## L-Functions and Number Theory
## Functions L et théorie des nombres
(Org: **Clifton Cunningham** and/et **Mathew Greenberg** (Calgary))

**ALINA BUCUR**, UCSD
*Counting points on curves over finite fields*

A curve is a one dimensional space cut out by polynomial equations, such as $y^2 = x^3 + x$. In particular, one can consider curves over finite fields, which means the polynomial equations should have coefficients in some finite field and that points on the curve are given by values of the variables ($x$ and $y$ in the example) in the finite field that satisfy the given polynomials. A basic question is how many points such a curve has, and for a family of curves one can study the distribution of this statistic. We will give concrete examples of families in which this distribution is known or predicted, and give a sense of the different kinds of mathematics that are used to study different families.

**MICHAEL COONS**, Fields Institute and University of Waterloo
*An irrationality exponent related to Fermat numbers*

Let $\xi$ be a real number. The irrationality exponent $\mu(\xi)$ of $\xi$ is defined to be the supremum of the real numbers $\mu$ such that the inequality $|\xi - p/q| < q^{-\mu}$ has infinitely many solutions in rational numbers $p/q$. Let $F_n = 2^{2^n} + 1$ denote the $n$th Fermat number. In this talk, exploiting a connection between Hankel matrices and Padé approximants, we will sketch a proof that

$$\mu\left(\sum_{n\geqslant 0}\frac{1}{F_n}\right) = 2.$$

**MICHAEL DEWAR**, Queen's University
*The image and kernel of Atkin's $U_p$ operator modulo $p$*

We determine the image of Atkin's $U_p$ operator acting on $\pmod p$ reduced modular forms. In 1972, Serre showed that for level 1 modular forms, $U_p$ was contractionary (i.e. the image has lower weight than the preimage.) We determine the exact weight of the space of images and generalize to all levels not divisible by $p$. As a consequence, we determine the dimension of the kernel of $U_p \pmod p$ for large weights. This contrasts with the situation for small weights, which is still confoundingly mysterious.

**BRANDON FODDEN**, University of Lethbridge
*Lower bounds for fractional moments of L-functions*

We give a general result concerning the lower bounds for fractional moments of a class of analytic functions which have a Dirichlet series representation on a complex half-plane. Using this result, we establish lower bounds of the conjectured order of magnitude for factional moments of several well known L-functions. This is joint work with Amir Akbary.

**LEO GOLDMAKHER**, University of Toronto
*Subconvexity for a family of double Dirichlet series*

In 2003, Friedberg, Hoffstein, and Liemann introduced a family of double Dirichlet series which are built out of $n$-th order twists of a fixed Hecke $L$-series (a closely related series was also studied by Diaconu and Tian). Among other nice properties, a typical member $Z(s,w)$ of this family satisfies a functional equation taking $(s,w)$ to $(1-s,1-w)$. This gives rise to a 'convexity' bound for $Z(1/2+iu,1/2+it)$, which specializes to the usual notion of convexity when either $u$ or $t$ is fixed. I will outline work (joint with Valentin Blomer and Benoit Louvel) in which we establish a subconvexity bound in the $(u,t)$ aspect.

**HESTER GRAVES**, Queen's University
*A Generalization of the Lagrange and Jacobi 4-Square Theorems*

Lagrange proved that every natural number is a sum of 4 squares and Jacobi found a formula for the number of ways to write n as a sum of four squares. We will show ways to generalize Jacobi's formula to universal quaternary quadratic forms studied by Ramanujan.

**NATHAN JONES**, University of Mississippi
*The Lang-Trotter Conjecture for Frobenius fields*

Let E be an elliptic curve defined over Q. For each prime p of good reduction for E, consider the quadratic extension K(p) obtained by adjoining to Q the roots of the p-th Frobenius polynomial. In 1976, S. Lang and H. Trotter predicted a precise asymptotic formula for the number of primes p up to X for which K(p) is equal to a fixed imaginary quadratic field. In this talk, I will discuss recent joint work with A.C. Cojocaru and H. Iwaniec, in which we prove that the Lang-Trotter Conjecture holds "on average" over families of elliptic curves.

**DIMITRIS KOUKOULOPOULOS**, Centre de Recherches Mathematiques
*When the sieve works*

Let $\mathcal{P}$ be a set of prime numbers. A basic question in sieve methods is to understand how many integers up to $x$ are composed of prime factors solely from the set $\mathcal{P}$. A standard probabilistic heuristic predicts that this number is about $x\prod_{\substack{p\in\mathcal{P}^c\\ p\leq x}}\left(1-\frac{1}{p}\right)$. We show that this is true if the set $\mathcal{P}$ contains enough prime factors between $x^{1/u}$ and $x$, for some fixed $u$. This is joint work with Andrew Granville and Kaisa Matomaki.

**MATILDE LALIN**, Université de Montréal
*Remarks on $\frac{\zeta(2j+1)}{\pi^{2j+1}}$ and variants of the Ramanujan polynomials*

We prove that some sets of polynomials have all of their zeros on the unit circle, a fact that was originally observed by numerical experiments. The polynomials are interesting because they have coefficients which involve Bernoulli numbers, Euler numbers, and the odd values of the Riemann zeta function and are closely related to the Ramanujan polynomials that were recently investigateb by Murty, Smyth and Wang.

This is joint work with Mathew Rogers.

**XIANNAN LI**, Stanford University
*Bounds on the least quadratic non-residue*

In this talk, I will discuss joint work with K. Soundararajan on bounding the least quadratic non-residue on GRH. This improves previous bounds by E. Bach whose motivation for examining this problem arises from interesting applications in computational number theory. I will briefly describe this motivation as well as our improved bounds. Finally, I will speculate on "optimal" bounds on GRH.

**CHARLES SAMUELS**, Simon Fraser University and the University of British Columbia
*Mahler measures in products of algebraic numbers*

Let $M(\alpha)$ denote the Mahler measure of the algebraic number $\alpha$ and assume $\alpha_1, \dots, \alpha_N \in \bar{\mathbb{Q}}$ are such that $\alpha = \alpha_1 \cdots \alpha_N$. It seems a generally difficult problem to give non-trivial information about $M(\alpha_n)$ in terms of $\alpha$, although the $t$-metric Mahler measure $M_t(\alpha)$, first studied by Dubickas and Smyth in 2000, is a convenient object to consider in this context. In joint work with J. Jankauskas, we resolve an earlier conjecture regarding $M_t(\alpha)$ in the case where $\alpha \in \mathbb{Q}$. This result suggests a generalization to other $\alpha \in \bar{\mathbb{Q}}$ which turns out, however, to be false. We give an infinitely collection of counterexamples of degree $2$ and discuss possible modifications to the conjecture.

**ETHAN SMITH**, Centre de recherches mathematiques
*Elliptic curves with a given number of points modulo $p$*

Let $E$ be an elliptic curve, $N$ a positive integer, and $M_E(N)$ the number of primes $p$ for which the reduction of $E$ modulo $p$ possesses exactly $N$ points over $\mathbb{F}_p$. We consider the problem of estimating $M_E(N)$. On average (over the set of all elliptic curves defined over $\mathbb{Q}$), we show upper bounds that are significantly better than the trivial bound. Under some hypotheses, we obtain an asymptotic formula for the average value of $M_E(N)$. This is joint work with Chantal David.

**MATTHEW SMITH**, University of British Columbia
*On solution-free sets via local uniformity and energy incrementing*

We consider a system of $k$ diagonal polynomials of degrees $1, 2, \dots, k$. Using methods developed by W.T. Gowers and refined by Green and Tao to obtain bounds in the 4-term case of Szemeredi's Theorem on long arithmetic progressions, we show that if a subset $\mathcal{A}_N$ of the natural numbers up to $N$ of size $\delta_N N$ exhibits sufficiently small local polynomial bias, then it furnishes roughly the expected number of solutions to the given system. If $\mathcal{A}_N$ furnishes no non-trivial solutions to the system, then we show via an energy incrementing argument that there is a concentration in a Bohr set of pure degree $k$, and consequently in a long arithmetic progression. We show that this leads to a bound on the density $\delta_N$ of the set $\mathcal{A}_N$ of the form $\delta_N \ll \exp(-c\sqrt{\log\log N})$, where $c > 0$ is a constant dependent at most on $k$.

**FRANK THORNE**, Stanford University
*Secondary terms in counting functions for cubic fields*

We will discuss our proof of secondary terms of order $X^{5/6}$ in the Davenport-Heilbronn theorems on cubic fields and 3-torsion in class groups of quadratic fields. For cubic fields this confirms a conjecture of Datskovsky-Wright and Roberts. We also will describe some generalizations, in particular to arithmetic progressions, where we discover a curious bias in the secondary term.

Roberts' conjecture has also been proved independently by Bhargava, Shankar, and Tsimerman. Their proof uses the geometry of numbers, while our proof uses the analytic theory of Shintani zeta functions. We will also discuss a combined approach which yields further improved error terms.

This is joint work with Takashi Taniguchi.

**TIM TRUDGIAN**, University of Lethbridge
*Tightening the screws on $S(t)$*

Backlund [1918] gave an estimate for $S(t)$, the argument of the Riemann zeta-function along the critical line. This estimate was improved, slightly, by Rosser [1941]: he showed that $|S(t)| \leq 0.137\log t + 0.443\log\log t + 1.588$, whenever $t \geq 1467$.

Such an estimate is used when approximating the potential contribution of zeroes off the critical line. This is used in explicit versions of the prime number theorem and the zero-free region. In this talk I will outline a sharpening of Rosser's result.