Number Theory
Théorie des nombres
(Org: **Mark Bauer** (Calgary), **Richard McIntosh** (Regina) and/et **Eric Roettger** (Mount Royal))

MICHAEL BENNETT, University of British Columbia
A problem of Erdos and Graham revisited

We construct, given an integer $r \geq 5$, an infinite family of r non-overlapping blocks of five consecutive integers with the property that their product is always a perfect square. In this particular situation, this answers a question of Erdős and Graham in the negative. We survey more general results in the literature and sketch what we hope are promising directions. This is joint work with Ronald van Luijk.

DAN BROWN, Certicom (subsidiary of Research in Motion)
Cryptography in Diophantine Cloak

Some important cryptographic problems can be easily expressed as Diophantine problems: quite simply for public-key cryptography, or using the notion of straight line program for symmetric-key cryptography. This talk will review some theorems about solving the factoring and Rivest–Shamir–Adleman (RSA) problems using a straight line program. This talk will also relate the security U.S. Federal Information Processing Standard (FIPS) 186-3 Digital Signature Algorithm (DSA) to the well-known discrete logarithm problem, and a not-so-well-known problem Diophantine problem: the one-up problem.

PAUL BUCKINGHAM, University of Alberta/PIMS
Connecting homomorphisms associated to Tate sequences

The Tate sequence is the result of a unification of local and global class field theory, and describes the cohomology of the S-units in a Galois extension of number fields. In the traditional construction, S was assumed to be large enough that the S-class-group was trivial. A refinement of Ritter and Weiss removed that assumption, so that their Tate sequence involved both the S-units and the S-class-group, giving rise to connecting homomorphisms not previously studied. We will provide the first descriptions of some of these connecting homomorphisms, and discuss some consequences.

MICHAEL COONS, University of Waterloo and Fields Institute
The rational-transcendental dichotomy of Mahler functions

In the late 1920s and early 1930s, Mahler wrote a series of articles concerning the algebraic character of values of power series which satisfy a certain type of functional equation; these functional equations (and functions) are now called Mahler-type functional equations (and Mahler functions). He was able to show that if a Mahler function $f(z)$ is transcendental then the number $f(a)$ is transcendental for all but finitely many nonzero algebraic numbers a in the radius of convergence of $f(z)$. Of course this result relies on the transcendence of a series, which may itself be difficult to ascertain. Some decades after Mahler's original investigations, Nishioka showed that a Mahler function was either transcendental or rational. Thus to show transcendence it is enough to show irrationality. In this talk, we will give a new (and much simpler) proof of Nishioka's theorem and discuss some refinements and generalizations.

KARL DILCHER, Dalhousie University
Congruences for sums of reciprocals

The sums of reciprocals modulo p over integers in N subintervals of equal length of the interval $1 \leq j \leq p-1$ are closely related to the Fermat quotients, and they have been studied in connection with the classical theory of Fermat's last theorem.

In this talk we present new classes of linear relations between these sums for both even and odd N, and it is shown that for each even N there are at least $\lfloor N/4 \rfloor$ linearly independent relations. (Joint work with Ladislav Skula).

MATTHEW GREENBERG, Calgary

PATRICK INGRAM, Colorado State University
The arithmetic of Henon maps

We will survey various recent results in the arithmetic dynamics of Henon maps.

MICHAEL JACOBSON, University of Calgary
Tabulating Class Groups of Real Quadratic Fields

Class groups of real quadratic fields have been studied since the time of Gauss, and in modern times have been used in applications such as integer factorization and public-key cryptography. Tables of class groups are used to provide valuable numerical evidence in support of a number of unproven heuristics and conjectures, including those due to Cohen and Lenstra. In this talk, we discuss recent progress in our efforts to extend existing, unconditionally correct tables of real quadratic fields. This includes incorporating ideas of Sutherland for computing orders of elements in a group, as well as constructing a unconditional verification algorithm using the trace formula of Maass forms based on ideas of Booker.

This is joint work with C. Bian, A. Booker, A. Shallue, and A. Strömbergsson.

DAVID JAO, University of Waterloo
Isogeny-based Cryptography

Cryptosystems based on isogenies between elliptic curves have recently been proposed as plausible alternatives to traditional public-key cryptosystems. These systems are of particular interest because they are conjectured to be resistant to attacks by quantum computers. We survey the existing constructions of isogeny-based public-key cryptosystems and describe the fastest known attacks against them. In the case of ordinary curves, we present an algorithm for evaluating isogenies, whose running time is provably subexponential under GRH. For supersingular curves, we propose a public-key cryptosystem based on pairs of isogenies over a curve with disjoint kernels, having performance competitive with standard cryptosystems, and describe our recent performance optimizations.

Joint work with A. Childs, L. De Feo, J. Plût, and V. Soukharev.

KEITH JOHNSON, Dalhousie University
Integer valued polynomials on noncommutative rings

Rings of polynomials taking integral values on specified sets have been of interest to algebraists and number theorists at least since the work of Polya and Ostrowski in 1919. In the past this has usually been restricted to subsets of commutative rings, particularly rings of algebraic integers. We will discuss some examples involving noncommutative rings and in particular will give a description of the ring of rational polynomials taking integal values on nxn lower triangular matrices.

RICHARD MCINTOSH, University of Regina
p-adic equations for power sums

For odd primes p and positive integers k, define $S_k = \sum_{r=1}^{p-1} r^{-k}$. Applying the p-adic logarithm to the identity $\prod_{r=1}^{p-1}(1-\frac{p}{r}) = 1$, we obtain $\sum_{k=1}^{\infty} p^k \frac{S_k}{k} = 0$, where the convergence is p-adic. (This means that the equation holds modulo p^m for arbitrarily large

m.) In this talk I will give some other p-adic equations for the power sums S_k. For example, $\sum_{k=1}^{\infty} p^k(-1)^{k-1}B_{k-1}S_k = 0$, where B_n is the nth Bernoulli number.

RENATE SCHEIDLER, University of Calgary
Cubic Function Field Tabulation and 3-Ranks of Hyperelliptic Curves

We present an algorithm for tabulating all cubic function fields of square-free discriminant $D(x) \in \mathbb{F}_q(x)$ up to a given discriminant degree bound B so that the hyperelliptic curve $y^2 = -3D(x)$ has only one infinite place. Our method is an extension of Belabas' technique for tabulating cubic number fields and requires $O(B^4q^B)$ operations in $\mathbb{F}_q$ as $B \to \infty$. The main ingredient is a function field analogue of the Davenport-Heilbronn correspondence between triples of $\mathbb{F}_q(x)$-conjugate cubic function fields and certain equivalence classes of binary cubic forms over $\mathbb{F}_q(x)$, described via reduced representatives.

Our method additionally finds for any $r \in \mathbb{Z}^{\geq 0}$ all hyperelliptic curves $y^2 = -3D(x)$ whose class group has 3-rank r. For $q \equiv -1 \pmod 3$, our numerical data largely supports the predicted heuristics of Friedman-Washington and partial results on the distribution of the counts of such curves due to Ellenberg-Venkatesh-Westerland. For $q \equiv 1 \pmod 3$, our data seems to agree with a result due to Achter as well as recent conjectures due to Garton that incorporate into the Friedmann-Washington heuristics a correction factor first proposed by Malle for the number field scenario.

CAMERON STEWART, University of Waterloo
Well spaced integers generated by an infinite set of primes

In this talk we discuss an old question of Wintner and its resolution by Tijdeman as well as recent developments due to the speaker and Jeongsoo Kim.We shall prove that there is an infinite set of prime numbers with the property that the sequence of positive integers made up from the set is well spaced. This is joint work with Jeongsoo Kim.

COLIN WEIR, University of Calgary
Decomposing the Jacobians of Hermitian Curves

Hermitian curves are examples of maximal curves - they contain as many points as possible when considered over $\mathbb{F}_{q^2}$. As such, they are well studied objects. For example, it is known that the Jacobian of a Hermitian curve is isogenous to a product of super-singular elliptic curves. However, it is not known in general how their Jacobians decompose up to isomorphism (instead of isogeny). We explore this problem by instead considering the decomposition of the p-torsion group scheme of their Jacobians. This approach allows us to translate this problem into one that is purely combinatoric. This gives rise to an explicit decomposition with several interesting consequences. This is joint work with Rachel Pries.

HUGH WILLIAMS, University of Calgary
Compact Representations of Certain Algebraic Integers

Suppose we have a real quadratic number field of discriminant d. If we have a principal ideal I, it usually requires an exponential (in log d) amount of time to write out a generator of I in the conventional way. However, there exists a representation of this generator, called a compact representation, which can be written out in polynomial time. In this talk I discuss algorithms for finding compact representations of such a generator, when we are given an approximate value of the logarithm of the absolute value of it and an integral basis of I. I go on to point out several improvements that have been to algorithms used in the past.