Analytic methods in Diophantine equations
Méthodes analytiques pour les équations Diophantiennes
(Org: **Michael Coons** (University of Newcastle, Austrailia) and/et **Patrick Ingram** (Colorado State University))

AMIR AKBARY, University of Lethbridge
On the greatest prime factor of some divisibility sequences

Let $P(m)$ denote the greatest prime factor of m. For integer $a > 1$, Ram Murty and Siman Wong proved that, under the assumption of the ABC conjecture, $P(a^n - 1) \gg n^{2-\epsilon}$ for any $\epsilon > 0$. Here we describe an analogous result for the divisibility sequence associated to denominators of multiples of a point on an elliptic curve. This is a joint work with Soroosh Yazdani.

CARMEN BRUNI, University of British Columbia
Twisted extensions of Fermat's Last Theorem

Let $x, y, z, p, n, \alpha \in \mathbb{Z}$ with $\alpha \geq 1$, p and $n \geq 5$ primes. In 2011, Michael Bennett, Florian Luca and Jamie Mulholland showed that the equation $x^3 + y^3 = p^\alpha z^n$ has no pairwise coprime nonzero integer solutions provided $p \geq 5$, $n \geq p^{2p}$ and $p \notin S$ where S is the set of primes q for which there exists an elliptic curve of conductor $N_E \in \{18q, 36q, 72q\}$ with at least one nontrivial rational 2-torsion point. I will present a solution that extends the result to include a subset of the primes in S; those $q \in S$ for which all curves with conductor $N_E \in \{18q, 36q, 72q\}$ with nontrivial rational 2-torsion have discriminants not of the form ℓ^2 or $-3m^2$ with $\ell, m \in \mathbb{Z}$. I will further discuss a similar approach used to solve the equation $x^5 + y^5 = p^\alpha z^n$ which in part generalizes work done from Billerey and Dieulefait in 2009. I will also discuss limitations of the method as they extend to further prime exponents.

STEPHEN CHOI, Simon Fraser University
On a Problem of Bourgain Concerning the Lp Norms of Exponential Sums

For $n \geq 1$ let

$$\mathcal{A}_n := \left\{ P : P(z) = \sum_{j=1}^{n} z^{k_j} : 0 \leq k_1 < k_2 < \cdots < k_n \,, k_j \in \mathbb{Z} \right\},$$

that is, $\mathcal{A}_n$ is the collection of all sums of n distinct monomials. These polynomials are also called Newman polynomials. Let

$$M_p(Q) := \left(\int_0^1 \left| Q(e^{i2\pi t}) \right|^p \, dt \right)^{1/p}, \qquad p > 0 \,.$$

We define

$$S_{n,p} := \sup_{Q \in \mathcal{A}_n} \frac{M_p(Q)}{\sqrt{n}} \qquad \text{and} \qquad S_p := \liminf_{n \to \infty} S_{n,p} \leq \Sigma_p := \sup_{n \in \mathbb{N}} S_{n,p}.$$

In this talk, we show that

$$\Sigma_p \geq \Gamma(1 + p/2)^{1/p} \,, \qquad p \in (0, 2) \,.$$

The special case $p = 1$ recaptures a recent result of Aistleitner, the best known lower bound for Σ_1.

KARL DILCHER, Dalhousie University
Pairs of reciprocal quadratic congruences involving primes

Using Pell equations and known solutions that involve Lucas sequences, we find all solutions of the reciprocal pair of quadratic congruences $p^2 \equiv \pm 1 \pmod{q}$, $q^2 \equiv \pm 1 \pmod{p}$ for odd primes p, q. In particular, we show that there is exactly one solution $(p, q) = (3, 5)$ when the right-hand sides are -1 and 1. When the right-hand sides are both -1, there are four known solutions, all of them pairs of Fibonacci primes, and when the the right-hand sides are both 1, there are no solutions. With similar methods one can completely characterize the solutions of $p^2 \equiv \pm N \pmod{q}$, $q^2 \equiv \pm N \pmod{p}$ for $N = 2$ and 4, and give partial results for $N = 3$ and 5. (Joint work with John B. Cosgrave).

ADAM FELIX, University of Lethbridge
On invariants of elliptic curves on average

In this talk, we discuss elliptic curve conjectures on average. The method will have applications to Koblitz's conjecture, the cyclicity problem and moments of the exponent of the group of points of the elliptic curve over finite fields. This is joint work with Amir Akbary.

KEVIN HARE, University of Waterloo
Simultaneous beta-expansions

We say that x has a beta-expansion with respect to β if there exists a sequence of a_i such that $x = \sum a_i \beta^{-i}$. It is known that if $\beta > 1$ is sufficiently close to 1, and the digits a_i are restricted to ± 1 then all x sufficiently close to 0 have an uncountable number of beta-expansions.

What is surprising is that for any x_1 and x_1 sufficiently close to 0 and $\beta_1 \neq \beta_2$ sufficiently close to 1 we can find a beta-expansion that is simultaneously a beta-expansion for x_1 in terms of β_1 and is a beta-expansion for x_2 in terms of β_2.

We will discuss the proof of this result, the generalization of this to higher numbers of simultaneous beta-expansions, and the limits of these techniques.

JONAS JANKAUSKAS, University of Waterloo, Department of Pure Mathematics
On Littlewood Polynomials with Prescribed Number of Zeros Inside the Unit Disk

We investigate the numbers of complex zeros of Littlewood polynomials $p(z)$ (polynomials with integer coefficients $\{-1, 1\}$) inside or on the unit circle $|z| = 1$, denoted by $N(p)$ and $U(p)$, respectively. Two types of Littlewood polynomials are considered: Littlewood polynomials with one sign change in the sequence of coefficients and Littlewood polynomials with one negative coefficient.

We obtain explicit formulas for $N(p)$, $U(p)$ for polynomials $p(z)$ of these types. In particular, we show that if $n+1$ is a prime number, then for each integer k, $0 \le k \le n-1$, there exists a Littlewood polynomial $p(z)$ of degree n with $N(p) = k$ and $U(p) = 0$. Furthermore, we describe some cases when the ratios $N(p)/n$ and $U(p)/n$ have limits as $n \to \infty$ and find the corresponding limit values.

WENTANG KUO, University of Waterloo
On Erdos-Pomerance conjecture

Let k be a global function field whose field of constants is the finite field $\mathbb{F}_q$. Let ∞ be a fixed place of degree one, and A is the ring of elements of k which have only ∞ as a pole.

Let ϕ be a sgn-normalized rank one Drinfeld A-module defined over $\mathcal{O}$, the integral closure of A in the Hilbert class field of A. We prove an analogue of a conjecture of Erdos and Pomerance for φ. Given any $0 \neq \alpha \in \mathcal{O}$ and an ideal $\mathfrak{M}$ in $\mathcal{O}$, let $f_\alpha(\mathfrak{M}) = \{f \in A \mid \phi_f(\alpha) \equiv 0 \pmod{\mathfrak{M}}\}$ be the ideal in A. We denote by $\omega\big(f_\alpha(\mathfrak{M})\big)$ the number of distinct prime ideal divisors of $f_\alpha(\mathfrak{M})$. If $q \neq 2$, we prove that there exists a normal distribution for the quantity

$$\frac{\omega\big(f_\alpha(\mathfrak{M})\big) - \frac{1}{2}(\log \deg \mathfrak{M})^2}{\frac{1}{\sqrt{3}}(\log \deg \mathfrak{M})^{3/2}}.$$

This is the jointed work with Yen-Liang Kuan and Wei-Chen Yao

JAMES PARKS, University of Lethbridge
Low-lying zeros of elliptic curve L-functions: Beyond the ratios conjecture

We study the low-lying zeros of L-functions attached to quadratic twists of a given elliptic curve E defined over $\mathbb{Q}$. We are primarily interested in the family of all twists coprime to the conductor of E and compute a very precise expression for the corresponding one-level density. In particular, for test functions whose Fourier transforms have sufficiently restricted support, we are able to compute the one-level density up to an error term that is significantly sharper than the square-root cancellation predicted by the L-functions Ratios Conjecture. This is joint work with Daniel Fiorilli and Anders Södergren.