## Number Theory
## Théorie des nombres
(Org: **Amir Akbary** (Lethbridge) and/et **Karl Dilcher** (Dalhousie))

**KEVSER AKTAS**, Queen's University
*Consecutive Squarefull Numbers*

Erdös conjectured that there are $\ll N^{\epsilon}$ consecutive squarefull number pairs for $n, n+1 \le N$ for any $\epsilon > 0$. We prove this conjecture under the asumption of the abc conjecture. We also show by an elementary method that this number is $\ll N^{2/5}$ unconditionally. At the end of the paper, we relate this to an old conjecture of Ankeny, Artin and Chowla regarding fundamental units of real quadratic fields.

**ABDULLAH AL-SHAGHAY**, Dalhousie University
*Analogues of the Binomial Coefficient Theorems of Gauss and Jacobi*

Two of the more well known congruences for binomial coefficients modulo $p$, due to Gauss and Jacobi, are related to the representation of an odd prime (or an integer multiple of the odd prime) $p$ as a sum of two squares (or an integer linear combination of two squares). These two congruences, along with many others, have been extended to analogues modulo $p^2$ and are well documented in the literature. More recently, J. Cosgrave and K. Dilcher have extended the congruences of Gauss, Jacobi, and a related one due to Hudson and Williams to their analogues modulo higher powers of $p$. We will have a look at the methods used by Cosgrave and Dilcher and discuss their application to obtaining more congruences for binomial coefficients.

**MICHAEL COONS**, University of Newcastle, Australia
*Algebraic independence results related to an automatic sequence*

We will survey some recent results on a specific automatic sequence related to Stern's diatomic sequence. After this survey, we present a method for determining the radial asymptotics of Mahler functions, and show how this information can be used to give algebraic independence results for automatic sequences and possibly their generalisations. (This is joint work with Wadim Zudilin and Richard Brent.)

**ADAM FELIX**, KTH, Royal Institute of Technology
*Common divisors of the index and order of $a$ modulo $p$*

Let $a$ be an integer different from $0$ or $\pm 1$. For primes $p \nmid a$, let $i_a(p)$ and $f_a(p)$ respectively denote the index and order of $a \bmod p$ in $(\mathbb{Z}/p\mathbb{Z})^*$. For $d \in \mathbb{N}$, we study the distribution of primes $p \le x$ for which $d | f_a(p)$ and $d | i_a(p)$. We also give some applications of these results.

**ALIA HAMIEH**, Queen's University
*Determining Hilbert modular forms by the central values of Rankin-Selberg convolutions*

We show that the central values of Rankin-Selberg convolutions, $L(f \otimes g, 1/2)$, uniquely determine a Hilbert modular form $g$, where $f$ varies in a carefully chosen infinite family of Hilbert modular forms. We prove our results in both the level and weight aspects. This is a joint work with Naomi Tanabe.

**PATRICK INGRAM**, Colorado State University
*Arithmetic dynamics of correspondences*

Arithmetic dynamics concerns the iteration of endomorphisms of an algebraic variety defined over a number field (or some other field of arithmetic interest). This talk will survey some attempts to extend some of the theory to finite-to-finite correspondences on varieties, focussing largely on the projective case.

---

**KEITH JOHNSON**, Dalhousie University
*Integer valued polynomials on rings of integer matrices*

Let $M_n(Z)$ denote the ring of $n \times n$ matrices with integer coefficients. If a polynomial $f(x)$ with rational coefficients has the property that $f(A) \in M_n(Z)$ for any $A \in M_n(Z)$ what can be said about $f$? That it need not necessarily have integer coefficients is demonstrated, for example, by the polynomial $x^2(x-1)^2(x^2+x+1)/2$ for $n=2$. This talk will present some recent results about the ring of polynomials satisfying this integrality property.

---

**OMAR KIHEL**, Brock University
*Denominators of algebraic numbers in a number field*

For any algebraic number $\gamma$, let $g(x)$ be the unique irreducible polynomial with integral coefficients, whose leading coefficient $c(\gamma)$ is positive, such that $g(\gamma) = 0$. Let $d(\gamma)$ be the denominator of $\gamma$. We fix a number field $K$, a prime $p$, a positive integer $k$ and we study the set of values of $v_p(c(\gamma))$, when $\gamma$ runs in the set of the primitive elements of $K$ over $\mathbb{Q}$, such that $v_p(d(\gamma)) = k$. We connect this set to the splitting types of $p$.

---

**ANDREW KNIGHTLY**, University of Maine
*The local equidistribution problem for Siegel modular forms*

For a fixed prime p, the p-th Hecke eigenvalues of GL(2) cusp forms of weight k and level N, when given certain natural harmonic weights, become equidistributed relative to the Sato-Tate measure as N+k goes to infinity. In joint work with Charles Li we prove an extension of this result to the symplectic group GSp(2n). The proof involves an asymptotic Petersson trace formula.

---

**MATILDE LALÍN**, Universite de Montreal
*The Mahler measure of elliptic curves*

The Mahler measure of a multivariable polynomial $P$ is given by the integral of $\log |P|$ where each of the variables moves on the unit circle and with respect to the Haar measure. In 1998 Boyd made a systematic numerical study of the Mahler measure of many polynomial families and found interesting conjectural relationships to special values of $L$-functions of elliptic curves. Recently, many of Boyd's conjectures have been proved by Burnault, Mellit, Rogers, and Zudilin. I will discuss some of those results and (possibly) other new ones (in collaboration with D. Samart and W. Zudilin).

---

**MARIE LANGLOIS**, Dalhousie University
*Elliptic Curves with Complex Multiplication and a Relation to their Quadratic Twist.*

This presentation will give a proof that every elliptic curve E over the rational numbers is isogenous to a quadratic twist if and only if E admits complex multiplication. To prove this, we use a famous result of Faltings comparing local and global isogenies of elliptic curves over number fields, and a famous theorem proven by Serre on the density of supersingular primes for elliptic curves over the rational numbers. While this result was certainly known to experts, a proof seems to not appear in the literature, my Master's thesis had for objective present this.

---

**CLAUDE LEVESQUE**, U. Laval
*On Thue equations*

This is joint work with Michel Waldschmidt. Consider the number field K=Q(w) of degree at least 3 over Q. We proved that for all units e of degree at least 3 in K, except for a finite number of them, the homogeneized version F(X,Y) of the minimal unitary polynomial F(X,1) of e has the property that the solutions of the Thue equation F(X,Y)=1 verify X=0 or Y=0. For the proof, which is not effective, we used the powerful subspace theorem of Wolfgang Schmidt. We also started to prove some effective results by using Baker's (and Waldschmidt's) results on linear forms in logarithms.

---

**ALLYSA LUMLEY**, University of Lethbridge

*New Bounds for $\psi(x;q,a)$*

Let $a,q$ be relatively prime integers. Then consider

$$\psi(x;q,a)=\sum_{\substack{n\leq x\\ n\equiv a \pmod q}}\Lambda(n).$$

We discuss new explicit bounds for $\psi(x;q,a)$, which provide an extension and improvement over the bounds given in the previous work of Ramaré and Rumely. This article introduces two new ideas. We smooth the prime counting function and use the partial verification of GRH by Platt along with an explicit zero-free region given by Kadiri.

This is joint work with Habiba Kadiri.

---

**KARYN MCLELLAN**, St. FX University

*A New Computation of Viswanath's Constant*

The random Fibonacci sequence is defined by $t_1=t_2=1$ and $t_n=\pm t_{n-1}+t_{n-2}$, for $n\geq 3$, where the $\pm$ sign is chosen at random with equal probabilities. We can think of all possible such sequences as forming a binary tree $T$. Viswanath has shown that almost all random Fibonacci sequences grow exponentially at the rate 1.13198824... He was only able to compute 8 decimal places of this constant, although Bai has extended the constant by 5 decimal places. We will discuss a new and simpler computation of Viswanath's constant which at present gives 8 decimal places of accuracy, but we feel this can be improved. It is based on a formula due to Kalmár-Nagy, and uses an interesting reduction of the tree $T$ developed by Rittaud.

---

**ROB NOBLE**, Dalhousie

*Conjugate algebraic numbers on plane curves*

If an algebraic number lies with all of its conjugates on a single line in the complex plane, then the number must either be totally real (so that the line is the real axis) or have rational real part and totally real imaginary part (so that the line is a vertical line consisting of those complex numbers with a fixed rational real part). Moving to the next level of complexity, we arrive at the conic sections. Roots of unity lie with their conjugates on the unit circle, and by a classical result of Kronecker, they provide the only example of algebraic integers satisfying this property. Work of Robinson, Ennola and Smyth completes the picture for circles, and Smyth and Berry have taken care of the other conic sections. It would be natural to next tackle the case of elliptic curves, but it may be easier to first treat curves of higher degree that arise as conic sections with respect to non-euclidean $L^p$ norms. In this talk, an overview of the literature on conjugate algebraic numbers on lines and conics with respect to the euclidean norm, as well as some preliminary results for circles with respect to $L^p$ norms will be given.

---

**JAMES PARKS**, University of Lethbridge

*The average number of elliptic curves with a fixed number of points*

Let $E$ be an elliptic curve defined over $\mathbb{Q}$. If $p$ is a prime of good reduction then we define the group of points on the reduced elliptic curve over $\mathbb{F}_p$ as $E_p(\mathbb{F}_p)$. Let $N$ be a fixed positive integer. David and Smith defined the function $M_E(N):=\#\{p\mid \#E_p(\mathbb{F}_p)=N\}$, and considered this function on average over a family of elliptic curves. They proved an asymptotic result with bounds on the size of the coefficients of the elliptic curves. In this talk we show how their result can be improved to hold for a larger range of elliptic curves.

---

**TATIANA HESSAMI PILEHROOD**, Fields Institute
*On $q$-analogs of Wolstenholme's theorem for multiple $q$-harmonic sums*

Congruences for ordinary single and multiple harmonic sums have been studied since the nineteenth century. It is well known that many multiple harmonic sums modulo a prime or a power of a prime can be expressed in terms of Bernoulli numbers. The situation with $q$-analogs is much less known. The first $q$-congruences for $q$-analogs of harmonic numbers, namely the $q$-analogs of Wolstenholme's theorem, were obtained by Andrews. In 2008, Dilcher showed that the higher order (depth 1) $q$-harmonic numbers are related to the so-called degenerate Bernoulli numbers. In this talk, we will discuss further $q$-extensions of the Wolstenholme theorem to multiple $q$-harmonic sums (strict and non-strict versions) of arbitrary depth on strings of one-two-three indices. This is joint work with Kh. Hessami Pilehrood and R. Tauraso.

---

**JULIAN ROSEN**, University of Waterloo
*Quadratic forms and curves on abelian surfaces*

The Néron-Severi group $\mathrm{NS}(A)$ of an algebraic variety $A$ is the group of divisors modulo algebraic equivalence. When $A = E_1 \times E_2$ is a product of two elliptic curves, there is a correspondence between elements of the Néron-Severi group and quadratic forms. In this talk, we will describe the correspondence and explain how geometric properties of a divisor correspond to arithmetic properties of the associated quadratic form. As an application, we will determine when a product $E_1 \times E_2$ contains a smooth embedded curve of any given genus, and when such a product embeds in $\mathbb{P}^4$. This is joint work with Ari Shnidman.

---

**NAOMI TANABE**, Queen's University
*Non-vanishing of Rankin-Selberg L-functions for Hilbert Modular Forms*

We establish some nonvanishing results on the central critical values of Rankin-Selberg L-functions for Hilbert modular forms in various families by obtaining bounds on their moments. This is an on-going joint project with Alia Hamieh.

---

**GRAEME TURNER**, Carleton University / Grenfell Campus, MUN
*The Conductor and Discriminant of Bicyclic Quartic Fields*

Let $K$ be a field of degree $4$ over the rational numbers which has a Galois group isomorphic to the Klein-4 group. Prime factorizations of the conductor and discriminant of $K$ are determined explicitly when $K$ is given in the form $K = \mathbb{Q}(\theta)$, where $\theta^4 + A\theta^2 + B\theta + C = 0$ for $A$, $B$, $C \in \mathbb{Z}$. The complete results will be presented exclusively in terms of the primes dividing $A$, $B$, $C$ and $A^2 - 4C$. This is joint work with Saban Alaca, Blair K. Spearman and Kenneth S. Williams.

---

**AKSHAA VATWANI**, Queen's University
*A higher rank Selberg sieve*

In May 2013, Yitang Zhang surprised the world by proving that there are infinitely many distinct primes $p$, $q$ such that $|p - q| < 70 \times 10^6$. In November 2013, Maynard and Tao independently gave a simplified approach to Zhang's theorem, obtaining better numerical results. We will present a general higher rank Selberg sieve, an application of which derives the results of Maynard and Tao. We will also discuss another application of this sieve to the $k$-tuple conjecture, which improves upon a result of Heath-Brown. This is joint work with Professor Ram Murty.