Analytic Number Theory and Diophantine Approximation
Théorie analytique des nombres et approximation diophantienne
(Org: **Cameron Stewart** (Waterloo))

SHABNAM AKHTARI, CRM, Montreal
Cubic Binary Forms That Do Not Represent 1.

Let F(x , y) be an irreducible binary cubic form. It is known that the equation F(x , y) = 1 has at most finitely many solutions in integers x and y. I am going to show that for a positive proportion of binary forms F(x , y), the equation F(x , y) = 1 has no solutions in integers x and y. This is a joint work with M. Bhargava.

JASON BELL, Simon Fraser University
Towards an Effective Mordell-Lang Theorem in positive characteristic

The general Mordell-Lang problem is to describe the intersection of a Zariski closed subset with a finitely generated abelian subgroup of a variety endowed with a natural group structure. Many interesting Diophantine problems can be described using this framework. We consider the problem of describing the intersection of a Zariski closed subset X of $\mathrm{GL}_d(K)$ with a finitely generated abelian subgroup Γ of $\mathrm{GL}_d(K)$ when K is a field of positive characteristic. We show that the set $X \cap \Gamma$ can be naturally described using the language of finite-state automata and, moreover, this description allows us to prove that the intersection can be effectively determined in this case. We discuss connections to S-unit equations and other Diophantine problems in positive characteristic. This is joint work with Boris Adamczewski

---

MICHAEL BENNETT, University of British Columbia
Twisted extensions of the cubic case of Fermat's Last Theorem

We classify primes p for which there exist elliptic curves $E/\mathbb{Q}$ with conductor $N_E \in \{18p, 36p, 72p\}$ and nontrivial rational 2-torsion, and, in consequence, show that, for "almost all" primes p, the Diophantine equation

$$x^3 + y^3 = p^\alpha z^n$$

has at most finitely many solutions in coprime nonzero integers x, y and z and positive integers α and $n \geq 4$. To prove this result, we appeal to such disparate techniques as lower bounds for linear forms in p-adic logarithms, Schmidt's Subspace Theorem, and methods based upon Frey curves and modularity of associated Galois representations.

This is joint work with Florian Luca and Jamie Mulholland.

TIMOTHY CALEY, University of Waterloo
The Prouhet-Tarry-Escott Problem and Applications

The Prouhet-Tarry-Escott (PTE) problem is a classical number theoretic problem which asks for integer solutions to sums of equal powers. Solutions to the PTE problem give improved bounds for the "Easier" Waring problem, but they are difficult to find using conventional methods. We will describe how solutions can be found computationally and by connecting the problem to finding rational points on elliptic curves. We will also discuss some other applications of the problem. There will also be a statement of open questions relating to the PTE problem.

MICHAEL COONS, University of Waterloo and Fields Institute
An irrationality measure for Mahler numbers

Let $F(x) \in \mathbb{Z}[[x]]$ be a power series that satisfies a Mahler-type functional equation; that is, there exist positive integers k and d and polynomials $p(x), a_0(x), \ldots, a_d(x) \in \mathbb{Z}[x]$ with $a_0(x)a_d(x) \neq 0$ such that

$$p(x) + \sum_{i=0}^{d} a_i(x)F(x^{k^i}) = 0.$$

Let ξ be a real number. The *irrationality exponent* $\mu(\xi)$ of ξ is defined as the supremum of the set of real numbers μ such that the inequality $|\xi - p/q| < q^{-\mu}$ has infinitely many solutions $(p, q) \in \mathbb{Z} \times \mathbb{N}$.

In this talk we will outline a proof that $\mu(F(a/b)) < \infty$ for all positive integers $b \geq 2$ such that a/b is in the radius of convergence of $F(x)$ and $\log|a|/\log b \in [0, 1/2)$; in particular, we show that $F(1/b)$ is not a Liouville number. This generalizes a result of Adamczewski and Cassaigne for automatic numbers.

This is joint work with Jason Bell.

KARL DILCHER, Dalhousie University

The Gauss-Wilson Theorem for Partial Products

For positive integers $M \geq 2$ and $n \equiv 1 \pmod{M}$ we define the *Gauss factorial* $(\frac{n-1}{M})_n!$ to be the product of all integers up to $\frac{n-1}{M}$ and relatively prime to n, a terminology suggested by Gauss's generalization of Wilson's theorem. While the multiplicative orders (mod n) of Gauss factorials are completely determined when $M = 2$, the general case presents numerous interesting challenges. After some general results, this talk will concentrate on the special cases $M = 3$ and $M = 4$. The binomial coefficient theorems of Gauss and Jacobi are important tools, as are certain Pell equations and their solutions. Some large-scale computations are also involved. (Joint work with John B. Cosgrave.)

JOHN FRIEDLANDER, University of Toronto

The Spin of Prime Ideals

For a given number field K and a fixed automorphism, we attach to ideals of K a symbol, the "spin", which describes the quadratic nature of the ideal relative to its Galois conjugate. We show the equidistribution of the spin when summed over prime ideals. The result is applied to the arithmetic statistics of Selmer groups of elliptic curves. This highlights work joint with H. Iwaniec, B. Mazur and K. Rubin.

ANDREW GRANVILLE, U de Montreal

Sieving with large primes

Can one sieve with primes bigger than $x^{1/2}$? Certainly no current sieve methods work in this range, and there are good reasons to believe that it should be difficult to go past this "barrier". However Dimitris Koukoulopoulos, Kaisa Matomaki and I have recently succeeded in a certain special case, which leads to some guesses as to the right questions to ask in the general situation. Part of our proof emerges from additive combinatorics, a tool that has not traditionally been used in sieve theory.

PATRICK INGRAM, Colorado State University

Heights and post-critically finite rational maps

In complex holomorphic dynamics, the orbits of critical points reveal much about the behaviour of a map under iteration. Rational functions of a single variable for which all of these critical orbits are finite, then, have a special status. It turns out that all such functions either come from endomorphisms of elliptic curves, or correspond to algebraic points on certain varieties defined over $\mathbb{Q}$. In this talk we will present the result of joint work with Jones and Levy, specifically a p-adic analogue of an old result of Fatou, which bounds the heights of these points.

MATILDE LALIN, Université de Montréal
Statistics on zeros of Artin-Schreier curves

We investigate statistics for the distribution of zeros of the L-function for the family of Artin-Schreier curves over finite fields. This is joint work with A. Bucur, C. David, B. Feigon, and K. Sinha.

KUMAR MURTY, University of Toronto
Transcendental Values of Class Group L-functions

We report on joint work with Ram Murty on the transcendence of the values $L(1,\chi)$ as χ ranges over non-trivial even characters of various ray class groups of an imaginary quadratic field.

NATHAN NG, University of Lethbridge
Simple zeros of modular L-functions

An old problem in analytic number theory is to show that an L-function possesses simple zeros. Thanks to work of Levinson and Bauer, it is known that any degree one L-function has infinitely many simple zeros. For degree two L-functions there are fewer results known. In this talk I will present some recent work which establishes the existence of infinitely many simple zeros for the L-functions attached to certain modular forms. This is joint work with M.B. Milinovich.

DAMIEN ROY, University of Ottawa
On rational approximation to real points on conics

Let $q(x_0, x_1, x_2)$ be a homogeneous polynomial of degree 2 in 3 variables, with rational coefficients. Assume that q admits a non-trivial real zero and that q is irreducible over the field $\mathbb{Q}$ of rational numbers. Denote by U the set of real zeros of q having $\mathbb{Q}$-linearly independent coordinates. We show that

a) each point in U has an exponent of uniform rational approximation between $1/2$ and $1/\gamma \cong 0.618$, where γ denotes the golden ratio,

b) the elements of U for which the upper bound is achieved form an infinite countable set.

For $q(x_0, x_1, x_2) = x_0x_2 - x_1^2$, the statement a) is due to Davenport and Schmidt (1967) while b) is due to the author (2003). When q is irreducible over $\mathbb{R}$ and admits a non-trivial rational zero, we are quickly reduced to that case. Otherwise, the proof of a) is simpler, but the existence of "extremal" points in b) requires additional tools.

MICHAEL RUBINSTEIN, University of Waterloo
Experiments with the explicit formula

The explicit formula relates the zeros of an L-function with its logarithmic derivative. I'll describe some experiments that I have carried out with the explicit formula.

KATHERINE STANGE, Stanford University
Integral points on elliptic curves and explicit valuations of division polynomials

Assuming Lang's conjectured lower bound on the heights of non-torsion points on an elliptic curve, we show that there exists an absolute constant C such that for any elliptic curve $E/\mathbb{Q}$ and non-torsion point P in $E(\mathbb{Q})$, there is at most one integral multiple $[n]P$ such that $n > C$. The proof is a modification of a proof of Ingram giving an unconditional but not uniform bound. The new ingredient is a collection of explicit formulae for the sequence of valuations of the division polynomials. For P of non-singular reduction, such sequences are already well described in most cases, but for P of singular reduction, we are led to define a new class of sequences called elliptic troublemaker sequences, which measure the failure of the Néron local height

to be quadratic. As a corollary in the spirit of a conjecture of Lang and Hall, we obtain a uniform upper bound on the height of integral points having two large integral multiples, in terms of the height of the curve.

CHESTER WEATHERBY, Queen's University
Special Values of the Gamma Function

We will discuss the Gamma function at arguments from an imaginary quadratic field. During the talk we will see a connection to infinite products and in some cases we are able to say something about their transcendental nature.

HUGH WILLIAMS, University of Calgary
Some Extensions of the Lucas Functions

From 1876 to 1878 Lucas developed his theory of the functions Vn and Un , which now bear his name. Today these functions find use in primality testing and integer factorization, among other computational techniques. Vn and Un can be expressed in terms of the nth powers of the zeros of a quadratic polynomial, and throughout his writings Lucas speculated about the possible extension of these functions to those which could be expressed in terms of the nth powers of the zeros of a cubic polynomial and of a quartic polynomial. Indeed, at the end of his life he stated that "by searching for the addition formulas of the numerical functions which originate from recurrence sequences of the third or fourth degree, and by studying in a general way the laws of the residues of these functions for prime moduli... we would arrive at important new properties of prime numbers." We only have scattered hints concerning what functions Lucas had in mind because he provided so little information about them in his published and unpublished work.

In this talk I will discuss two pairs of functions that are easily expressed as certain symmetric polynomials of the zeros of a quartic polynomial and a sextic polynomial, respectively. Several new results, which illustrate the striking analogy between our functions and those of Lucas, will be discussed.