the height of the following decreasing tree.

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 expand 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 greatly extending Devitt's computations using modern factoring algorithms.

This is joint work with K. Chum and R. Guy.

ANTON MOSUNOV, University of Waterloo
Some computational evidence on the heuristics of Guy and Selfridge

Let $s(n)$ denote the sum of the proper divisors of a positive integer n. An aliquot sequence is a sequence of the form $n, s(n), s_2(n) = s(s(n)), s_3(n) = s(s(s(n)))$, and so on. In 2003, Bosma and Kane proved that the geometric mean of $s(2n)/(2n)$ exists and is slightly less than one. Recently, Carl Pomerance demonstrated that the geometric means of $s(s(2n))/s(2n)$ and $s(2n)/(2n)$ for $n > 1$ match. Both of these results give a strong probabilistic evidence that most of the aliquot sequences starting with an even number are bounded. In our work, we show that the geometric means of $s_k(2n)/s_{k-1}(2n)$ for $2n \leq X$ exceed one for $X = 2^{37}$ and $k = 6, 7, 8, 9, 10$ when averaged over all n such that $s_k(2n) > 0$. Moreover, as k increases, the geometric means grow, too. However, as k remains fixed, the geometric means decrease with the growth of X, possibly approaching the geometric mean of $s(2n)/(2n)$. This can be counted as a computational evidence both for and against the heuristics of Guy and Selfridge given in 1976 that most of the aliquot sequences starting with an even number should be unbounded.

MONIREH REZAI RAD, University of Calgary
Jacobian Versus Infrastructure in Real Hyperelliptic Curves

Real hyperelliptic curves admit two structures: the Jacobian and the infrastructure. While both structures in real models could be employed for cryptographic purposes, it was not clear which one has better performance in practice.

In this talk, we describe that how exactly the infrastructure and the Jacobian are related. We suggest an alternative distance map for the infrastructure in order to improve the efficiency of this structure. We show that the infrastructure with the new distance and the Jacobian have identical performance in practice for cryptographic sized curves. We support this claim both mathematically and computationally.

CHARLES SAMUELS, Christopher Newport University
Using Fibonacci numbers to solve certain extremal problems regarding the Mahler measure

A 2001 article of Dubickas and Smyth studies a modified version of the Mahler measure which they called the *metric Mahler measure*. Roughly speaking, the metric Mahler measure exposes a family of extremal problems many of which appear to be quite difficult. We discuss a certain collection of special cases which can be reduced to the study of the Fibonacci sequence. In these cases, we shall examine a strategy for computing the values of the metric Mahler measures. Our study also reveals an apparently difficult open problem on the Fibonacci numbers.

RENATE SCHEIDLER, University of Calgary
Computing Quadratic Function Fields With High 3-Rank Via Cubic Field Tabulation

We present extensive numerical data on global quadratic function fields whose class group has positive 3-rank, obtained via an adaptation to function fields of a method due to Belabas for finding quadratic number fields of high 3-rank. Our algorithm generates fields of minimal discriminant degree for any given 3-rank. It relies on previous work by he authors for tabulating cubic function fields, but incorporates a significant computational speed-up when the quadratic extension is ramified at infinity. We provide numerical data for discriminant degree up to 11 over the finite fields of respective orders 5, 7, 11 and 13. We compare our data with a variety of heuristics on the density of such fields of a given 3-rank by Friedmann-Washington, Ellenberg et al, Achter, and Garton. In most cases, our our data supports the validity of these heuristics. This is joint work with Mike Jacobson and Pieter Rozenhardt.

KATHERINE STANGE, University of Colorado Boulder
Lattice properties of number fields and lattice-based cryptography

I will discuss open questions about number field lattices arising from the Ring Learning with Errors problem in lattice-based cryptography. This hard lattice problem is a promising candidate for post-quantum cryptography. This is joint work with Hao Chen and Kristin Lauter.