ELEFANT

Emerging Leaders and Evolving Frontiers in Analytic Number Theory
Hausdorff Center for Mathematics
14 – 18 July 2014

L-functions and Kloosterman sums
Valentin Blomer (Universität Göttingen)
We prove various asymptotic formulae with power saving error terms for moments of L-functions, based on spectral analysis of automorphic forms and an algebro-arithmetic treatment of short sums of products of Kloosterman sums.

Cycle integrals of meromorphic forms
Kathrin Bringmann (Universität Köln)
This talk generalizes classical sums of quadratic forms, which are cusp forms and which played a key role in connection with the Shimura/Shintani lift, to the meromorphic setting. Integrating against these forms leads to certain CM traces which are related to new automorphic objects. This work in preparation is joint with Ben Kane.

The tic-tac-toe of Manin's conjecture
Tim Browning (University of Bristol)
The Manin conjecture concerns the distribution of rational solutions to suitable systems of Diophantine equations. The landscape has undergone extensive development since it was first proposed a quarter of a century ago. In this talk I will give a brief account of certain recent extremal results and highlight some of the difficulties that lie ahead.

Anisotropic Diagonal Forms
Jörg Brüdern (Universität Göttingen)
This talk is based on joint work with H. Godinho, and is motivated by the famous conjecture of Artin that a rational form of degree d in more than d^2 variables should have non-trivial zeros over the p-adic numbers. Although the conjecture is desperately false, it is known to hold for diagonal forms. Also, the bound on the number of variables is sharp in that there are examples of diagonal forms in d^2 variables that have no non-trivial zeros. By a new method related to zero sum problems in finite fields we shall be able to classify all such examples provided that the number of variables is not too much smaller than d^2. In a certain sense, the results turn out to be best possible, and are new whenever the degree exceeds 2.

Effective Sato-Tate
Alina Bucur (UC San Diego)
Based on the Lagarias-Odlyzko effectivization of the Chebotarev density theorem, Kumar Murty gave an effective version of the Sato-Tate conjecture for an elliptic curve conditional on analytic continuation and Riemann hypothesis for the symmetric power L-functions. We use a stronger version of Chebotarev from the same Lagarias-Odlyzko paper to give a similar conditional effectivization of the generalized Sato-Tate conjecture for an arbitrary motive. As an application, we give a conditional upper bound of the form $O((\log N)^2)$ for the smallest prime at which two given rational elliptic curves with conductor at most N have Frobenius traces of opposite sign. Then we will talk about the corresponding result for higher dimensional abelian varieties.

Multiplicative orders and distribution of points on varieties mod p
Mei-Chu Chang (UC Riverside)
The questions considered belong to the general theme of "unlikely intersections" but in this talk we focus on various instances in the mod p setting, where p is a large prime. We will discuss in particular mod p versions of Lang's conjecture on torsion points on varieties and related questions. Generally speaking, in the

absence of a direct finite field approach, our basic method consists in lifting the problem to a number field and then relying on finiteness results in this setting. The conclusions for individual p are rather weak but much stronger for "almost all p." Our main tool is effective Nullstellensatz.

A Sharpened Hausdorff-Young Inequality

Michael Christ (UC Berkeley)

One of the most fundamental facts about the Fourier transform is the Hausdorff-Young inequality, which states that for any locally compact Abelian group, the Fourier transform maps L^p boundedly to L^q, where the two exponents are conjugate and $p \in [1, 2]$. For Euclidean space, the optimal constant in this inequality was found by Babenko for q an even integer, and by Beckner for general exponents. Lieb showed that all extremizers are Gaussian functions. This is a uniqueness theorem; these Gaussians form the orbit of a single function under the group of symmetries of the inequality.

We establish a stabler form of uniqueness for $1 < p < 2$: (i) If a function f nearly achieves the optimal constant in the inequality, then f must be close in norm to a Gaussian. (ii) There is a quantitative bound involving the square of the distance to the nearest Gaussian. The qualitative form (i) can be equivalently formulated as a precompactness theorem in the style of the calculus of variations. Form (ii) is a strengthening of the inequality. Ingredients taken from additive combinatorics are at the heart of the analysis. Arithmetic progressions, of arbitrarily high rank, play an important part.

The frequency of elliptic curve groups and group orders

Chantal David (Concordia University)

We present in this talk several results related to the counting functions

$$\begin{aligned} M_E(N) &= \#\{p : \#E(\mathbb{F}_p) = N\} \\ M_E(G) &= \#\{p : \#E(\mathbb{F}_p) \simeq G_{m,k}\} \end{aligned}$$

where E is a fixed elliptic curve over $\mathbb{Q}$ without multiplication, N is a fixed integer, and $G \simeq Z/m\mathbb{Z} \times \mathbb{Z}/mk\mathbb{Z}$, where $N = m^2k$. We remark that the set of primes counted by $M_E(N)$ and $M_E(G)$ is finite because of the Hasse bound, since the primes counted are in the interval $(N + 1 - 2\sqrt{N}, N + 1 + 2\sqrt{N})$. This gives the trivial bound $M_E(N) \leq 4\sqrt{N}/\log N$, and no better bound is known for curves without complex multiplication. We present in this talk several average results for $M_E(N)$ and $M_E(G)$. Averaging over all elliptic curves, one can prove that, assuming some conjecture for the distribution of primes on the short intervals $(N + 1 - 2\sqrt{N}, N + 1 + 2\sqrt{N})$, we have that as $m, k \to \infty$ and $m \leq (\log k)^C$ that

$$\frac{1}{4AB} \sum_{|a| \leq A, |b| \leq B} M_{E(a,b)}(G) \sim \frac{\#G}{\#\mathrm{Aut}(G)} K(G) \frac{1}{\log \#G},$$

for some explicit constant $K(G)$ which is uniformly bounded in terms of G.

We also show that the above asymptotic holds unconditionally for "most" groups G, and as an upper bound on the average, using average results for the distribution of primes in short intervals and the combinatorial sieve. Finally, we revisit the average results in terms of random matrix theory, giving an interpretation for the probabilities that $\#E(\mathbb{F}_p) = N$ and $E(\mathbb{F}_p) \simeq G_{m,k}$ on average over the finite fields $\mathbb{F}_p$. This follows the work of Gekeler for the Lang-Trotter conjecture. In some work in progress, we use the random matrix interpretation to re-prove several average results for distribution associated to elliptic curves. This is joint work with F. Chandee, D. Koukoulopoulos and E. Smith.

Largest prime factor of integer value of polynomial of degree 4

Régis de la Bretèche (Université Paris Diderot)

Let $P^+(n)$ denote the largest prime factor of the integer n. Using Heath-Brown and Dartyge methods, we prove that for all even unitary irreducible quartic polynomials Φ with integral coefficients and an associated Galois group isomorphic to V_4, there exists a positive constant c_Φ such that the set of integers $n \leq X$ satisfying $P^+(\Phi(n)) \geq X^{1+c_\Phi}$ has a positive density. Such a result was recently proved by Dartyge for $\Phi(n) = n^4 - n^2 + 1$.

Intersections of cubic and quadric hypersurfaces
Rainer Dietmann (Royal Holloway)
Though there is quite a substantial literature about the intersection of rational hypersurfaces all having the same degree, in particular Birch's influential 1962 paper on 'Forms in many variables', much less is known in the case of different degrees. In this talk we want to report on recent joint work with Tim Browning and Roger Heath-Brown on the simplest non-trivial such example, namely the intersection of a quadric Q and a cubic C in n variables. Writing ϱ for the rank of Q and h for the h-invariant for C, we can for example show that the smooth Hasse principle for the intersection $X : C = Q = 0$ holds true, providing that $(h-32)(\varrho-4) > 128$. If X is non-singular, this would in particular allow one to take $n = 37$, but in this case one can reduce the number of variables even further to $n = 29$. We also established a result valid under very mild assumptions, to the effect that X has a non-trivial rational point providing that n is at least 49, the cubic form contains at least 17 variables explicitly (in a sense to be defined appropriately), and X has a smooth real point. The proof uses the circle method, both classically and in its more modern Poisson summation form, and also a fibration technique approach in case only very mild assumptions for C and Q are satisfied.

Unnormalized differences between zeros of L-functions
Kevin Ford (U. Illinois Urbana-Champaign)
We prove, unconditionally, a subtle inequity in the distribution of unnormalized differences between imaginary parts of zeros of the Riemann zeta function and of other L-functions. We discuss several striking aspects of this phenomenon. For example, the location of each Riemann zero is encoded in the distribution of large Riemann zeros. Also, the (analytic) rank of an elliptic curve over $\mathbb{Q}$ is encoded in the sequences of zeros of *other* L-functions, not only the one associated to the curve. This is joint work with Alexandru Zaharescu.

Thin Monodromy Groups
Elena Fuchs (Berkeley and U. Illinois Urbana-Champaign)
In recent years, it has become interesting from a number-theoretic point of view to be able to determine whether a finitely generated subgroup of $GL_n(\mathbb{Z})$ is a so-called thin group. In general, little is known as to how to approach this question. In this talk we discuss this question in the case of hypergeometric monodromy groups, which were studied in detail by Beukers and Heckman in 1989. We will convey what is known, explain some of the difficulties in answering the thinness question, and show how one can successfully answer it in many cases where the group in question acts on hyperbolic space. This work is joint with Meiri and Sarnak.

Beyond endoscopy and nonabelian trace formulae
Jayce Getz (Duke University)
Langlands has proposed a method to establish Langlands functoriality in general. The basic idea is to build L-functions into the trace formula and take their residues, thereby isolating automorphic representations that are functorial lifts. As emphasized by Sarnak, the analytic difficulties in executing Langlands' proposal are formidable, and in particular it is unknown in most cases how to produce absolutely convergent trace formulae via this method. In this talk we will discuss a soft method to circumvent this difficulty in a special case relevant to establishing base change and descent along nonsolvable Galois extensions. This is joint work with P.E. Herman.

Bob Hough's solution of Erdős's covering congruences conjecture
Ben Green (University of Oxford)
One of Paul Erdős's very favourite questions (possibly his favourite of all) was the following: Let M_0 be arbitrary. Can you cover $\mathbb{Z}$ with finitely many congruence conditions $a \pmod m$, $m > M_0$, at most one for each m? In 2013, Bob Hough showed that the answer is no if M_0 is sufficiently large. That is, there is some constant C such that in any covering of $\mathbb{Z}$ by finitely many congruences to distinct moduli m, at least one of the m's must be at most C. I will present his proof.

A general simple relative trace formula and a relative Weyl law
Heekyoung Hahn (Duke University)
In this talk, we prove a general simple relative trace formula. As an application, we prove a relative analogue of the Weyl law. This is joint work with Jayce R. Getz.

Primes of the form $a^2 + p^4$
Roger Heath-Brown (University of Oxford)
The well-known theorem of Friedlander and Iwaniec says that there are infinitely many primes of the form $a^2 + b^4$. Our result shows that this remains true if one restricts b to take only prime values. The argument appears to be simpler than that used by Friedlander and Iwaniec, and can probably be extended to allow b to take values in other sequences satisfying a Siegel-Walfisz condition. This is joint work with Xiannan Li.

Local-Global in Thin Orbits and Applications
Alex Kontorovich (Yale University)
We will discuss an ongoing program with Jean Bourgain to study local-global phenomena in orbits that are "thin." Consequences include applications to numerical integration, pseudorandom sequences, and Diophantine geometry.

Mahler measures and $L(\mathscr{E}, 3)$
Matilde Lalín (Université de Montréal)
The Mahler measure of a Laurent polynomial P is defined as the integral of $\log|P|$ over the unit torus with respect to the Haar measure. For multivariate polynomials, it often yields special values of L-functions. In this talk I will discuss some of these relationships and current developments and present some results involving $L(\mathscr{E}, 3)$ for $\mathscr{E}$ an elliptic curve.

Small gaps between primes
James Maynard (Montreal)
It is believed that there should be infinitely many pairs of primes which differ by 2; this is the famous twin prime conjecture. More generally, it is believed that for every positive integer m there should be infinitely many sets of m primes, with each set contained in an interval of size roughly $m \log m$. Although proving these conjectures seems to be beyond our current techniques, recent progress has enabled us to obtain some partial results. We will introduce a refinement of the 'GPY sieve method' for studying these problems. This refinement will allow us to show (amongst other things) that $\liminf_n (p_{n+m} - p_n) < \infty$ for any integer m, and so there are infinitely many bounded length intervals containing m primes. We also discuss some extensions of this result.

Elliptic curves and random matrices
Nina Snaith (University of Bristol)
There is much evidence to support the Katz-Sarnak philosophy in the case of a family of quadratic twists of an elliptic curve. That is, as the conductor, the parameter that orders the curves in the family, becomes large, the zeros of the associated L-functions behave statistically like the eigenvalues of matrices from the orthogonal group $O(N)$. In 2006 Steven J. Miller produced numerical evidence that for finite conductor, statistics of zeros in these families of L-functions are not well modeled by the group $O(N)$. In this talk we will investigate some statistics of zeros when we are far from the large-conductor limit.

Moments of L-functions and a one-sided central limit theorem
Kannan Soundararajan (Stanford University)
I will discuss recent work with Radziwill which shows that if asymptotics for some moment in a family of L-functions is known (with a little extra flexibility) then one may derive upper bounds of the conjectured order of magnitude for all smaller moments. This work also leads to a conjecture on the distribution of the size of Tate-Shafarevich groups of rank zero quadratic twists of a given elliptic curve, and one can establish a one sided central limit theorem proving one part of that conjecture.

Equidistribution estimates for the primes
Terence Tao (UC Los Angeles)
One of the basic questions in analytic number theory is to understand how the prime numbers are distributed in arithmetic progressions; this information can be combined with sieve-theoretic tools to obtain results such as the recent establishment of an infinite sequence of bounded gaps between the prime numbers. For progressions of small modulus, one can obtain satisfactory results using the theory of Dirichlet L-functions,

but for progressions of large modulus, even the generalised Riemann hypothesis is insufficient to obtain useful distributional results for all progressions. However, a celebrated and very useful theorem of Bombieri and Vinogradov unconditionally gives equidistribution of arithmetic progressions *on the average*, as long as the spacing of the progression is less than the square root of the magnitude of the entries.

It has been a major challenge to break this "square root barrier" and obtain stronger equidistribution estimates on the primes. Limited results in this direction were initially obtained by Bombieri, Fouvry, Friedlander, and Iwaniec, but last year there was a significant advance by Yitang Zhang, who obtained a robust family of such estimates, by combining the dispersion method of Linnik with known estimates on exponential sums. These estimates have since been strengthened, with somewhat simplified proofs, by the online collaborative Polymath project, and have been used to improve the bounds on gaps between primes. In this talk, we will survey these equidistribution estimates, and give some indication of their proofs.

Efficient congruencing and a Diophantine inequality of Bourgain and Demeter
Trevor Wooley (University of Bristol)
As a consequence of recent work concerning the proof of the ℓ^2 decoupling conjecture, Bourgain and Demeter show that for each fixed $k \geq 2$ and $C > 0$, the Diophantine system

$$|n_1^k + n_2^k + n_3^k - n_4^k - n_5^k - n_6^k| \leq CN^{k-2}$$
$$n_1 + n_2 + n_3 - n_4 - n_5 - n_6 = 0$$

has $O(N^{3+\epsilon})$ integral solutions with $n_i \leq N$. We explore the consequences of the efficient congruencing method (from Vinogradov's mean value theorem) for this problem and its generalisations.