Mathematisches Forschungsinstitut Oberwolfach

Report No. 50/2019

DOI: 10.4171/OWR/2019/50

Analytic Number Theory

Organized by
Jörg Brüdern, Göttingen
Kaisa Matomäki, Turku
Robert C. Vaughan, State College
Trevor D. Wooley, West Lafayette

3 November – 9 November 2019

Abstract. Analytic number theory is a subject which is central to modern mathematics. There are many important unsolved problems which have stimulated a large amount of activity by many talented researchers. At least two of the Millennium Problems can be considered to be in this area. Moreover in recent years there has been very substantial progress on a number of these questions.

Mathematics Subject Classification (2010): 11Bxx, 11Dxx, 11Jxx-11Pxx.

Introduction by the Organizers

The workshop *Analytic Number Theory*, organised by Jörg Brüdern (Göttingen), Kaisa Matomäki (Turku), Robert C. Vaughan (State College) and Trevor D. Wooley (West Lafayette) was well attended with over 50 participants from a broad geographic spectrum, all either distinguished and leading workers in the field or very promising younger researchers.

Over the last decade or so there has been considerable and surprising movement in our understanding of a whole series of questions in analytic number theory and related areas. This includes the establishment of infinitely many bounded gaps in the primes by Zhang, Maynard and Tao, significant progress on our understanding of the behaviour of multiplicative functions such as the Möbius function by Matomäki and Radziwiłł, the work on the Vinogradov mean value theorem by Wooley, and the injection of ideas from harmonic analysis by Bourgain, Demeter and Guth leading to the best possible version of the theorem, and the substantial

recent activity by Bhargava, de la Bretèche, Browning, Heath-Brown and Salberger in applying analytic methods to making statistical counts of what are, in principal, algebraic or geometric objects, such as number fields, ranks of elliptic curves, and the density of rational points on varieties, including various forms of the Manin-Peyre conjectures.

The workshop was most timely as two of the participants, Koukoulopoulos and Maynard, had just proved the Duffin and Schaeffer conjecture, a famous problem in the metric theory of diophantine approximation dating from 1941, and they set the tone on the first morning by presenting their work in a double session.

There was also significant progress reported by Fouvry, Matomäki, Sawin, Soundararajan, Teräväinen and others on properties of multiplicative functions. Thus Matomäki reported on some striking results on averages of the Möbius function in short intervals which were stronger than what one expects to obtain from the theory of the Riemann zeta function alone.

Bharghava, Blomer, Browning, Ghidelli, Heath-Brown, Salberger, Thompson, Zhao spoke on various counting questions using analytic techniques combined with methods from algebraic geometry and combinatorics. For example Bhargava gave precise estimates for the frequency with which a large class of integral forms can take on squarefree values when the variables lie in a large box centered at the origin. This is a known difficult open question for general integral forms of degree three or more, but Bhargava showed that it is possible to treat forms which arise as discriminants of polynomials. Moreover it is particularly useful in applications to be able to ascertain when such forms are squarefree.

Salberger gave precise estimates for the number of rational points of bounded height on threefolds and fourfolds which were significantly stronger than those obtained earlier by Browning and Heath-Brown.

There were also accounts of work in a variety of other directions. Chow showed how methods of combinatorics and analytic number theory could be applied to classify solutions of diophantine equations. Green presented results which improved our understanding of Hooley's Δ function, a function fundamental to much work in additive number theory. There was also a surprising result by Grimmelt on Goldbach numbers in short intervals and Lamzouri described striking new results on the distribution of maximal exponential sums over rings of residue classes, and in particular Kloosterman sums. Conrey and Florea presented new results on various kinds of Dirichlet L-functions and their mean values.

One evening Montgomery led a problem session which gave rise to a large number of interesting questions and a lively discussion.

There was a general feeling among the participants that the quality of research reported upon and discussed at the workshop made the meeting one of the very strongest and most stimulating that they had attended.

Acknowledgement: The MFO and the workshop organizers would like to thank the National Science Foundation for supporting the participation of junior researchers in the workshop by the grant DMS-1641185, "US Junior Oberwolfach Fellows".

Workshop: Analytic Number Theory

Table of Contents

Abstracts

Squarefree values of polynomial discriminants

Manjul Bhargava

The purpose of this talk is to determine the density of monic integer polynomials of given degree whose discriminant is squarefree. For polynomials $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$, the term $(-1)^i a_i$ represents the sum of the i-fold products of the roots of f. It is thus natural to order monic polynomials $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ by the height $H(f) := \max\{|a_i|^{1/i}\}$ (see, e.g., [3], [8], [10]). We determine the density of monic integer polynomials having squarefree discriminant with respect to the ordering by this height, and show that the density is positive. The existence of infinitely many monic integer polynomials of each degree having squarefree discriminant was first demonstrated by Kedlaya [6]. However, it has not previously been known whether the density exists or even that the lower density is positive.

To state the theorem, define the constants $\lambda_n(p)$ by

$$\lambda_n(p) = \begin{cases} 1 & \text{if } n = 1, \\ 1 - \dfrac{1}{p^2} & \text{if } n = 2, \\ 1 - \dfrac{2}{p^2} + \dfrac{1}{p^3} & \text{if } n = 3, \\ 1 - \dfrac{1}{p} + \dfrac{(p-1)^2(1-(-p)^{2-n})}{p^2(p+1)} & \text{if } n \geq 4 \end{cases} \tag{1}$$

for $p \neq 2$; also, let $\lambda_1(2) = 1$ and $\lambda_n(2) = 1/2$ for $n \geq 2$. Then a result of Brakenhoff [1, Theorem 6.9] states that $\lambda_n(p)$ is the density of monic polynomials over $\mathbb{Z}_p$ having discriminant indivisible by p^2. Let $\lambda_n := \prod_p \lambda_n(p)$, where the product is over all primes p. We prove:

Theorem 1. *Let $n \geq 1$ be an integer. Then when monic integer polynomials $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ of degree n are ordered by*

$$H(f) := \max\{|a_1|, |a_2|^{1/2}, \ldots, |a_n|^{1/n}\},$$

the density having squarefree discriminant $\Delta(f)$ exists and is equal to $\lambda_n > 0$.

Our method of proof implies that the theorem remains true even if we restrict only to those polynomials of a given degree n having a given number of real roots.

It is easy to see from the definition of the $\lambda_n(p)$ that the λ_n rapidly approach a limit λ as $n \to \infty$, namely,

$$\lambda = \lim_{n\to\infty} \lambda_n = \prod_p \left(1 - \frac{1}{p} + \frac{(p-1)^2}{p^2(p+1)}\right) \approx 35.8232\%. \tag{2}$$

Therefore, as the degree tends to infinity, the probability that a random monic integer polynomial has squarefree discriminant tends to $\lambda \approx 35.8232\%$.

In algebraic number theory, one often considers number fields that are defined as a quotient ring $K_f := \mathbb{Q}[x]/(f(x))$ for some irreducible integer polynomial $f(x)$. The question naturally arises as to whether $R_f := \mathbb{Z}[x]/(f(x))$ gives the ring of integers of K_f. Our second main theorem states that this is in fact the case for most polynomials $f(x)$. We prove:

Theorem 2. *The density of irreducible monic integer polynomials $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$ of degree $n > 1$, when ordered by*

$$H(f) := \max\{|a_1|, |a_2|^{1/2}, \ldots, |a_n|^{1/n}\},$$

such that $\mathbb{Z}[x]/(f(x))$ is the ring of integers in its fraction field is $\zeta(2)^{-1}$.

Note that $\zeta(2)^{-1} \approx 60.7927\%$. Since a density of 100% of monic integer polynomials are irreducible (and indeed have associated Galois group S_n) by Hilbert's irreducibility theorem, it follows that $\approx 60.7927\%$ of monic integer polynomials f of any given degree $n > 1$ have the property that f is irreducible and $\mathbb{Z}[x]/(f(x))$ is the maximal order in its fraction field. The quantity $\rho_n(p) := 1 - 1/p^2$ represents the density of monic integer polynomials of degree $n > 1$ over $\mathbb{Z}_p$ such that $\mathbb{Z}_p[x]/(f(x))$ is the maximal order in $\mathbb{Q}_p[x]/(f(x))$. The determination of this beautiful p-adic density, and its independence of n, is due to Hendrik Lenstra (see [1, Proposition 3.5]). Theorem 2 again holds even if we restrict to polynomials of degree n having a fixed number of real roots.

If the discriminant of an order in a number field is squarefree, then that order must be maximal. Thus the irreducible polynomials counted in Theorem 1 are a subset of those counted in Theorem 2. The additional usefulness of Theorem 1 in some arithmetic applications is that if $f(x)$ is a monic irreducible integer polynomial of degree n with squarefree discriminant, then not only is $\mathbb{Z}[x]/(f(x))$ maximal in the number field $\mathbb{Q}[x]/(f(x))$ but the associated Galois group is necessarily the symmetric group S_n (see, e.g., [11], [7] for further details and applications).

We prove both Theorems 1 and 2 with power-saving error terms. More precisely, let $V_n^{\mathrm{mon}}(\mathbb{Z})$ denote the subset of $\mathbb{Z}[x]$ consisting of all monic integer polynomials of degree n. Then it is easy to see that

$$\#\{f \in V_n^{\mathrm{mon}}(\mathbb{Z}) : H(f) < X\} = 2^n X^{\frac{n(n+1)}{2}} + O(X^{\frac{n(n+1)}{2}-1}).$$

We prove

$$\#\{f \in V_n^{\mathrm{mon}}(\mathbb{Z}) : H(f) < X \text{ and } \Delta(f) \text{ squarefree}\} = \lambda_n \cdot 2^n X^{\frac{n(n+1)}{2}} + O_\varepsilon(X^{\frac{n(n+1)}{2}-\frac{1}{5}+\varepsilon});$$

$$\#\{f \in V_n^{\mathrm{mon}}(\mathbb{Z}) : H(f) < X \text{ and } \mathbb{Z}[x]/(f(x)) \text{ maximal}\} = \frac{6}{\pi^2} \cdot 2^n X^{\frac{n(n+1)}{2}} + O_\varepsilon(X^{\frac{n(n+1)}{2}-\frac{1}{5}+\varepsilon})$$

for $n > 1$.

These asymptotics imply Theorems 1 and 2. Since it is known that the number of reducible monic polynomials of a given degree n is of a strictly smaller order of

magnitude than the error terms above, it does not matter whether we require f to be irreducible in the above asymptotic formulae.

Recall that a number field K is called *monogenic* if its ring of integers is generated over $\mathbb{Z}$ by one element, i.e., if $\mathbb{Z}[\theta]$ gives the maximal order of K for some $\theta \in K$. As a further application of our methods, we obtain the following corollary to Theorem 1:

Corollary 3. *Let $n > 1$. The number of isomorphism classes of number fields of degree n and absolute discriminant less than X that are monogenic and have associated Galois group S_n is $\gg X^{1/2+1/n}$.*

We note that our lower bound for the number of monogenic S_n-number fields of degree n improves slightly the best-known lower bounds for the number of S_n-number fields of degree n, due to Ellenberg and Venkatesh [5, Theorem 1.1], by simply forgetting the monogenicity condition in Corollary 3. We conjecture that the exponent in our lower bound in Corollary 3 for monogenic number fields of degree n is optimal.

As is illustrated by Corollary 3, Theorems 1 and 2 give a powerful method to produce number fields of a given degree having given properties or invariants. We give one further example of interest. Given a number field K of degree n with r real embeddings $\xi_1, \dots, \xi_r$ and s complex conjugate pairs of complex embeddings $\xi_{r+1}, \bar{\xi}_{r+1}, \dots, \xi_{r+s}, \bar{\xi}_{r+s}$, the ring of integers $\mathcal{O}_K$ may naturally be viewed as a lattice in $\mathbb{R}^n$ via the map $x \mapsto (\xi_1(x), \dots, \xi_{r+s}(x)) \in \mathbb{R}^r \times \mathcal{C}^s \cong \mathbb{R}^n$. We may thus ask about the length of the shortest vector in this lattice generating K.

In their final remark [5, Remark 3.3], Ellenberg and Venkatesh conjecture that the number of number fields K of degree n whose shortest vector in $\mathcal{O}_K$ generating K is of length less than Y is $\asymp Y^{(n-1)(n+2)/2}$. They prove an upper bound of this order of magnitude. We use Theorem 2 to prove also a lower bound of this size, thereby proving their conjecture:

Corollary 4. *Let $n > 1$. The number of isomorphism classes of number fields K of degree n whose shortest vector in $\mathcal{O}_K$ generating K has length less than Y is $\asymp Y^{(n-1)(n+2)/2}$.*

Again, Corollary 4 remains true even if we impose the condition that the associated Galois group is S_n (by using Theorem 1 instead of Theorem 2).

Finally, we remark that our methods allow the analogues of all of the above results to be proven with any finite set of local conditions imposed at finitely many places (including at infinity); the orders of magnitudes in these theorems are then seen to remain the same—with different (but easily computable in the cases of Theorems 1 and 2) positive constants—provided that no local conditions are imposed that force the set being counted to be empty (i.e., no local conditions are imposed at p in Theorem 1 that force p^2 to divide the discriminant, no local conditions are imposed at p in Theorem 2 that cause $\mathbb{Z}_p[x]/(f(x))$ to be non-maximal over $\mathbb{Z}_p$, and no local conditions are imposed at p in Corollary 3 that cause such number fields to be non-monogenic locally).

References

[1] A. Ash, J. Brakenhoff, and T. Zarrabi, Equality of Polynomial and Field Discriminants, *Experiment. Math.* **16** (2007), 367–374.

[2] M. Bhargava, The geometric sieve and the density of squarefree values of polynomial discriminants and other invariant polynomials, `http://arxiv.org/abs/1402.0031`.

[3] M. Bhargava and B. Gross, The average size of the 2-Selmer group of Jacobians of hyperelliptic curves having a rational Weierstrass point, *Automorphic representations and L-functions*, 23–91, Tata Inst. Fundam. Res. Stud. Math. **22**, Mumbai, 2013.

[4] T. Ekedahl, An infinite version of the Chinese remainder theorem, *Comment. Math. Univ. St. Paul.* **40** (1991), 53–59.

[5] J. Ellenberg and A. Venkatesh, The number of extensions of a number field with fixed degree and bounded discriminant, *Ann. of Math.* (2) **163** (2006), no. 2, 723–741.

[6] K. S. Kedlaya, A construction of polynomials with squarefree discriminants, *Proc. Amer. Math. Soc.* **140** (2012), 3025–3033.

[7] T. Kondo, Algebraic number fields with the discriminant equal to that of a quadratic number field, *J. Math. Soc. Japan* **47** (1995), no. 1, 31–36.

[8] B. Poonen and M. Stoll, Most odd degree hyperelliptic curves have only one rational point, *Ann. of Math.* (2) **180** (2014), no. 3, 1137–1166.

[9] A. Shankar, A. Södergren, and N. Templier, Sato-Tate equidistribution of certain families of Artin L-functions, `https://arxiv.org/abs/1507.07031`.

[10] A. Shankar and X. Wang, Average size of the 2-Selmer group for monic even hyperelliptic curves, `http://arxiv.org/abs/1307.3531`.

[11] K. Yamamura, On unramified Galois extensions of real quadratic number fields, *Osaka J. Math.* **23** (1986), no. 2, 471–478.

Fine scale statistics of binary quadratic forms

Valentin Blomer

(joint work with C. Aistleitner, M. Radziwiłł)

Let $Q_{\boldsymbol{\alpha}}(\mathbf{x}) = \alpha_1 x_1^2 + \alpha_2 x_1 x_2 + \alpha_3 x_3^2$ be a positive binary quadratic form with real coefficients $\alpha_1, \alpha_2, \alpha_3$. Substituting integer values $x_1 \in \mathbb{Z}$, $x_2 \in \mathbb{N}$ we consider the ordered sequence $0 \le \lambda_1 \le \lambda_2 \le \dots$ of its values. Up to scaling, this can be interpreted as the sequence of eigenvalues of the Laplacian on the corresponding torus. Weyl's law states $\#\{\lambda_j \le X\} \sim cX$ for some constant c, and by appropriate scaling we can assume that $c = 1$.

We are interested in the fine scale statistics of this sequence. The Berry-Tabor conjecture predicts that at least for "generic" coefficients $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$, the local statistical properties coincide with those of a sequence of points coming from a Poisson process.

In this direction, it was shown by Sarnak [Sa] that for almost all forms $Q_{\boldsymbol{\alpha}}$ (in a Lebesgue sense) the pair correlation is Poissonian:

$$\frac{1}{N}\#\{i, j \le N \mid \lambda_i - \lambda_j \in I\} \sim |I|, \quad N \to \infty,$$

for every fixed interval $I \subseteq \mathbb{R}$ of length $|I|$. Eskin, Margulis and Mozes [EMM] showed that this is the case for all non-diophantine forms. In [BBRR] the smallest

gap

$$\delta_{\min}(N) = \min_{j \le N}(\lambda_{j+1} - \lambda_j)$$

was considered, and it was shown that almost all forms satisfy $\delta_{\min}(N) \ll N^{\varepsilon-1}$ for every $\varepsilon > 0$ and all $N \ge 1$.

Here we are interested in the behaviour of the largest gap

$$\delta_{\max} = \limsup_{j\to\infty}(\lambda_{j+1} - \lambda_j).$$

It is not unreasonable to assume that $\delta_{\max} = \infty$, but even the statement $\delta_{\max} > 1$ does not seem to have been known. In this talk we report on the work [ABR] where the following two theorems are proved.

Theorem 1. *a) If $(\lambda_j)_j$ is any sequence of positive real numbers with mean spacing one and Poisson pair correlation, then $\delta_{\max} \ge 3/2$.*
b) There exists a sequence of positive real numbers with mean spacing one and Poisson pair correlation with $\delta_{\max} \le 2$.
c) For almost all quadratic forms, the ordered sequence of its values at integers satisfies $\delta_{\max} \ge 2.006$.

Remarks: 1) In view of [EMM], this implies that the ordered sequence $x^2+\sqrt{2}y^2$, $x \in \mathbb{Z}$, $y \in \mathbb{N}$, has infinitely many gaps that are at least 1.5 times as large as the average gap.
2) It is an interesting open problem as to what the smallest value of $\delta_{\max}$ is for a sequence of positive real numbers with mean spacing one and Poisson pair correlation. In view of the above, this value is in $[3/2, 2]$.
3) In order to prove c), we have to use something beyond pair correlation. This is the content of the following theorem.

Let

$$T_3(\boldsymbol{\alpha}, I, N) = \frac{1}{N}\#\Big\{(i,j,k) \le N \mid i,j,k \text{ pairwise distinct}, \lambda_i - \lambda_j, \lambda_i - \lambda_k \in I\Big\}$$

for an interval $I \subseteq \mathbb{R}$, $N \in \mathbb{N}$ and a triple of coefficients $\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$ where (λ_j) denotes the ordered sequence of $Q_{\boldsymbol{\alpha}}(\mathbf{x}) = \alpha_1 x_1^2 + \alpha_2 x_1 x_2 + \alpha_3 x_3^2$ as above.

Theorem 2. *Let D be a compact set in the space of coefficients $\boldsymbol{\alpha}$. Then we have*

$$\int_D T_3(\boldsymbol{\alpha}, I, N) d\mu(\boldsymbol{\alpha}) \sim |I|^2 \mu(D)$$

as $N \to \infty$, in particular

$$\liminf_{N\to\infty} T_3(\boldsymbol{\alpha}, I, N) \le |I|^2 \le \limsup_{N\to\infty} T_3(\boldsymbol{\alpha}, I, N)$$

for almost all forms $Q_{\boldsymbol{\alpha}}$.

The proof starts with Fourier analysis. This translates the question into a counting problem in a highly cuspidal region, for which an asymptotic formula is required. Depending on the size of the variables, various techniques are used including geometry of numbers, Poisson summation, and non-trivial bounds for Kloosterman sums. From this one derives part c) of the previous theorem by an

elaborate combinatorial optimization. The number 2.006 comes as an approximation for the real root of

$$35 - 18x - 9x^2 + (12x - 10)\sqrt{6x - 5} = 0.$$

It is an interesting problem if there exists a sequence whose pair and triple correlation is Poisson, but its gaps are bounded.

References

[ABR] C. Aistleitner, V. Blomer, M. Radziwiłł, Triple correlation and long gaps in the spectrum of flat tori, `arxiv:1809.07881`

[BBRR] V. Blomer, J. Bourgain, M. Radziwiłł, Z. Rudnick, Small gaps in the spectrum of the rectangular billiard, Ann. Sci. Ecole Norm. Sup. 50(2017), 1283-1300.

[EMM] A. Eskin, G. Margulis, S. Mozes, Quadratic forms of signature (2, 2) and eigenvalue spacings on rectangular 2-tori, Ann. of Math. (2)161(2005), 679-725.

[Sa] P. Sarnak, Values at integers of binary quadratic forms. Harmonic analysis and number theory (Montreal 1996), 181-203, CMS Conf. Proc. 21, Amer. Math. Soc., Providence, RI, 1997.

The Hasse principle for random Fano hypersurfaces

Tim Browning

(joint work with Pierre Le Boudec, Will Sawin)

Let $d, n \geq 2$ be such that $n \geq d$ and let $N_{d,n} = \binom{n+d}{n}$ be the number of monomials of degree d in $n+1$ variables. Ordering monomials lexicographically, degree d hypersurfaces in $\mathbb{P}^n$ that are defined over $\mathbb{Q}$ are parametrized by $\mathbb{V}_{d,n} = \mathbb{P}^{N_{d,n}-1}(\mathbb{Q})$. The assumption $n \geq d$ implies that a generic element of $\mathbb{V}_{d,n}$ is a smooth Fano hypersurface. We order elements of $\mathbb{V}_{d,n}$ using the usual exponential height on projective space, letting

$$\mathbb{V}_{d,n}(A) = \{V \in \mathbb{V}_{d,n} : ||\mathbf{a}_V|| \leq A\},$$

for $A \geq 1$, where $||\mathbf{a}_V||$ is the Euclidean norm of one of the two coefficient vectors $\mathbf{a}_V \in \mathbb{Z}^{N_{d,n}}_{\text{prim}}$ associated to V. The primary goal is to investigate the asymptotic behaviour of the quantity

$$\varrho_{d,n}(A) = \frac{\#\{V \in \mathbb{V}_{d,n}(A) : V(\mathbb{Q}) \neq \emptyset\}}{\#\mathbb{V}_{d,n}(A)},$$

as $A \to \infty$. This is the proportion of degree d hypersurfaces in $\mathbb{P}^n$ which are defined over $\mathbb{Q}$, have height at most A, and which admit a rational point.

For any $V \in \mathbb{V}_{d,n}$, let $V(\mathbf{A}_\mathbb{Q})$ denote the set of adèles of V. It is convenient to introduce the set

$$\mathbb{V}^{\text{loc}}_{d,n}(A) = \{V \in \mathbb{V}_{d,n}(A) : V(\mathbf{A}_\mathbb{Q}) \neq \emptyset\},$$

which is comprised of the elements of $\mathbb{V}_{d,n}(A)$ that are everywhere locally soluble. It follows from work of Poonen and Voloch [4, Theorem 3.6] that if $(d, n) \neq (2, 2)$

then the limit

$$\varrho_{d,n}^{\mathrm{loc}} = \lim_{A\to\infty} \frac{\#\mathbb{V}_{d,n}^{\mathrm{loc}}(A)}{\#\mathbb{V}_{d,n}(A)}$$

exists, is positive, and is equal to a product of local densities. Moreover, Poonen and Voloch [4, Conjecture 2.2(ii)] conjecture that $\varrho_{d,n}(A)$ tends to a limit as $A \to \infty$ and $\lim_{A\to\infty} \varrho_{d,n}(A) = \varrho_{d,n}^{\mathrm{loc}}$. Note that the case $d = 2$ holds unconditionally by the Hasse–Minkowski theorem. Poonen and Voloch prove [4, Proposition 3.4] that their prediction follows from the conjecture of Colliot-Thélène [3] that for smooth, proper, geometrically integral and rationally connected varieties, the Brauer–Manin obstruction to the Hasse principle is the only one.

If $n \geq 2^d(d-1)$ then the Poonen–Voloch prediction follows from Birch's work on forms in many variables [1]. In the special setting of diagonal hypersurfaces, Brüdern and Dietmann have confirmed in [2, Theorem 1.3] that the analogue of the Poonen–Voloch prediction holds under the assumption $n > 3d$. The following is our main result and only leaves open few cases in the Poonen–Voloch conjecture for Fano hypersurfaces.

Theorem 1. *Let $d \geq 3$. Assume that $n \geq d+1$ or $n = d \geq 7$. Then we have*

$$\lim_{A\to\infty} \varrho_{d,n}(A) = \varrho_{d,n}^{\mathrm{loc}}.$$

In other words, when degree d hypersurfaces in $\mathbb{P}^n$ which are defined over $\mathbb{Q}$ and are ordered by height, then 100% of these hypersurfaces satisfy the Hasse principle provided that $n \geq d+1$ or $n = d \geq 7$.

The proof of the theorem relies crucially upon arguments coming from the geometry of numbers together with a careful study of local densities. Associated to a Fano hypersurface $V \in \mathbb{V}_{d,n}$ is the anticanonical height function $H : V(\mathbb{Q}) \to \mathbb{R}_{>0}$ metrised by the Euclidean norm $||\cdot||$ on $\mathbb{R}^{n+1}$. Thus, for $x \in V(\mathbb{Q})$ we choose $\mathbf{x} = (x_0, \dots, x_n) \in \mathbb{Z}^{n+1}_{\mathrm{prim}}$ such that $x = (x_0 : \cdots : x_n)$ and we set $H(x) = ||\mathbf{x}||^{n+1-d}$. This allows us to define the counting function

$$N_V(B) = \#\{x \in V(\mathbb{Q}) : H(x) \leq B\}.$$

To tackle the theorem we will first show that $N_V(B)$ is well-approximated on average by a certain localised counting function, which we proceed to define now.

Of special importance in our work is the Veronese embedding $\nu_{d,n} : \mathbb{R}^{n+1} \to \mathbb{R}^{N_{d,n}}$, defined by listing all the monomials of degree d in $n+1$ variables using the lexicographical ordering. Next, let

$$\Xi_{d,n}(B) = \left\{\mathbf{x} \in \mathbb{Z}^{n+1}_{\mathrm{prim}} : ||\mathbf{x}|| \leq B^{1/(n+1-d)}\right\}.$$

The localised counting function we work with is chosen to mimic the expected main term in the expected asymptotic formula for $N_V(B)$. For any real $\alpha > 1$ and $\mathbf{v} \in \mathbb{R}^{N_{d,n}}$, we introduce the region

$$\mathcal{C}_\alpha(\mathbf{v}) = \left\{\mathbf{t} \in \mathbb{R}^{N_{d,n}} : |\langle \mathbf{v}, \mathbf{t}\rangle| \leq \frac{||\mathbf{v}|| \cdot ||\mathbf{t}||}{2\alpha}\right\},$$

where $\langle \cdot, \cdot \rangle$ denotes the usual Euclidean inner product. Moreover, for any positive integer W and $\mathbf{c} \in \mathbb{Z}^{N_{d,n}}$, we define the lattice

$$\Lambda_{\mathbf{c}}^{(W)} = \left\{ \mathbf{y} \in \mathbb{Z}^{N_{d,n}} : \langle \mathbf{c}, \mathbf{y} \rangle \equiv 0 \bmod W \right\}.$$

Our localised counting function is then defined as

$$N_V(B; \alpha, W) = \frac{1}{2} \frac{\alpha W}{||\mathbf{a}_V||} \sum_{\substack{\mathbf{x} \in \Xi_{d,n}(B) \\ \mathbf{a}_V \in \Lambda_{\nu_{d,n}(\mathbf{x})}^{(W)} \cap \mathcal{C}_\alpha(\nu_{d,n}(\mathbf{x}))}} \frac{1}{||\nu_{d,n}(\mathbf{x})||}.$$

As $\alpha, W \to \infty$ this sum approximates the product of the singular series and singular integral that appear in the circle method. By taking α and W to tend to infinity slowly with respect to B (with W highly divisible), we need to prove that the localised counting function $N_V(B; \alpha, W)$ is only rarely smaller than its expected value.

References

[1] B.J. Birch, Forms in many variables, Proc. Roy. Soc. Ser. A 265(1961/62), 245–263.

[2] J. Brüdern and R. Dietmann, Random diophantine equations, I, Advances Math. 256(2014), 18–45.

[3] J.-L. Colliot-Thélène. Points rationnels sur les fibrations, Higher dimensional varieties and rational points (Budapest, 2001), 171–221, Springer-Verlag, 2003.

[4] B. Poonen and J. F. Voloch, Random Diophantine equations, Arithmetic of higher dimensional algebraic varieties (Palo Alto,CA, 2002), 175–184, Progr. Math. 226, Birkhäuser, 2004.

Rado's criterion over squares and higher powers

Sam Chow

(joint work with Sofia Lindqvist, Sean Prendiville)

Schur's theorem [Sch1916] is a foundational result in Ramsey theory, asserting that for any finite colouring of the positive integers there exists a monochromatic solution to the equation $x + y = z$ (a solution in which each variable receives the same colour). A notorious question of Erdős and Graham asks if the same is true for the Pythagorean equation $x^2 + y^2 = z^2$, offering \$250 for an answer. The computer-aided verification [HKM16] of the two colour case of this problem is reported to be the largest mathematical proof in existence, consuming 200 terabytes [Lam16]. We provide an affirmative answer to the analogue of the Erdős–Graham question for generalised Pythagorean equations in five or more variables.

Theorem 1 (Schur-type theorem in the squares)**.** *In any finite colouring of the positive integers there exists a monochromatic solution to the equation*

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = x_5^2.$$

This is a consequence of a more general phenomenon. Given enough variables, we completely describe which diagonal forms have the above property and which do not.

Definition 1 (Partition regular)**.** *Given a polynomial $P \in \mathbb{Z}[x_1, \dots, x_s]$ and a set S, call the equation $P(x) = 0$* partition regular over S *if, in any finite colouring of S, there exists a solution $x \in S^s$ whose coordinates all receive the same colour. We say that the equation is* non-trivially partition regular *if every finite colouring of S has a monochromatic solution in which each variable is distinct.*

Rado [Rad33] established an elegant characterisation of partition regular homogeneous linear equations.

Rado's criterion for one equation. *Let $c_1, \dots, c_s \in \mathbb{Z} \setminus \{0\}$, where $s \geq 3$. Then the equation $\sum_{i=1}^{s} c_i x_i = 0$ is (non-trivially) partition regular over the positive integers if and only if there exists a non-empty set $I \subseteq \{1, 2, \dots, s\}$ such that $\sum_{i \in I} c_i = 0$.*

Several authors have sought similar characterisations of partition regularity within families of non-linear Diophantine equations. The example of the Fermat equation $x^k + y^k = z^k$ shows that one cannot hope for something as simple as Rado's criterion for diagonal forms. Nevertheless, provided that the number of variables is sufficiently large in terms of the degree, we establish that the same criterion characterises partition regularity for homogeneous diagonal equations.

Theorem 2 (Rado over kth powers)**.** *There exists $s_0(k) \in \mathbb{N}$ such that for $s \geq s_0(k)$ and $c_1, \dots, c_s \in \mathbb{Z} \setminus \{0\}$ the following holds. The equation*

$$\sum_{i=1}^{s} c_i x_i^k = 0 \tag{1}$$

is (non-trivially) partition regular over the positive integers if and only if there exists a non-empty set $I \subseteq \{1, 2, \dots, s\}$ such that $\sum_{i \in I} c_i = 0$. Moreover, we may take $s_0(2) = 5$, $s_0(3) = 8$ and

$$s_0(k) = k(\log k + \log\log k + 2 + O(\log\log k / \log k)). \tag{2}$$

Notice that Rado's criterion for a linear equation shows that the condition $\sum_{i \in I} c_i = 0$ is necessary for 1 to be partition regular. The content of Theorem 2 is that this condition is also sufficient.

For higher-degree equations one cannot avoid the assumption of some lower bound on the number of variables, as the example of the Fermat equation demonstrates. Given current knowledge on the solubility of diagonal Diophantine equations [Woo92], the bound 2 is at the cutting edge of present technology. Indeed, it is unlikely that one could improve this condition without making an analogous breakthrough in Waring's problem, since partition regularity implies the existence of a non-trivial integer solution to the equation 1.

When the coefficients of 1 sum to zero, partition regularity follows easily, since any element of the diagonal constitutes a monochromatic solution. However, there are results in the literature which also guarantee *non-trivial* partition regularity in this situation, provided that $s \geq k^2 + 1$. This was first established for quadrics in [BP17] and for general k in [Cho17]. In fact in [Cho17] it is established

that, under these assumptions, dense subsets of the *primes* contain many solutions to 1.

We believe that when the solution set of a given equation contains the diagonal it is more robust with respect to certain local issues—indeed one expects dense sets (such as congruence classes) to contain solutions under this assumption. As a consequence, the local issues for such equations are easier to handle using elementary devices, such as passing to a well-chosen subprogression. The novelty in our methods is that for general equations, instead of tackling the somewhat thorny local problem head on, we show how we may assume our colouring possesses a certain homogeneous structure, and this structure allows the same devices available in the dense regime to come into play.

Definition 2 (Homogeneous set)**.** *A set $B \subset \mathbb{N}$ is called* M-homogeneous *when for any $q \in \mathbb{N}$ we have*

$$B \cap q \cdot [M] \neq \emptyset. \tag{3}$$

We leave it as an exercise for the reader to verify that if B is an M-homogeneous set then $|B \cap [N]| \gg_M N$ for N sufficiently large in terms of M, so homogeneous sets are dense. In fact they are dense on all sufficiently long homogeneous arithmetic progressions. The following observation explains why Definition 2 is important.

Lemma 3. *A dilation-invariant system of equations is partition regular if it has a solution in every homogeneous set.*

This is proved by an induction on the number of colours: if the colour classes are not homogeneous then we can rescale the variables to eliminate a colour class. Chapman [Cha18] has since shown that the converse of Lemma 3 also holds.

Consider the example of the generalised Pythagorean equation,

$$x_1^2 + x_2^2 + x_3^2 = x_5^2 - x_4^2,$$

to which we wish to find a solution in homogeneous variables. Homogeneous variables are dense, so we can apply Green's Fourier-analytic transference principle [Gre05] to compare the number of solutions to that of

$$y_1^2 + y_2^2 + y_3^2 = n_1 - n_2, \tag{4}$$

after some changes of variables involving the W-trick (which massages the squares to make them well-distributed to small prime moduli). The latter requires the coefficients on the right hand side to sum to zero, as we have carefully arranged. This simpler equation 4 is controlled by Fourier analysis, c.f. Sarközy's theorem, but in general we invoke the multidimensional polynomial Szemerédi theorem of Bergelson and Leibman [BL96].

References

[BL96] V. Bergelson and A. Leibman, Polynomial extensions of van der Waerden's and Szemerédi's theorems, J. Amer. Math. Soc. **9** (1996), no. 3, 725–753.

[BP17] T. D. Browning and S. Prendiville, A transference approach to a Roth-type theorem in the squares, IMRN **7** (2017), 2219–2248.

[Cha18] J. Chapman, Partition regularity and multiplicatively syndetic sets, preprint (2019) `arXiv:1902.01149`.

[Cho17] S. Chow, Roth–Waring–Goldbach, IMRN (2017), 34 pp.

[Gre05] B. Green, Roth's theorem in the primes, Ann. of Math. **161** (2005), 1609–1636.

[HKM16] M. Heule, O. Kullmann & V. Marek, Solving and verifying the Boolean Pythagorean triples problem via cube-and-conquer, Theory and applications of satisfiability testing – SAT 2016: 19th International Conference, Bordeaux, France, July 5-8, 2016, Proceedings (2016), Springer, 228–245.

[Lam16] E. Lamb, Maths proof smashes size record, Nature **534** (2016), 17–18.

[Rad33] R. Rado, Studien zur Kombinatorik, Math. Z. **36** (1933), 242–280.

[Sch1916] I. Schur, Über die Kongruenz $x^m + y^m \equiv z^m \pmod p$, Jahresber. Dtsch. Math.-Ver. **25** (1916), 114–117.

[Woo92] T. D. Wooley, Large improvements in Waring's problem, Ann. of Math. (2) **135** (1992), 131–164.

Averages of quadratic twists of long Dirichlet polynomials

Brian Conrey

(joint work with Brad Rogers)

This report is about some progress on understanding higher moments of families of L-functions. In [CFKRS] is described a "recipe" which can be applied to families of L-functions and conjecturally gives all of the main terms in and moment of this family. In describing the conjecture of that paper it is convenient to give a formula for averages of products of L-functions with small shifts. One example of the recipe is for shifted moments of the Riemann zeta on the critical line.

Conjecture 1. *(CFKRS) Let A and B be sets of complex numbers with $|\Re\alpha| \ll (\log T)^{-1}, |\Im\alpha| \ll T$ for all $\alpha \in A$ with similar inequalities for the $\beta \in B$; let ψ be a smooth function supported on $[1,2]$. Then there is a $\delta > 0$ such that*

$$\int_0^\infty \psi\left(\frac{t}{T}\right) \prod_{\substack{\alpha\in A\\ \beta\in B}} \zeta(s+\alpha)\zeta(1-s+\beta)\, dt$$

$$= \int_0^\infty \psi\left(\frac{t}{T}\right) \sum_{\substack{U\subset A\\ V\subset B\\ |U|=|V|}} \left(\frac{t}{2\pi}\right)^{-U-V} \mathcal{B}(A-U+V^-, B-V+U^-)\, dt$$

$$+O(T^{1-\delta}).$$

as $T \to \infty$ where

$$\mathcal{B}(A,B) = \sum_{n=1}^\infty \frac{\tau_A(n)\tau_B(n)}{n}$$

(or the analytic continuation of that sum) with

$$\prod_{\alpha\in A}\zeta(s+\alpha)=\sum_{n=1}^{\infty}\frac{\tau_A(n)}{n^s}$$

Also, the notation $A-U+V^-$ means the set A with the elements in the subset U removed and the negatives of the elements of V inserted.

In the formula above the terms with $|U|=|V|=\ell$ are referred to as the "ℓ-swap" terms. If $A|=|B|=k$ then the number of ℓ-swap terms is $\binom{k}{\ell}^2$. Note that (in the case $|A|=|B|=k$) there are a total of k^2 singularities of $\mathcal{B}(A,B)$ (which occur when $\alpha+\beta=0$). So, each of the $\binom{2k}{k}$ terms of the recipe has k^2 singularities; however the sum of all of these expressions is analytic in the α and β. When one allows all of the shifts α and β to go to 0, one obtains a formula for the $2k$th moment of the zeta-function on the critical line in the form of T times a polynomial of degree k^2 in $\log\frac{T}{2\pi}$.

In a series of papers (see [CK5]) Conrey and Keating outlined an approach to understanding this conjecture from a classical analytic number theoretic perspective. They considered the average of a long polynomial

$$\int_0^{\infty}\psi\left(\frac{t}{T}\right)\sum_{m,n\le X}\frac{\tau_A(m)\tau_B(n)}{m^{1/2+it}n^{1/2-it}}\,dt$$

where $X=T^{\eta}$. Integrating term-by-term one finds the above is

$$T\sum_{m,n\le X}\frac{\tau_A(m)\tau_B(n)\hat{\psi}\left(\frac{T}{2\pi}\log\frac{m}{n}\right)}{\sqrt{mn}}$$

The diagonal $m=n$ corresponds to the 0-swap terms in the recipe. If $0<\eta<1$ these are the only terms that occur. If $1<\eta<2$ then we sort the $m\neq n$ terms by writing $n=m+h$. We can then input conjectural information abut the coefficient correlations

$$\sum_{n\le u}\tau_A(m)\tau_B(m+h)$$

gleaned from the delta-method. In this way we obtain the one-swap terms from the recipe. When $2<\eta<3$ we expect the two-swap terms to arise, but from where? It turns out that if we partition $A=A_1\cup A_2$ and $B=B_1\cup B_2$ and introduce parameters M and N we are led to consider

$$\int_0^{\infty}\psi\left(\frac{t}{T}\right)\sum_{\substack{m_1m_2\le X\\ n_1n_2\le X}}\frac{\tau_{A_1}(m_1)\tau_{B_1}(n_1)}{\sqrt{m_1n_1}}\frac{\tau_{A_2}(m_2)\tau_{B_2}(n_2)}{\sqrt{m_2n_2}}\left(\frac{m_1Mm_2N}{n_1Nn_2M}\right)^{it}\,dt$$

We estimate the m_1,n_1 sum by the "twisted" delta-method and similarly for the sum over m_2 and n_2. When we sum over the (co-prime) parameters M and N and all the possible partitions of A and B (suitably weighted) we obtain the two-swap terms. This process can be iterated to give all of the higher swap terms in the recipe.

The analog for moments of quadratic L-functions is the subject of this report. Let $\mathcal{D}$ be the collection of fundamental discriminants and for each $d \in \mathcal{D}$ let χ_d be the character given by the Kronecker symbol $\chi_d(n) = \binom{d}{n}$. The recipe predicts that up to a $O(D^{1-\delta})$ we have

$$\sum_{d\in\mathcal{D}} \psi\left(\frac{d}{D}\right) \prod_{\alpha\in A} L(1/2+\alpha,\chi_d) = \sum_{d\in\mathcal{D}} \psi\left(\frac{d}{D}\right) \sum_{U\subset A} \prod_{u\in U} X_d(1/2+u)\mathcal{B}^{(d)}(A-U+U^-)$$

where

$$\mathcal{B}^{(d)}(A) = \sum_{\substack{(n,d)=1\\ n=\square}} \frac{\tau_A(n)}{\sqrt{n}}$$

and where $X_d(s)$ is the factor in the functional equation for $L(s,\chi_d)$. One can consider the long polynomial version of this, for which the recipe predicts

Conjecture 2.

$$\sum_{d\in\mathcal{D}} \psi\left(\frac{d}{D}\right) \sum_{n\le X} \frac{\tau_A(n)\chi_d(n)}{\sqrt{n}} = \sum_{d\in\mathcal{D}} \psi\left(\frac{d}{D}\right) \frac{1}{2\pi i}\int_{1-ID}^{1+iD} \frac{X^s}{s} \sum_{\substack{U\subset A_s\\ |U|<\eta}} \prod_{u\in U} X_d(1/2+u)\mathcal{B}^{(d)}(A_s-U+U^-)\,ds + O(D^{1-\delta})$$

where A_s denotes the set $\{\alpha+s : \alpha\in A\}$.

In work in preparation Conrey and Brad Rodgers have proven that, assuming the Lindelöf Hypothesis, this conjecture is true for $\eta < 2$ and arbitrary sets A with $|\Re\alpha| \ll (\log D)^{-1}$ and $|\Im\alpha| \ll D$ The proof relies on Soundararajan's Poisson summation formula (see [Sou]) for $\sum_{d\in\mathcal{D}} \psi\left(\frac{d}{D}\right)\chi_d(n)$.

If $2 < \eta < 3$ then we believe that one should split the set A into two sets $A = A_1 \cup A_2$ and introduce a squarefree parameter M and consider

$$\sum_{d\in\mathcal{D}} \psi\left(\frac{d}{D}\right) \sum_{mn\le X} \frac{\tau_{A_1}(m)\chi_d(mM)}{\sqrt{m}} \frac{\tau_{A_2}(n)\chi_d(nM)}{\sqrt{n}}.$$

Now one has the result, conditional on the Lindelöf Hypothesis, that

$$\sum_{d\in\mathcal{D}} \psi\left(\frac{d}{D}\right) \sum_{n\le X} \frac{\tau_A(n)\chi_d(nM)}{\sqrt{n}} = \sum_{d\in\mathcal{D}} \psi\left(\frac{d}{D}\right) \frac{1}{2\pi i}\int_{1-ID}^{1+iD} \frac{X^s}{s} \sum_{\substack{U\subset A_s\\ |U|<\eta}} \prod_{u\in U} X_d(1/2+u)\mathcal{B}_M^{(d)}(A_s-U+U^-)\,ds$$

$+O(M^{1/2}XD^{\epsilon})$ where

$$\mathcal{B}_M^{(d)}(A) = \sum_{\substack{(n,d)=1\\ nM=\square}} \frac{\tau_A(n)}{\sqrt{n}}.$$

If one averages over M then the dependence is $\ll M^{\epsilon}$ on average. The above formula can be interpreted as saying that

$$\frac{\tau_A(n)\chi_d(nM)}{\sqrt{n}}\Big|_{n=v}$$

is on average approximated by

$$\frac{1}{2\pi i}\int_{(c)} v^{s-1} \sum_{\substack{U\subset A_s\\ |U|<\eta}} \prod_{u\in U} X_d(1/2+u)\mathcal{B}_M^{(d)}(A_s - U + U^-)\, ds.$$

If we replace the m term and the n-term by this approximation, and use the identity

$$\mathcal{B}^{(d)}(A) = \sum_{M_1\dots M_\ell=\square} \prod_{j=1}^{\ell} \mu^2(M_j)\mathcal{B}_{M_j}^{(d)}(A_j),$$

then in the case $\ell = 2$ we heuristically recover the two-swap terms from the recipe. In general, all of the terms of the recipe show up in a similar way.

Finally, we note that back in the zeta-function case there is also an identity that governs the general picture. With the functions

$$\mathcal{B}(A,B) := \sum_{m=n} \frac{\tau_A(m)\tau_B(n)}{\sqrt{mn}}$$

and

$$\mathcal{B}_{M,N}(A,B) := \sum_{Mm=nN} \frac{\tau_A(m)\tau_B(n)}{\sqrt{mn}},$$

the relevant identity is

$$\mathcal{B}(A,B) = \sum_{\substack{M_1\dots M_\ell=N_1\dots N_\ell\\ (M_j,N_j)=1}} \prod_{j=1}^{\ell} \mathcal{B}_{M_j,N_j}(A,B).$$

References

[CFKRS] J.B. Conrey, D.W. Farmer, J.P. Keating, M.O. Rubinstein and N.C. Snaith. Integral moments of L-functions. Proc. Lond. Math. Soc. 91 (2005) 33–104.

[CK5] Brian Conrey, Jonathan Keating. Moments of zeta and correlations of divisor-sums: V. Proc. Lond. Math. Soc. (3) 118 (2019), no. 4, 729–752.

[Sou] K. Soundararajan. Nonvanishing of quadratic Dirichlet L-functions at s=1/2. Ann. of Math. (2) 152 (2000), no. 2, 447–488.

The mean values of cubic L–functions over function fields

Alexandra Florea
(joint work with Chantal David, Matilde Lalin)

The problem we consider is that of computing the mean value of Dirichlet L–functions $L_q(s,\chi)$ evaluated at the critical point $s=1/2$, as χ varies over the primitive cubic Dirichlet characters of $\mathbb{F}_q[T]$. We solve this problem in two different settings: when the base field $\mathbb{F}_q$ contains the cubic roots of unity (or equivalently when $q\equiv 1 \pmod 3$; we call this the Kummer setting) and when $\mathbb{F}_q$ does not contain the cubic roots of unity (when $q\equiv 2 \pmod 3$; we call this the non-Kummer setting.)

We will count primitive cubic characters ordering them by the degree of their conductor, or equivalently by the genus g of the cyclic cubic field extension of $\mathbb{F}_q[T]$ associated to such a character.

We compute the first moment of cubic L–functions for the two settings. In the non-Kummer case, we have the following.

Theorem 1. *Let q be an odd prime power such that $q\equiv 2 \pmod 3$. Then*

$$\sum_{\substack{\chi \text{ primitive cubic}\\ \text{genus}(\chi)=g}} L_q(1/2,\chi)=\frac{\zeta_q(3/2)}{\zeta_q(3)}\mathcal{A}_{\mathrm{nK}}q^{g+2}+O(q^{\frac{7g}{8}+\varepsilon g}),$$

with $\mathcal{A}_{\mathrm{nK}}$ an explicit constant.

In the Kummer case, we prove the following.

Theorem 2. *Let q be an odd prime power such that $q\equiv 1 \pmod 3$. Then,*

$$\sum_{\substack{\chi \text{ primitive cubic}\\ \text{genus}(\chi)=g}} L_q(1/2,\chi)=C_{\mathrm{K},1}gq^{g+1}+C_{\mathrm{K},2}q^{g+1}+O\left(q^{g\frac{1+\sqrt{7}}{4}+\varepsilon g}\right),$$

where $C_{\mathrm{K},1}$ and $C_{\mathrm{K},2}$ are explicit constants.

Since L-functions satisfy the Lindelöf hypothesis over function fields, one can easily bound the second moment, and we get the following corollary.

Corollary 3. *Let q be an odd prime power. Then,*

$$\#\{\chi \text{ cubic, primitive of genus } g \,:\, L_q(1/2,\chi)\neq 0\}\gg q^{(1-\varepsilon)g}.$$

I also reported on joint work in progress on obtaining a positive proportion of non-vanishing for the family of cubic L–functions. Proving such a result relies on obtaining sharp upper bounds for mollified moments of cubic L–functions, with a suitable choice of a mollifier.

The first step in the proof of the two theorems above is using the approximate functional equation to write the special value $L_q(1/2,\chi)$ as a sum of two terms, the principal sum and the dual sum. We obtain asymptotic formulas for the principal sum and the dual sum and we exhibit some explicit cancellation between the two terms. Computing the dual sum relies on evaluating averages of cubic Gauss sums

over function fields. Cubic Gauss sums are not multiplicative, so their generating series does not possess an Euler product. To deal with these averages, we rely on the theory of metaplectic Eisenstein series and then explicitly compute the residue of the pole of the generating series.

The level of distribution of unbalanced convolutions

Étienne Fouvry
(joint work with Maksym Radziwiłł)

Let (α_m) and (β_n) be two sequences of real numbers such that $|\alpha_m| \leq 1$ and $|\beta_n| \leq 1$. We suppose that (β_n) satisfies the following Siegel–Walfisz type condition of order K (where $K \geq 1$ is a given integer and τ_K is the divisor function of order K) : for every $A > 0$, we have the equality

$$\sum_{\substack{n \leq N \\ n \equiv a \bmod q \\ (n,d)=1}} \beta_n = \frac{1}{\varphi(q)} \sum_{\substack{n \leq N \\ (n,dq)=1}} \beta_n + O_A\big(\tau_K(d) N (\log 2N)^{-A}\big),$$

uniformly for $N \geq 1$, for integers a, $d \geq 1$ and $q \geq 1$ satisfying $(a, q) = 1$. To state the theorems, we introduce the notations $x := MN$ and $\mathcal{L} := \log 2x$. By $n \sim N$ we mean that n satisfies the inequalities $N < n \leq 2N$. We have [6, Corollary 1.1*(i)*]

Theorem 1. *Let (α_m) and (β_n) be two sequences as above and let $\varepsilon > 0$. Then for every $A > 0$, we have*

$$\sum_{\substack{q \sim Q \\ (q,a)=1}} \Big| \sum_{\substack{m \sim M \\ mn \equiv a \bmod q}} \sum_{n \sim N} \alpha_m \beta_n - \frac{1}{\varphi(q)} \sum_{\substack{m \sim M \\ (mn,q)=1}} \sum_{n \sim N} \alpha_m \beta_n \Big| = O_A(x \mathcal{L}^{-A}), \tag{1}$$

uniformly for

$$1 \leq |a| \leq x/12 \text{ and } \exp\big(\mathcal{L}^{\varepsilon}\big) \leq N \leq x^{17/36-\varepsilon} Q^{-11/12}. \tag{2}$$

A classical consequence of the large sieve inequality implies that, for some function $B(A)$, the equality (1) is true for

$$Q \leq x^{1/2} \mathcal{L}^{-B(A)} \text{ and } \exp\big(\mathcal{L}^{\varepsilon}\big) \leq N \leq x \exp\big(-\mathcal{L}^{\varepsilon}\big), \tag{3}$$

uniformly for $a \neq 0$ (see for instance [2, Theorem 0 (b)]). It is a challenging problem to increase the value of the exponent $1/2$ in the above bound for Q appearing in (3). The first and unique results of that type where obtained by Fouvry [5, Théorème 1] and Bombieri, Friedlander and Iwaniec [2, Theorem 3] who proved that (1) holds uniformly for

$$Q \leq \min(x^{1/2} N^{1/2}, x^{5/8} N^{-3/4})\, x^{-\varepsilon},\ N > x^{\varepsilon} \text{ and } 1 \leq |a| \leq \mathcal{L}^{A}. \tag{4}$$

The conditions (4) show that (1) is true for $Q = x^{1/2+\delta}$ (where δ is a small positive constant) as soon as we have $x^{2\delta-\varepsilon} \leq N \leq x^{1/6-4\delta/3-\varepsilon}$, which means that

N cannot be tiny. On the other hand, the new conditions (2) show that N can be very tiny ($\exp((\log x)^{\varepsilon}) \le N \le x^{1/72-11\delta/12-\varepsilon}$) to obtain the value $1/2+\delta$ for the exponent of distribution of the convolution $(\alpha_m) * (\beta_n)$.

All the applications of Theorem 1 benefit from the size of a tiny variable in the convolution that we meet and they mainly deal with the average distribution of multiplicative functions. It is interesting to compare these applications with the recent works of Green [9] and Granville and Shao [8]. Let us only mention the following

Corollary 2. *Fix an integer $k \ge 1$ and $\varepsilon > 0$. Then uniformly for $x \ge 2$, $Q \le x^{17/33-\varepsilon}$ and $1 \le |a| \le x/12$ one has the inequality*

$$\sum_{\substack{q\sim Q\\(q,a)=1}} \Big| \sum_{\substack{n\sim x\\ n\equiv a \bmod q}} \tau_k(n) - \frac{1}{\varphi(q)} \sum_{\substack{n\sim x\\(n,q)=1}} \tau_k(n)\Big| = O_{\varepsilon}\Big(\frac{x}{\mathcal{L}^{1-\varepsilon}}\Big). \tag{5}$$

The trivial bound for the sum studied in (5) is $O(x\mathcal{L}^{k-1})$.

The proof of Theorem 1 is based on Linnik's dispersion method and it has many similarities with [2] and [5]. But instead of using bounds for sums of Kloosterman sums (see [3, Theorems 10 & 12]), we directly appeal to bounds of so–called Kloosterman fractions, which means trilinear sums of the shape

$$\sum_{a\sim A} \sum_{b\sim B} \sum_{\substack{c\sim C\\(c,b)=1}} \exp\Big(2\pi i \frac{a\overline{b}}{c}\Big),$$

where $\overline{b}$ is the multiplicative inverse of b mod c, and where $\alpha(a)$, $\beta(b)$ and $\gamma(c)$ are general coefficients. These bounds are based on the amplification method initiated in [4] and improved in [1].

By the same bound for Kloosterman fractions and a variation in the application of the dispersion method we prove the following [7, Theorem 1]

Theorem 3. *The statement of Theorem 1 remains true if the inequalities* (2) *are replaced by the inequalities*

$$1 \le |a| \le x \text{ and } Qx^{\varepsilon} \le N \le x^{17/56-\varepsilon}Q^{23/56}.$$

Hence, the equality (1) is true for $Q = x^{1/2+\delta}$, with δ a small positive constant as soon as N is slightly larger than $x^{1/2}$, more precisely when N satisfies the inequalities

$$x^{1/2+\delta+\varepsilon} < N < x^{1/2+1/112-23\delta/56-\varepsilon}.$$

Apparently Theorem 3 has less applications than Theorem 1. This is a consequence of the large size of N which allows less flexibility in the combinatorics of the arithmetical functions we would like to study.

References

[1] S. Bettin and V. Chandee, *Trilinear forms with Kloosterman fractions*, Adv. Math. **328** (2018), 1234–1262.
[2] E. Bombieri, J.B. Friedlander and H. Iwaniec, Primes in arithmetic progressions to large moduli, Acta Math. **156** (1986), no 3–4, 203–251.
[3] J.–M. Deshouillers and H. Iwaniec, Kloosterman sums and Fourier coefficients of cusp forms, Invent. Math. **70** (1982/83), no 2, 219–288.
[4] W. Duke, J. Friedlander and H. Iwaniec, Bilinear forms with Kloosterman fractions, Invent. Math. **128** (1997), no 1, 23–43.
[5] É. Fouvry, Autour du théorème de Bombieri–Vinogradov, Acta Math. **152** (1984), no 3–4, 219–234.
[6] É. Fouvry and M. Radziwiłł, Level of distribution of unbalanced convolutions, (submitted), arXiv:1811.08672.
[7] É. Fouvry and M. Radziwiłł, Another application of Linnik's dispersion method, Chebyshevskiĭ Sb. **19** (2018), no 3, 148–163.
[8] A. Granville and X. Shao, Bombieri-Vinogradov for multiplicative functions, and beyond the $x^{1/2}$-barrier, Adv. Math. **350** (2019), 304–358.
[9] B. Green, A note on multiplicative functions on progressions to large moduli, Proc. Roy. Soc. Edinburgh Sect. A **148** (2018), no 1, 63–77.

Arbitrarily long gaps between sums of powers

Luca Ghidelli

Let $s \in \mathbb{N}_+$ and let $F(\mathbf{x}) = a_1x_1^s + \cdots + a_sx_s^s$ be a diagonal form of degree s in s variables with positive integer coefficients $a_1, \ldots, a_s \in \mathbb{N}_+$. By *values of* $F(\mathbf{x})$ we mean the natural numbers obtained by evaluating the diagonal form at nonnegative integers $x_1, \ldots, x_s \in \mathbb{N}$. A *gap* of length K between these values is a sequence of consecutive nonnegative integers $n+1, \ldots, n+K$ that are not values of $F(\mathbf{x})$. When $s = 2$ the polynomial $F(\mathbf{x})$ is a multiple of a norm form and so the values of $F(\mathbf{x})$ form a set with natural density 0 in $\mathbb{N}$ (see Landau [7] for the prototypical case $F(\mathbf{x}) = x_1^2 + x_2^2$ and Odoni [8] for general norm forms). In particular if $s = 2$ there are arbitrarily long gaps between the values of $F(\mathbf{x})$. When $s \geq 3$ the polynomial $F(\mathbf{x})$ is irreducible over $\mathbb{C}$ and so it is not a norm form. In fact very little is known unconditionally about the distribution of the values of $F(\mathbf{x})$ if $s \geq 3$ (see [6] for some results conditional on GRH) but it is reasonable to expect, on the basis of probabilistic models [3] [4], that the set of values of $F(\mathbf{x})$ has positive density. Nevertheless, we may ask if there are arbitrarily long gaps between the values of $F(\mathbf{x})$, when $s \geq 3$. Here we give a positive answer in two cases. First, for all trinomial positive-definite cubic diagonal forms:

Theorem 1. *Let $F(\mathbf{x})$ be as above, with $s = 3$. Then there is a constant $\kappa_{F(\mathbf{x})} > 0$ such that for all integers N, K satisfying $N > e^e$, $K \geq 2$ and $K < \kappa_{F(\mathbf{x})} \frac{\sqrt{\log N}}{(\log\log N)^2}$ there exist gaps of length K between the values of $F(\mathbf{x})$ less than N.*

Second, for almost all quadrinomial positive-definite biquadratic diagonal forms:

Theorem 2. *Let $F(\mathbf{x})$ be as above, with $s = 4$, and suppose that $F(\mathbf{x})$ is not equal to $a(c_1x_1)^4 + b(c_2x_2)^4 + 4a(c_3x_3)^4 + 4b(c_4x_4)^4$, for some $a, b, c_1, c_2, c_3, c_4 \in \mathbb{N}_+$, up*

to a permutation of the variables. Then there is a constant $\kappa_{F(\mathbf{x})} > 0$ *such that for all integers* N, K *satisfying* $N > e^{e^{e^e}}$, $K \geq 2$ *and* $K < \kappa_{F(\mathbf{x})} \frac{\log\log\log N}{\log\log\log\log N}$ *there are gaps of length at least* K *between the values of* $F(\mathbf{x})$ *less than* N.

We are also able to show more precisely that, for a suitable $\kappa_F > 0$ and the same hypotheses, there exist at least $c(F,K)N$ gaps of length K between the values of $F(\mathbf{x})$ less than N, where $c(F,K) > 0$ is independent of N.

The above theorems include the important special cases $F(\mathbf{x}) = x_1^3+x_2^3+x_3^3$ and $F(\mathbf{x}) = x_1^4+x_2^4+x_3^4+x_4^4$. The values of these forms are often studied in connection with Waring's problem [10], which more generally concerns the representability of natural numbers as sums of perfect powers. Moreover, the results of the present paper concerning these two special cases have been used in a crucial way to improve some results of Bradshaw [1] in regard to values of cubic and biquadratic theta series [5].

On the other hand 2 doesn't apply to some biquadratic forms such as $F(\mathbf{x}) = x_1^4 + x_2^4 + 4x_3^4 + 4x_4^4$. We show that these exceptions are characterized among all biquadratic diagonal forms by a local property.

We now compare the above results with the literature. When $s = 2$ Richards [9] proved, with an ingenious elementary proof, that there are gaps of length at least $\gamma_F \log N$ between the values of $F(\mathbf{x})$, for some constant $\gamma_F > 0$. It is an important open-problem to estimate sharply the order of growth of the gaps between the values of $F(\mathbf{x}) = x_1^2 + x_2^2$. However when $s \geq 3$ our knowledge is even weaker. For example, if $F(\mathbf{x}) = x_1^3 + x_2^3 + x_3^3$ we only know by an elementary greedy argument [2] that for N large enough there are no gaps of size greater than $3^{19/9}N^{8/27}(1 + o(1))$, among the values of $F(\mathbf{x})$ less than N. On the other hand, working out the predictions of the probabilistic models, we should expect the existence of gaps of length as large as $O(\log N/\log\log N)$, for all $s \geq 3$.

In the following section we expose our strategy towards the proofs of 1 and 2. As it will be clear, the same method can be used to prove the existence of arbitrarily long gaps between the values of other polynomials, provided they satisfy a certain local property. Following a suggestion of Wooley, we are going to treat in a future publication the case of non-homogeneous diagonal forms such as $x_1^2+x_2^3+x_3^7+x_4^{42}$.

References

[1] Bradshaw, R., Arithmetic properties of values of lacunary series, Master's Thesis, University of Ottawa, 2013.

[2] Daniel, Stephan, On gaps between numbers that are sums of three cubes, Mathematika 44(1997), 1–13.

[3] Deshouillers, J.M., Hennecart, F. and Landreau, B., Sums of powers: an arithmetic refinement to the probabilistic model of Erdös and Rényi, Acta Arithmetica 85(1998), 13–33.

[4] Deshouillers, Jean-Marc, Hennecart, François and Landreau, Bernard, On the density of sums of three cubes, Algorithmic number theory, Lecture Notes in Comput. Sci. 4076(2006), 141–155.

[5] Ghidelli, Luca, Arithmetic properties of cubic and biquadratic theta series, Preprint, 2019.

[6] Hooley, C., On Hypothesis K^* in Waring's problem, Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995), London Math. Soc. Lecture Note Ser. 237, 175–185, Cambridge Univ. Press, Cambridge.
[7] Landau, Edmund, Über die Einteilung der positiven ganzen Zahlen in vier Klassen nach der Mindestzahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate, Archiv der Mathematik und Physik, 13(1908), 305–312.
[8] Odoni, R.W.K., The Farey density of norm subgroups in global fields (I), Mathematika 20(1973), 155–169.
[9] Richards, Ian, On the gaps between numbers which are sums of two squares, Advances in Mathematics 46(1982), 1–2.
[10] Vaughan, Robert C. and Wooley, Trevor D., Waring's problem: a survey, in Number theory for the millennium 3(2002), 301–340.

Propinquity of divisors

Ben Green
(joint work with Dimitris Koukoulopoulos, Kevin Ford)

Let n be a "typical" integer (say selected at random from $[1, X]$, for large X). What do the divisors of n look like? We will be interested in the particular question of how concentrated they are.

Define the Erdős–Hooley Δ-function

$$\Delta(n) := \max_i \#\{d|n : e^i \leq d \leq e^{i+1}\}.$$

How big do we expect this to be, for almost all n? Trivially $\Delta(n) \geq 1$, but nothing else is obvious. In 1985, resolving a conjecture of Erdős from 1948, Maier and Tenenbaum showed that $\Delta(n) \geq 2$ a.s. In fact, they obtained the stronger bound

$$\Delta(n) \gg (\log\log n)^{c_1+o(1)}$$

a.s., where

$$c_1 = -\log 2/\log(1 - \frac{1}{\log 3}) \approx 0.288.$$

In 2009, with a much more elaborate argument, they improved this to

$$\Delta(n) \gg (\log\log n)^{c_2+o(1)},$$

where

$$c_2 = \frac{\log 2}{\log\left(\frac{1-1/\log 27}{1-1/\log 3}\right)} \approx 0.338.$$

They conjectured that this is optimal.

Our main result is a disproof of this:

Theorem 1. *We have*

$$\Delta(n) \gg (\log\log n)^{c_3+o(1)},$$

where $c_3 = \eta \approx 0.353$.

Moreover, we conjecture, backed up by quite a bit of evidence, that *this* is optimal – therefore we had better say exactly what this η is. It is given by

$$\eta = \frac{\log 2}{\log(2/\rho)},$$

where $\rho \approx 0.281$ is given in terms of a rather complicated recurrence, as follows:

This ρ satisfies the equation

$$\frac{1}{1-\rho/2} = \log 2 + \sum_{j=1}^{\infty} \frac{1}{2^j} \log\Big(\frac{a_{j+1}+a_j^\rho}{a_{j+1}-a_j^\rho}\Big),$$

where the sequence a_j is defined by

$$a_1 = 2, \quad a_2 = 2+2^\rho, \quad a_j = a_{j-1}^2 + a_{j-1}^\rho - a_{j-2}^{2\rho} \qquad (j \ge 3).$$

We now discuss some key ideas from this work. The first key idea is to introduce a random model for the problem. This is the notion of a *logarithmic random set* $\mathbf{A}$. This is a subset of $\mathbb{N}$ in which we select i to lie in $\mathbf{A}$ with probability $1/i$, these choices being independent. A well-known principle (the Turán–Kubilius model) states that the prime factors of a random (squarefree) integer $n \le X$ behave somewhat like $\mathbf{A} \cap [1,\dots,D]$, $D = \log X$, at least away from the edges. Correspondingly, log the divisors of $n \le X$ should behave like the sums of elements of $\mathbf{A}$ in $[1,\dots,D]$. This suggests the following

Model problem. Let $r_{\mathbf{A}}(x)$ be the number of ways of writing x as a sum of elements of $\mathbf{A}$. What is $\max_x r_{\mathbf{A}}(x)$?

We have not studied precisely this problem, but rather the following kind of truncated version of it.

Truncated model problem. Determine β_k, the supremum of all exponents $c < 1$ for which the following is true, a.s. as $D \to \infty$: there is some x representable in k different ways as a sum of elements of $\mathbf{A} \cap [D^c, D]$.

The connection between this and the Hooley Δ-function is the following:

Lemma 2. *For any k, we have*

$$\Delta(n) \gg (\log\log n)^{\log k/\log(1/\beta_k)-o(1)}$$

a.s.

Our main theorem is then a consequence of the following statement about the β_k:

Proposition 3. *We have*

$$\limsup_{k\to\infty} \frac{\log k}{\log(1/\beta_k)} \ge \eta.$$

An apparently completely different problem. One of the main ideas of our paper is that β_k (essentially) coincides with the answer to what appears to be a completely different problem, to do with optimizing measures over the cube $\{0,1\}^k$. Even stating this problem requires some work.

Definition 1 (Flags and subflags)**.** *Let $k \in \mathbb{N}$. By an r-step* flag *we mean a nested sequence*

$$\mathcal{V} : \langle \mathbf{1} \rangle = V_0 \leq V_1 \leq V_2 \leq \cdots \leq V_r \leq \mathbb{Q}^k$$

of vector spaces. Here $\mathbf{1} = (1, 1, \ldots, 1) \in \mathbb{Q}^k$. Another flag

$$\mathcal{V}' : \langle \mathbf{1} \rangle = V_0' \leq V_1' \leq V_2' \leq \cdots \leq V_r' \leq \mathbb{Q}^k$$

is said to be a subflag *of $\mathcal{V}$ if $V_i' \leq V_i$ for all i. In this case we write $\mathcal{V}' \leq \mathcal{V}$. It is a* proper subflag *if it is not equal to $\mathcal{V}$.*

Definition 2 (Entropy of a subspace)**.** *Suppose that ν is a finitely supported probability measure on $\mathbb{Q}^k$ and that $W \leq \mathbb{Q}^k$ is a vector subspace. Then we define*

$$\mathbb{H}_\nu(W) := -\sum_x \nu(x) \log \nu(W + x).$$

Remark that this is the (Shannon) entropy of the distribution on cosets $W + x$ induced by ν.

Optimisation problem. Define γ_k to be the supremum of all constants c_{r+1} such that the following exist:

(1) An r-step flag $\mathcal{V}$ whose members are distinct, spanned by elements of $\{0,1\}^k$ and which is nondegenerate in the sense that V_r is not contained in any subspace $\{x \in \mathbb{Q}^k : x_i = x_j\}$;
(2) Parameters $1 \geq c_1 \geq c_2 \geq \cdots \geq c_{r+1} \geq 0$;
(3) Probability measures $\mu_1, \ldots, \mu_r$, with μ_i supported on $\{0,1\}^k \cap V_i$

such that we have the following *entropy condition*

$$\mathrm{e}(\mathcal{V}') \geq \mathrm{e}(\mathcal{V}), \tag{1}$$

for all subflags $\mathcal{V}' \leq \mathcal{V}$, where

$$\mathrm{e}(\mathcal{V}') := \sum_{j=1}^{r} (c_j - c_{j+1}) \mathbb{H}_{\mu_j}(V_j') + \sum_{j=1}^{r} c_j \dim(V_j'/V_{j-1}').$$

Define the variant $\tilde{\gamma}_k$ in exactly the same way, except with 1 replaced by the *strict entropy condition*

$$\mathrm{e}(\mathcal{V}') > \mathrm{e}(\mathcal{V})$$

for all proper subflags $\mathcal{V}' < \mathcal{V}$.

The main theorem of the first part of our paper is then

Theorem 4. *We have $\tilde{\gamma}_k \leq \beta_k \leq \gamma_k$ (and probably all three are equal, but we cannot quite prove this).*

The optimisation problem is very complicated. We have (under certain conditions) been able to solve it when the flag $\mathcal{V}$ is fixed.

Theorem 5. *Suppose that the flag $\mathcal{V}$ is fixed. Under certain conditions (satisfied in situations of interest) the optimal value of c_{r+1} in the optimisation problem is given by the formula*

$$\tilde{\gamma}_k(\mathcal{V}) = (\log 3 - 1)\Big/\Big(\log 3 + \sum_{i=1}^{r-1} \frac{\dim(V_{i+1}/V_i)}{\rho_1 \cdots \rho_i}\Big). \tag{2}$$

Here, the ρ_i are certain parameters defined in terms of the tree structure induced on $\{0,1\}^k$ by the flag $\mathcal{V}$ (draw a picture): for $\rho = (\rho_1, \rho_2, \dots)$ define $f^C(\rho) = 1$ for C at level 0 and then $f^C(\rho) = \sum_{C \to C'} f^{C'}(\rho)^{\rho_{i-1}}$ where C' runs over the children of C. Then our parameters are the ones which satisfy the ρ-equations

$$f^{\Gamma_{j+1}}(\rho) = (f^{\Gamma_j}(\rho))^{\rho_j} e^{\dim(V_{j+1}/V_j)}, \qquad j = 1, 2, \dots, r-1.$$

Finally, let me describe the flags $\mathcal{V}$ which, by extensive numerical experimentation and "naturality" we believe to be (asymptotically) optimal.

Definition. (Binary flags) Let $k = 2^r$ be a power of two. Identify $\mathbb{Q}^k$ with $\mathbb{Q}^{\mathcal{P}[r]}$ (where $\mathcal{P}[r]$ means the power set of $[r] = \{1, \dots, r\}$) and define a flag $\mathcal{V}$, $\langle \mathbf{1} \rangle = V_0 \le V_1 \le \cdots \le V_r = \mathbb{Q}^{\mathcal{P}[r]}$, as follows: V_i is the subspace of all $(x_S)_{S \subset [r]}$ for which $x_S = x_{S \cap [i]}$ for all $S \subset [r]$.

For these flags, we have been able to show that $\rho = \lim_{i \to \infty} \rho_i$ exists and is given by the recipe described at the start of the report.

References

[1] K. Ford, B. Green and D. Koukoulopoulos, Equal sums in random sets and the concentration of divisors, arxiv 1908.00378.

Goldbach Numbers in Short Intervals

Lasse Grimmelt

In this talk, I present how one can decrease the length of the shortest interval for which almost all even numbers in it are the sum of two primes. More precisely the main result is the following.

Theorem 1. *Let $\epsilon > 0$, $A > 0$, and X be large. If*

$$H > X^{7/120+\epsilon},$$

then all but at most

$$O_{\epsilon,A}(H(\log X)^{-A})$$

even $n \in [X - H, X]$ are the sum of two primes.

This is improves Harman's previous result (see chapter 10 of [Harm07]), who obtained the exponent

$$11/180 + \epsilon.$$

Note that $7/120 \approx 0.0583$ and $11/180 \approx 0.0611$.

For this no new Dirichlet Polynomial related results are used, instead the improvement is caused by applying a version of the Circle Method that uses minorants

for the primes more efficiently than Harman's approach. Harman uses minorants and majorants together with a vector sieve type inequality. This means he needs strong numerical results for the applied functions. I will explain how one can instead use a nonnegative model for one of the minorants. In this way we do need neither a vector sieve inequality nor majorants and any minorant with positive density is sufficient.

The application of a nonnegative model he increased efficiency of the applications of minorants is owing to a shifted perspective of the Circle Method. Instead of dissecting into major and minor arcs, a suitable approximation in physical space is used. This idea can be found in similar form in the proofs of Vinogradov's three primes theorem in Heath-Brown's [H-B85] or in chapter 19 of Iwaniec and Kowalski's book [IK04]. See also Green's transference principle in [Gre05] that uses the fact that there is a well behaved (namely constant) fourier close approximation to the W-tricked von Mangoldt function.

References

[Harm07] G. Harman. Prime-detecting sieves. London Mathematical Society Monographs Series, 33. Princeton University Press, Princeton, (NJm 2007). xvi+362 pp.

[H-B85] D.R. Heath-Brown. The ternary Goldbach problem. Rev. Mat. Iberoamericana 1 (1985), no. 1, 45–59.

[IK04] H. Iwaniec and E. Kowalski. Analytic number theory. American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, (2004), xii+615 pp.

[Gre05] B. Green. Roth's theorem in the primes. Ann. of Math. (2) 161 (2005), no. 3, 1609–1636.

[GT07] B. Green and T. Tao. Restriction theory of the Selberg sieve, with applications. J. Théor. Nombres Bordeaux 18 (2006), no. 1, 147–182.

The Sieve of Ekedahl Over Quadrics

D.R. Heath-Brown

(joint work with Tim Browning)

The results described are provisional. Let $F(X_1, \dots, X_n)$ and $G(X_1, \dots, X_n)$ be coprime homogeneous polynomials defined over $\mathbb{Z}$, and suppose we want to know the asymptotic behaviour of

$$\#\{\mathbf{x} \in \mathbb{Z}^n : |\mathbf{x}|_\infty \le B,\, \gcd(F(\mathbf{x}), G(\mathbf{x})) = 1\}$$

as $B \to \infty$. If we attack this problem with a simple sieve procedure we can easily handle common prime factors $p \le B$, but primes bigger than B are potentially problematic. However we have the estimate

$$\#\{\mathbf{x} \in \mathbb{Z}^n : |\mathbf{x}|_\infty \le B,\, \exists p > M,\, p \mid F(\mathbf{x}), G(\mathbf{x})\} \ll_{F,G} (B^{n-1} + BM^{-1} \log B),$$

uniformly in M, which allows us to deal satisfactorily with large primes. This result is known as the "Sieve of Ekedahl" (or the "Geometric Sieve") and originates in work of Torsten Ekedahl [1].

The literature contains some quite divers applications of the Sieve of Ekedahl. For example, Bhargava, Shankar and Wang [2] use it in an auxiliary capacity in their proof that a positive proportion of monic integer polynomials of given degree have square-free discriminant.

There are situations in which one wants to count only points $\mathbf{x}$ that lie on a subvariety of $\mathbb{A}^n$, and still to get a non-trivial sieve bound. In order to achieve this it is clearly necessary that we should be able to recover the correct estimate when $M = 1$. In other words, we need to be able to count points on the variety in question, getting the correct order of magnitude. In practice this restricts us to quadric hypersurfaces (or perhaps to higher dimensional varieties, using the circle method). Thus we seek a good upper bound for

$$\#\{\mathbf{x} \in \mathbb{Z}^n : Q(\mathbf{x}) = 0,\ |\mathbf{x}|_\infty \le B,\ \exists p > M,\ p \mid F(\mathbf{x}), G(\mathbf{x})\}$$

when Q is a quadratic form, subject to suitable conditions on F and G.

In general we should be able to use the equation $Q = 0$ to eliminate one of the variables from F and G, and indeed we should be able to eliminate a variable between F and G. Then, with a change of notation replacing n by $n + 2$, the following is our Sieve of Ekedahl over quadrics.

Theorem. Let $Q(X_1, \dots, X_n), F(X_1, \dots, X_{n+1})$ and $G(X_1, \dots, X_n)$ be homogeneous polynomials defined over $\mathbb{Z}$, where Q is a quadratic form. Suppose further that

(i) The rank of Q as a quadratic form is at least 3;
(ii) F is coprime to X_{n+1} and G; and
(iii) G is coprime to Q and is primitive (i.e. there is no prime which divides G identically).

For $B, M \ge 1$ we define $N(B, M)$ to be the number of integer vectors $\mathbf{x} \in \mathbb{Z}^{n+2}$ in the box $|\mathbf{x}|_\infty \le B$ which lie on the quadric $Q(x_1, \dots, x_n) = x_{n+1}x_{n+2}$ and for which the forms $F(x_1, \dots, x_{n+1})$ and $G(x_1, \dots, x_n)$ have a common prime divisor $p \ge M$.

Then

$$N(B, M) \ll_{Q,F,G,\varepsilon} B^\varepsilon \{B^{n-1/(n+1)} + B^n M^{-1}\}$$

for any fixed $\varepsilon > 0$.

When $M = 1$ we recover the bound $O_\varepsilon(B^{n+\varepsilon})$ for the number of integral points on the quadric $Q(x_1, \dots, x_n) = x_{n+1}x_{n+2}$ in the box $[-B, B]^{n+2}$.

The proof of the theorem covers the points on the quadric by a large number of affine linear spaces. One then employs a suitable version of the usual Sieve of Ekedahl to count the relevant points on each of these linear spaces.

References

[1] T. Ekedahl, An infinite version of the Chinese remainder theorem, Comment. Math. Univ. St. Paul. 40(1991), 53–59.
[2] M. Bhargava, A. Shankar, and X. Wang, Squarefree values of polynomial discriminants I, arXiv:1611.09806.

On the Erdős discrepancy problem over $\mathbb{F}_q[x]$

Oleksiy Klurman
(joint work with Alexander Mangerel, Joni Teräväinen)

This report is based on a joint work A. Mangerel and J. Teräväinen. The Erdős Discrepancy Problem (EDP) states that, given any sequence $f : \mathbb{N} \to \{-1, +1\}$, the *discrepancy* of f on homogeneous arithmetic progressions satisfies

$$\sup_{d,N\geq 1}\left|\sum_{n\leq N} f(dn)\right| = \infty.$$

It is not difficult to see that for completely multiplicative sequences (i.e., when $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}$), the extra supremum over d is inconsequential, and therefore such sequences might be expected to have minimal discrepancy among all sequences. It is thus a natural problem within the framework of the EDP to classify all such completely multiplicative functions.

In Tao's solution of the EDP [1], he indeed reduced the problem to proving that for any (stochastic) completely multiplicative function $f : \mathbb{N} \to S^1$, one has

$$\limsup_{N\to\infty}\left|\sum_{n\leq N} f(n)\right| = \infty. \tag{1}$$

Thus, in number fields, all completely multiplicative functions taking values on the unit circle have infinite discrepancy, and this is sufficient to establish the EDP.

It is natural to consider the corresponding problem regarding completely multiplicative functions defined in the context of the ring of polynomials over a finite field. Let q be a prime power and let $\mathcal{M}$ denote the set of monic polynomials in $\mathbb{F}_q[t]$. Given a completely multiplicative function $f : \mathcal{M} \to \{-1, +1\}$, must it be true that

$$\mathcal{L}_f := \limsup_{N\to\infty}\left|\sum_{\substack{G\in\mathcal{M}\\ \deg G\leq N}} f(G)\right| = \infty? \tag{2}$$

As was noted during the Polymath 5 project leading to the solution of the EDP, the answer to this question is no: while no constructive examples are given, a recipe to build such functions stems from the recurrence relation

$$m\sum_{\substack{G\in\mathcal{M}\\ \deg G=m}} f(G) = \sum_{0\leq k\leq m}\left(\sum_{\substack{G\in\mathcal{M}\\ \deg G=m-k}} f(G)\right)\cdot\left(\sum_{\substack{P\in\mathcal{P}\\ \deg P=k}} kf(P)\right),$$

from which an initial choice of values of $f(P)$ can be made to force these sums (averaged over $m \leq N$) to be small.

Our purpose in this paper is to consider an alternative variant of the discrepancy problem in function fields, wherein our measure of discrepancy will differ from that

proposed above. Given $f : \mathcal{M} \to S^1$ completely multiplicative, we consider the more complicated expression

$$\mathcal{S}_f := \limsup_{N\to\infty} \max_{1\le H\le N} \max_{\substack{G_0\in\mathcal{M}\\ \deg G_0\le N}} \left| \sum_{\substack{G\in\mathcal{M}\\ \deg G - G_0 < H}} f(G) \right|,$$

which we shall refer to as the *short sum discrepancy*, in contrast to (2) which we shall call the *long sum discrepancy*.
It is not hard to see that $\mathcal{S}_f \ge \mathcal{L}_f$ (when $\deg G_0 = N-1$ and $H = N$, $\{G \in \mathcal{M} : \deg G - G_0 < H\} = \mathcal{M}_{\le N-1}$), so getting a handle on the boundedness of $\mathcal{S}_f$ is generally more difficult than for $\mathcal{L}_f$. Note that in number fields these problems are identical: since the integers are linearly ordered, we get by the triangle inequality that

$$\limsup_{N\to\infty} \left| \sum_{n\le N} f(n) \right| \le \limsup_{N\to\infty} \max_{1\le H\le N} \left| \sum_{N-H<n\le N} f(n) \right| \le 2 \limsup_{N\to\infty} \left| \sum_{n\le N} f(n) \right|.$$

Our objective is to to classify those completely multiplicative functions that have bounded short sum discrepancy in function fields. Our main result is the followin

Theorem 1. *Let $f : \mathcal{M} \to S^1$ be a sequence. Then $\mathcal{S}_f < \infty$ if and only if there is a prime power P^k, a non-principal Dirichlet character χ modulo P^k, a short interval character ξ of bounded length ν and $\theta \in [0,1]$ such that $f(P') = \chi(P')\xi(P')e_\theta(P')$ for all primes $P' \ne P$, and either $\theta = 0$ or $\theta \ne 0$ and $f(P) \ne 1$.*

We can show that the collection of completely multiplicative functions with *bounded* long sum discrepancy and unbounded short sum discrepancy is non-empty.

Proposition 2. *There are infinitely many completely multiplicative functions $f : \mathcal{M} \to \{-1,+1\}$ for which $\mathcal{L}_f < \infty$ but $\mathcal{S}_f = \infty$.*

References

[1] Tao, T., The Erdos Discrepancy Problem, Discrete Anal. 1(2016), 29 pp.

On the Duffin-Schaeffer conjecture

Dimitris Koukoulopoulos, James Maynard

Let $\psi : \mathbb{N} \to \mathbb{R}_{\ge 0}$ be an arbitrary function from the positive integers to the non-negative reals. Given $\alpha \in \mathbb{R}$, we wish to understand when we can find infinitely many integers a and q such that

$$\left| \alpha - \frac{a}{q} \right| \le \frac{\psi(q)}{q}. \tag{1}$$

Clearly, it suffices to restrict our attention to numbers $\alpha \in [0,1]$.

When $\psi(q) = 1/q$ for all q, Dirichlet's approximation theorem implies that, given *any* $\alpha \in [0,1]$, there are infinitely many coprime integers a and q satisfying (1). On the other hand, the situation can become significantly more complicated if ψ behaves more irregularly. However, the conjecture of Duffin and Schaeffer [2] give a classification of when *almost all* α have infinitely many solutions to (1), and when *almost no* α have infinitely many solutions. We establish this result, giving the following.

Theorem 1 (Duffin-Schaeffer conjecture)**.** *Let*

$$\mathcal{A}_\psi := \{\alpha \in [0,1] : (1) \text{ has infinitely many solutions with } (a,q) = 1\}.$$

Then

$$\operatorname{meas}(\mathcal{A}_\psi) = \begin{cases} 1, & \text{if } \sum_q \frac{\phi(q)}{q}\psi(q) = \infty, \\ 0, & \text{if } \sum_q \frac{\phi(q)}{q}\psi(q) < \infty. \end{cases}$$

It was known by work of Gallagher [4] based on ergodic theory that $\operatorname{meas}(\mathcal{A}) \in \{0,1\}$, and so the key content of the theorem is the simple classification of when $\operatorname{meas}(\mathcal{A}) = 0$ and when $\operatorname{meas}(\mathcal{A}) = 1$. It is vital in the Duffin-Schaeffer conjecture that we only consider $(a,q) = 1$; the natural equivalent statement without this condition fails in general due to overcounting non-reduced residues. However, as a direct corollary, we obtain Catlin's conjecture [1] which does handle solutions to (1) where the approximations are not necessarily reduced fractions, extending a classical theorem of Khinchin [5].

Theorem 2. *Let* $\psi : \mathbb{N} \to \mathbb{R}_{\geq 0}$. *Define* $\tilde{\psi}(q) := q \sup_{q|n} \frac{\psi(n)}{n}$, *and let*

$$\mathcal{K}_\psi := \{\alpha \in [0,1] : (1) \text{ has infinitely many solutions with } a, q \in \mathbb{Z}\}.$$

Then

$$\operatorname{meas}(\mathcal{K}_\psi) = \begin{cases} 1, & \text{if } \sum_q \frac{\phi(q)}{q}\tilde{\psi}(q) < \infty, \\ 0, & \text{if } \sum_q \frac{\phi(q)}{q}\tilde{\psi}(q) < \infty. \end{cases}$$

Consider the situation that we choose $\alpha \in [0,1]$ uniformly at random, and let E_q be the event that

$$\alpha \in [0,1] \cap \bigcup_{\substack{1 \leq a \leq q \\ \gcd(a,q)=1}} \Big[\frac{a-\psi(q)}{q}, \frac{a+\psi(q)}{q}\Big].$$

Then the probability of E_q is essentially $2\phi(q)\psi(q)/q$, and so the 'easy' direction of the Borel-Cantelli theorem states that almost surely only finitely many of the events E_q occur if

$$\sum_{q \geq 1} \mathbb{P}(E_q) = 2 \sum_q \frac{\phi(q)}{q}\psi(q) < \infty.$$

This shows that if the above sum is finite, then $\mathrm{meas}(\mathcal{A}_\psi) = 0$. The 'hard' direction of the Borel-Cantelli theorem gives a converse to the above result if the E_q are independent. Thus the Duffin-Schaeffer conjecture can be thought of as the statement that the events E_q are 'almost independent'. Indeed, by Gallagher's Theorem it suffices to show $\mathrm{meas}(\mathcal{A}_\psi) > 0$ when the sum diverges, and by a second moment argument this reduces to showing

$$\mathbb{P}(E_q \text{ and } E_r) \ll \mathbb{P}(E_q)\mathbb{P}(E_r)$$

'on average' over q, r. This inequality holds unless q, r have a large common divisor, and understanding the structure of sets with many pairs having large common divisors is the key to our proof. This leads us to the following model problem.

Question. *Let $\mathcal{S} \subseteq [x, 2x]$ satisfy $\#\mathcal{S} \asymp x^c$ and be such that there are $\#\mathcal{S}^2/100$ pairs $(a_1, a_2) \in \mathcal{S}^2$ with $\gcd(a_1, a_2) > x^{1-c}$. Must it be the case that there is an integer $d \gg x^{1-c}$ which divides $\gg \#\mathcal{S}$ elements of $\mathcal{S}$?*

It turns out that this is false as stated, but we can prove a technical variant of this, which, when combined with ideas of Erdős-Vaaler [3, 6] on the anatomy of integers, suffices for Theorem 1.

To attack this model problem we use a 'compression' argument. We repeatedly pass to subsets of $\mathcal{S}$ where we have increasing control over whether given primes occur in the GCDs or not, whilst at the same time showing that the size of the original set is controlled in terms of the size of the new set. At the end of the iteration procedure we will then have arrived at a subset which controls the size of $\mathcal{S}$, and where we know that all large GCDs are caused by a fixed divisor. Since the final set then has a very simple GCD structure, it is very easy to analyse, and since we control the statistics of the original set we will have enough information to establish a positive result.

References

[1] P. A. Catlin, Two problems in metric Diophantine approximation. I, J. Number Theory 8 (1976), no. 3, 282–288.

[2] R. J. Duffin and A. C. Schaeffer, Khinchin's problem in metric Diophantine approximation. Duke Math. J. 8, (1941). 243–255.

[3] P. Erdős, On the distribution of the convergents of almost all real numbers, J. Number Theory 2 (1970), 425–441.

[4] P. Gallagher, Approximation by reduced fractions, J. Math. Soc. Japan 13 (1961), 342–345.

[5] A. Khintchine, Einige Sätze über Kettenbrüche, mit Anwendungen auf die Theorie der Diophantischen Approximationen, Math. Ann. 92 (1924), no. 1-2, 115–125.

[6] J. D. Vaaler, On the metric theory of Diophantine approximation, Pacific J. Math. 76 (1978), no. 2, 527–539.

The distribution of the maximum of partial sums of Kloosterman sums and other trace functions

Youness Lamzouri
(joint work with Pascal Autissier, Dante Bonolis)

Let $m \geq 2$ be an integer, and $\varphi : \mathbb{Z}/m\mathbb{Z} \to \mathbb{C}$ a complex valued function which we extend to an m-periodic function $\varphi : \mathbb{Z} \to \mathbb{C}$. An important problem in analytic number theory is to obtain non-trivial estimates for the quantity

$$\mathcal{M}(\varphi) := \max_{x<m} \Big| \sum_{0\leq n\leq x} \varphi(n)\Big|.$$

The special case where $\varphi = \chi$ is a Dirichlet character modulo m has been extensively studied over the last century, going back to the classical inequality proved by Pólya and Vinogradov in 1918: $\mathcal{M}(\chi) \ll \sqrt{m}\log m$. A straightforward generalization of this bound for a general m-periodic complex valued function φ gives

$$\mathcal{M}(\varphi) \ll ||\widehat{\varphi}||_\infty \sqrt{m}\log m, \tag{1}$$

where $\widehat{\varphi} : \mathbb{Z} \to \mathbb{C}$ is the normalized discrete Fourier transform of φ, defined by $\widehat{\varphi}(h) := \frac{1}{\sqrt{m}} \sum_{n \pmod m} \varphi(n)e_m(hn)$, where $e_m(z) := \exp(2\pi iz/m)$. We shall only consider those φ for which the Fourier transform $\widehat{\varphi}$ is uniformly bounded (this includes primitive Dirichlet characters). In the case of character sums, Montgomery and Vaughan [8] proved that this bound is not optimal conditionally on the generalized Riemann hypothesis GRH. Indeed, they showed that assuming GRH we have $\mathcal{M}(\chi) \ll \sqrt{m}\log\log m$, for all non-principal Dirichlet characters $\chi \pmod m$. This last bound is in fact optimal in view of an old result of Paley [9] who showed that $\mathcal{M}(\chi_m) \gg \sqrt{m}\log\log m$ for infinitely many m, where χ_m is the quadratic character modulo m.

Recently, Bober, Goldmakher, Granville and Koukoulopoulos [2] investigated the distribution of $\mathcal{M}(\chi)$ over non-principal characters χ modulo a large prime q. If we denote by $\Phi_{\text{char}}(V)$ the proportion of non-principal characters $\chi \bmod q$ for which $\mathcal{M}(\chi)/\sqrt{q} > V$, then the main result of [2] states that for $1 \leq V \leq C_0 \log\log q - C$ (where C is an absolute constant, and $C_0 = e^\gamma/\pi$, where γ is the Euler-Mascheroni constant), one has

$$\Phi_{\text{char}}(V) = \exp\left(-\frac{e^{V/C_0+O(1)}}{V}\right). \tag{2}$$

Motivated by a recent work of Kowalski and Sawin [5], we obtain similar results in [1] for the distribution of the maximum of partial sums of several families of exponential sums, including Birch and Kloosterman sums. For a prime $p \geq 3$, the (normalized) Birch sums and Kloosterman sums are defined respectively as follows

$$\mathrm{Bi}_p(a) := \frac{1}{\sqrt{p}} \sum_{n\in\mathbb{F}} e_p(n^3 + an), \text{ and } \mathrm{Kl}_p(a,b) := \frac{1}{\sqrt{p}} \sum_{n\in\mathbb{F}_p^\times} e_p(an + b\overline{n}),$$

where $(a,b) \in \mathbb{F}_p^\times \times \mathbb{F}_p^\times$ and $\overline{n}$ denotes the multiplicative inverse of n modulo p. Livné [7] proved that $\mathrm{Bi}_p(a)$ becomes equidistributed according to the Sato-Tate measure as a varies in $\mathbb{F}_p^\times$ and $p \to \infty$, and Katz [4] proved the analogous result for $\mathrm{Kl}_p(a,1)$. Let $\varphi_a(n) = e_p(n^3 + an)$ and $\psi_{(a,b)}(n) = e_p(an + b\overline{n})$ and define

$$\Phi_{\mathrm{Bi}}(V) = \frac{1}{p-1}\left|\left\{a \in \mathbb{F}_p^\times : \mathcal{M}(\varphi_a)/\sqrt{p} > V\right\}\right|.$$

and

$$\Phi_{\mathrm{Kl}}(V) := \frac{1}{(p-1)^2}\left|\left\{(a,b) \in \mathbb{F}_p^\times \times \mathbb{F}_p^\times : \mathcal{M}(\psi_{(a,b)})/\sqrt{p} > V\right\}\right|.$$

Improving on the work of Lamzouri [6], we prove the following result, which is the analogue of (2) for Birch and Kloosterman sums.

Theorem 1. *Let p be large. There exists a constant C such that for all real numbers $1 \le V \le (2/\pi)(\log\log p - 2\log\log\log p - C)$ we have*

$$\Phi_{\mathrm{Kl}}(V) = \exp\left(-\exp\left(\frac{\pi}{2}V + O(1)\right)\right).$$

Moreover, the same result holds for $\Phi_{\mathrm{Bi}}(V)$.

The techniques used to prove this result are different from [2], due to the lack of multiplicativity for these exponential sums. Indeed, in the case of character sums, Bober, Goldmakher, Granville and Koukoulopoulos [2] exploit the relation with L-functions and smooth numbers, while ingredients from algebraic geometry and notably Deligne's equidistribution theorem [3] play a central role in the proof of Theorem 1.

Our results apply to general families of periodic functions satisfying certain conditions. More specifically, let $\mathcal{F} = \{\varphi_a\}_{a\in\Omega_m}$ be a family of m-periodic complex valued functions, where $\Omega_m \neq \emptyset$ is a finite set, and consider the following assumptions:

Assumption 1. Uniform boundedness. We have $\max_{a\in\Omega_m} ||\varphi_a||_\infty \ll 1$, where the implied constant is independent of m.

Assumption 2. Support of the Fourier transform. There exists an absolute constant $N > 0$ such that for all $a \in \Omega_m$ and $h \in \mathbb{Z}/m\mathbb{Z}$ we have $\widehat{\varphi_a}(h) \in [-N, N]$.

Assumption 3. Joint distribution of the Fourier transform. There exists a sequence of I.I.D. random variables $\{\mathbb{X}(h)\}_{h\in\mathbb{Z}^*}$ supported on $[-N,N]$, and absolute constants $\eta \ge 1/2$ and $C_1 > 1$, such that for all positive integers $k \le \log m/\log\log m$, and all k-uples $(h_1,\dots,h_k) \in (-m/2, m/2]^k$ with $h_i \neq 0$ for $i = 1, ..., k$ we have $\dfrac{1}{|\Omega_m|}\displaystyle\sum_{a\in\Omega_m} \widehat{\varphi_a}(h_1)\cdots\widehat{\varphi_a}(h_k) = \mathbb{E}\left(\mathbb{X}(h_1)\dots\mathbb{X}(h_k)\right) + O\left(C_1^k/m^\eta\right)$.

Furthermore, if we let $\mathbb{X}$ be a random variable with the same distribution as the $\mathbb{X}(h)$, then $\mathbb{X}$ verifies the following conditions:

3a. There exists a positive constant A such that for all $\varepsilon \in (0,1]$ we have $\mathbb{P}(\mathbb{X} > N - \varepsilon) \gg \varepsilon^A$, and $\mathbb{P}(\mathbb{X} < -N + \varepsilon) \gg \varepsilon^A$.

3b. For all integers $\ell \ge 0$ we have $\mathbb{E}\left(\mathbb{X}^{2\ell+1}\right) = 0$.

Assumption 4. Strong bounds for short sums on average. There exist absolute constants $\alpha \geq 1$, and $0 < \delta < 1/2$ such that for any interval I of length $|I| \leq m^{1/2+\delta}$, one has $\frac{1}{|\Omega_m|} \sum_{a \in \Omega_m} \left| \frac{1}{\sqrt{m}} \sum_{n \in I} \varphi_a(n) \right|^\alpha \ll m^{-1/2-\delta}$.

Our main result is the following theorem.

Theorem 2. *Let m be large, and $\mathcal{F} = \{\varphi_a\}_{a \in \Omega_m}$ be a family of m-periodic complex valued functions satisfying one of the following subsets of the above assumptions:*

A. *Assumption 2 and Assumption 3 with $\eta > 1$.*
B. *Assumptions 1, 2, and Assumption 3 with $1/2 < \eta \leq 1$.*
C. *Assumptions 1, 2, 4, and Assumption 3 with $\eta = 1/2$.*

Then there exists a constant $B = B(A)$ such that for all real numbers $1 \leq V \leq (N/\pi)(\log\log m - 2\log\log\log m - B)$ we have

$$\Phi_{\mathcal{F}}(V) := \frac{1}{|\Omega_m|} \left| \left\{ a \in \Omega_m : \frac{\mathcal{M}(\varphi_a)}{\sqrt{m}} > V \right\} \right| = \exp\left(- \exp\left(\frac{\pi}{N} V + O(1) \right) \right).$$

Using ingredients from algebraic geometry, we exhibit several families of exponential sums which satisfy the assumptions of Theorem 2. These correspond to certain families of ℓ-adic trace functions for which the arithmetic and geometric monodromy groups are both equal to $\mathrm{Sp}_{2r}(\mathbb{C})$, for a certain integer $r \geq 1$. In particular Theorem 2 apply to the following families :

1. $\mathcal{F}_1 = \{\varphi_a\}_{a \in \mathbb{F}_p^\times}$ where $\varphi_a(n) = e_p(an + g(n))$, and $g \in \mathbb{Z}[t]$ is an odd polynomial.
2. $\mathcal{F}_2 = \{\varphi_{(a,b)}\}_{(a,b) \in \mathbb{F}_p^\times \times \mathbb{F}_p^\times}$ where $\varphi_{(a,b)}(n) = e_p(bn + (a\overline{n})^r)$ and $r \geq 1$ is odd.
3. $\mathcal{F}_3 = \{\varphi_{(a,b)}\}_{(a,b) \in \mathbb{F}_p^\times \times \mathbb{F}_p^\times}$ where $\varphi_{(a,b)}(n) = \mathrm{Kl}_r(\overline{an}; p) e_p(bn)$, and Kl_r is the r-th hyper-Kloosterman sum.

A direct application of Theorem 2 shows that if $\mathcal{F} = \{\varphi_a\}_{a \in \Omega_m}$ satisfies the assumptions of this result then there are many elements $a \in \Omega_m$ such that

$$\mathcal{M}(\varphi_a) \gg \sqrt{m} \log\log m. \tag{3}$$

Due the double exponential decay of $\Phi_{\mathcal{F}}(V)$ and the uniformity of Theorem 2, one is led to conjecture that this bound is optimal if $|\Omega_m| \ll m^B$. Surprisingly, we show that this is in fact false. Indeed, we are able to construct a family $\mathcal{F} = \{\varphi_a\}_{a \in \Omega_m}$ of m-periodic complex valued functions satisfying the assumptions of Theorem 2, such that $|\Omega_m| \asymp m^3$, and for which the Pólya-Vinogradov inequality is sharp, that is

$$\max_{a \in \Omega_m} \mathcal{M}(\varphi_a) \gg \sqrt{m} \log m.$$

This suggests the existence of a transition in the behavior of the distribution function $\Phi_{\mathcal{F}}(V)$ near the maximal values. It also confirms the common belief in analytic number theory that the Pólya-Vinogradov inequality, though simple to derive, is extremely difficult to improve.

References

[1] P. Autissier, D. Bonolis, and Y. Lamzouri, The distribution of the maximum of partial sums of Kloosterman sums and other trace functions. Submitted, 45 pages. arXiv:1909.03266.

[2] J. Bober, L. Goldmakher, A. Granville, and D. Koukoulopoulos, The frequency and the structure of large character sums. J. Eur. Math. Soc. (JEMS) 20 (2018), no. 7, 1759–1818.

[3] P. Deligne, La conjecture de Weil. II, Inst. Hautes Études Sci. Publ. Math. (1980) no. 52, 137-252.

[4] N.M. Katz, Gauss sums, Kloosterman sums, and monodromy groups, Annals of Mathematics Studies 116, (1988), x+246.

[5] E. Kowalski and W. Sawin, Kloosterman paths and the shape of exponential sums, Compos. Math. 152 (2016), no. 7, 1489–1516.

[6] Y. Lamzouri, On the distribution of the maximum of cubic exponential sums, To appear in J. Inst. Math. Jussieu, 28 pages.

[7] R. Livné, The average distribution of cubic exponential sums, J. reine angew. Math. 375–376 (1987), 362–379.

[8] H. L. Montgomery, and R. C. Vaughan, Exponential sums with multiplicative coefficients,Invent. Math. 43 (1977), no. 1, 69–82.

[9] R. E. A. C. Paley, A theorem on characters, J. London Math. Soc. 7 (1932), 28–32.

The Möbius function in all short intervals

Kaisa Matomäki

(joint work with Joni Teräväinen)

Let $\Lambda(n)$ and $\mu(n)$ denote the von Mangoldt and Möbius functions. In 1972 Huxley [3] proved that the prime number theorem holds in intervals of length $H \geq x^{7/12+\varepsilon}$, i.e.

$$\sum_{x<n\leq x+H} \Lambda(n) = (1+o(1))H \quad \text{for } H \geq x^{7/12+\varepsilon}. \tag{1}$$

Soon after Huxley's work, Ramachandra [5] adapted the proof to sequences arising as Dirichlet series coefficients of products of Dirichlet L-functions, their powers, logarithms, and derivatives (a class of sequences whose most notable representatives are $\mu(n)$ and $\Lambda(n)$), showing for instance that

$$\sum_{x<n\leq x+H} \mu(n) = O\left(H \exp\left(-c\left(\frac{\log x}{\log\log x}\right)^{1/3}\right)\right) \quad \text{for } H \geq x^{7/12+\varepsilon}.$$

The only improvement on Huxley's and Ramachadra's results is that of Heath-Brown [2] that one can obtain asymptotic formula for intervals of length $H \geq x^{7/12-\varepsilon(x)}$ for any $\varepsilon(x)$ tending to 0 at infinity.

In the talk I discussed our recent work showing that in various instances, including the Möbius function but not the von Mangoldt function, the length of the interval $x^{7/12+\varepsilon}$ can be improved to $x^{0.55+\varepsilon}$. For the Möbius function our result is

Theorem 1. *Let $\theta > 0.55$ and $\varepsilon > 0$ be fixed. Then, for x large enough and $H \geq x^\theta$, we have*

$$\sum_{x<n\leq x+H} \mu(n) = O\left(\frac{H}{(\log x)^{1/3-\varepsilon}}\right). \tag{2}$$

Note that even under the Riemann Hypothesis, one can only get such results for $\theta > 1/2$ (see e.g. [4, Section 10.5]), so our theorem moves a long-standing record significantly closer to a natural barrier (note that $7/12 = 0.5833\ldots$).

The 7/12 exponent in Huxley's and Ramachandra's works is a very natural barrier: A crucial piece of information needed in Huxley's and Ramachandra's proofs is a bound of the form $N(\sigma, T) \ll T^{B(1-\sigma)}$ (where $N(\sigma, T)$ is the number of zeros of the Riemann zeta function in the rectangle $\Re(s) \geq \sigma$, $|\Im(s)| \leq T$) for $T \geq 2$, $\sigma \in [1/2, 1]$, with B as small as possible. The best value of B to date is Huxley's $B = \frac{12}{5} + o(1)$, which is the reason for the appearance of the 7/12 exponent.

Huxley's prime number theorem (1) was proved differently by Heath-Brown in [1], but this proof also runs into serious difficulties when one tries to lower θ below 7/12. Heath-Brown does not use zero density results but rather uses a combinatorial decomposition (Heath-Brown's identity) and mean and large value estimates for Dirichlet polynomials, but since zero density estimates are based on these, the difficulty one runs into is actually essentially the same.

Our proof of Theorem 1 manages to avoid the lack of improvements to Huxley's zero-density estimate by means of Ramaré's identity, which allows a more flexible combinatorial factorization of the Möbius function than what arises from applying Heath-Brown's identity from [1] alone: We will first apply Ramaré's identity to extract a small prime factor and then Heath-Brown's identity to the remaining long variable.

Like Ramachandra's, our method works for a wide class of multiplicative functions. In particular, in intervals of length $x^{0.55+\varepsilon}$, we can show an asymptotic formula for the number of integers that can be written as a sum of two squares, and an asymptotic formula for the mean value of k-fold divisor function (where k is allowed to be also complex).

Our method can also be used for twisted sums. For instance we can show that, uniformly for $\alpha \in \mathbb{R}$, the twisted Möbius function $\mu(n)e(\alpha n)$ exhibits cancellations in intervals of length $x^{3/5+\varepsilon}$, improving a result of Zhan [6, Theorem 5] from 1991 that worked for intervals of length

$$\geq x^{5/8}(\log x)^A.$$

The proof of Theorem 1 is inapplicable for the corresponding problem for the von Mangoldt function, since one cannot extract small prime factors from numbers n in the support of $\Lambda(n)$. Nevertheless, as pointed out to us by Maksym Radziwiłł in the Oberwolfach meeting, the proof does work for E_2 almost primes, that is to say numbers of the form p_1p_2 with p_1, p_2 primes: We are able to obtain an asymptotic formula for the count of E_2 numbers on intervals of length $x^{0.55+\varepsilon}$.

Theorem 2. *Let $\theta > 0.55$ be fixed. Then for x large enough and $H \geq x^\theta$ we have*

$$\sum_{\substack{x<n\leq x+H\\ n\in E_2}} 1 = H\frac{\log\log x}{\log x} + O\left(H\frac{\log\log\log x}{\log x}\right).$$

References

[1] D. R. Heath-Brown, Prime numbers in short intervals and a generalized Vaughan identity, Canadian J. Math., 34(1982), 1365–1377.

[2] D. R. Heath-Brown, The number of primes in a short interval, J. Reine Angew. Math., 389(1988), 22–63.

[3] M. N. Huxley, On the difference between consecutive primes, Invent. Math., 15(1972), 164–170.

[4] H. Iwaniec and E. Kowalski, Analytic number theory, volume 53 of American Mathematical Society Colloquium Publications, American Mathematical Society, Providence, RI (2004).

[5] K. Ramachandra, Some problems of analytic number theory, Acta Arith., 31(1976), 313–324.

[6] T. Zhan, On the representation of large odd integer as a sum of three almost equal primes, Acta Math. Sinica (N.S.) 7(1991), 259–272.

Problem Session

Hugh L. Montgomery

1. (Montgomery) List the primes, then form unsigned differences between consecutive primes, and repeat:

2		3		5		7		11		13		17		19		$\cdots$				
	1		2		2		4		2		4		2		$\cdots$					
		1		0		2		2		2		2		$\cdots$						
			1		2		0		0		0		$\cdots$							

Norman Gilbreath (1958) conjectured that every row after the first one begins with a 1. Later it was discovered that Proth (1878) proposed a proof of this, and it had been found that the proof was faulty. Does our present state of knowledge of the primes allow us to solve this old problem?

2. (Wooley) The Vinogradov Mean Value Theorem asserts that

$$\int_{[0,1]^k} \Big|\sum_{0\leq n\leq X} e\big(\alpha_1 n + \alpha_2 n^2 + \cdots + \alpha_k n^k\big)\Big|^{2s} \boldsymbol{d\alpha} \ll X^{s+\varepsilon} + X^{2s-\frac{1}{2}k(k+1)}.$$

Let $\mathcal{B}$ be a measurable subset of $[0,1]^k$. The object is to extend the above by showing that

$$\int_{\mathcal{B}} \Big|\sum_{0\leq n\leq X} e\big(\alpha_1 n + \alpha_2 n^2 + \cdots + \alpha_k n^k\big)\Big|^{2s} \boldsymbol{d\alpha} \ll (\operatorname{meas}\mathcal{B})X^{s+\varepsilon} + X^{2s-\frac{1}{2}k(k+1)}.$$

Demeter, Guth, Wong arXiv2019 have done this when $k = 3$ and $\mathcal{B} = [0,1] \times [0,1] \times [0, X^{-\beta}]$ and $\beta < 3/2$.

3. (Green) We are interested in positive integers up to X, and we set $H = X^\theta$ where θ is slightly greater than $1/2$, say $\theta = 0.51$. Put $I = [H, 2H]$. For each prime $p \in I$, choose a residue class a_p. Set

$$\mathcal{K} = [1, X] \cap \bigcup_{p \in I} a_p \,.$$

Is it always true that $\operatorname{card} \mathcal{K} \gg X^{1-\varepsilon}$?

4. (Bober) It is easy to show that if χ is a nonprincipal character modulo p, then

$$\max_{0 \le x \le p} \Big| \sum_{0 < n \le x} \chi(n) \Big| > \frac{\sqrt{p}}{12} \,.$$

What is the best constant C such that

$$\min_{\chi} \max_{0 \le x \le p} \Big| \sum_{0 < n \le x} \chi(n) \Big| < C\sqrt{p}\,?$$

5. (Bober) Is it true that

$$\max_{0 \le x \le p} \Big| \sum_{0 < n \le x} \chi(n) \Big| < 2\sqrt{p}$$

for at least 99% of the characters χ mod p?

6. (Sawin) We know a sharp bound for

$$\Big| \Big\{ f_1, f_2, \dots, f_{2s} \in \mathbb{F}_q[T] : \sum_{i=1}^{s} f_i^r = \sum_{i=s+1}^{2s} f_i^r \text{ for } 1 \le r \le k \Big\} \Big|$$

if $p > k$. Here it is intended that the f_i have degrees not exceeding B, and the 'sharp bound' depends on B. Now consider

$$\Big| \Big\{ f_1, f_2, \dots, f_{2s} \in \mathbb{F}_q[T] : \prod_{i=1}^{s} (1 + f_i u) = \prod_{i=s+1}^{2s} (1 + f_i u) \Big\} \Big|$$

Here the two sides have the same first $k+1$ coefficients. These two problems are equivalent only if $p > k$. Try $k = 3$, $p = 2, 3$.

7. (Myerson) Let $f(n)$ be one of $\sqrt{n}$, n, $n^{3/2}$, n^2, n^3. Let M denote an $a \times b$ matrix of the following sort:

$$M = \begin{bmatrix} f(m_{11}) & \cdots & f(m_{1b}) \\ \vdots & \vdots & \vdots \\ f(m_{a1}) & \cdots & f(m_{ab}) \end{bmatrix}$$

Define

$$\Delta_k = \max |\det N|$$

where the maximum is extended over all the $k \times k$ minors of M. Consider

$$\#\big\{ (m_{ij}) : \Delta_k \sim D_k \ k = 1, 2, \dots, \min(a, b) \big\}$$

Question: what upper bounds can one obtain for this counting function? As motivation, one can observe that

$$\text{measure}\{\vec{v} \in [0,1]^b : |M\vec{v}| < \delta\} \asymp (1 + \sum_{k=1}^{\min\{a,b\}} \delta^{-1}\Delta_k)^{-1}.$$

This quantity arises in various restriction problems.

8. (Radziwiłł) Consider integers x, y, z such that $x^2 + y^2 + z^2 = n$ where $n \equiv 3 \pmod 8$. Duke showed that the set of points

$$\Big(\frac{x}{\sqrt{n}}, \frac{y}{\sqrt{n}}, \frac{z}{\sqrt{n}}\Big)$$

tend toward uniform distribution as $n \to \infty$. Bourgain, Rudnick, and Sarnak consider the number of these points that lie on a tiny cap Ω_n on S^3 of volume $n^{-1/2+\varepsilon}$. Compute

$$\int_{g \in SO(3)} \Big| \#\widehat{\xi}(n) \cap g\Omega_n - \#\widehat{\xi}(n) \operatorname{vol}(\Omega_n) \Big|^2 \, dg \, .$$

9. (Vaughan) Redheffer `https://en.wikipedia.org/wiki/Redheffer_matrix` defined a family of matrices $A_n = [e_{ij}]$ where $e_{i1} = 1$ for all i, and for $i > 1$, $e_{ij} = 1$ if $i|j$, and $e_{ij} = 0$ otherwise. Bounding the determinant of these matrices is equivalent to RH, since it is easy to show that

$$\det A_n = \sum_{k \le n} \mu(k) \, .$$

Since $\det A_n$ is the product of the eigenvalues of A_n it is very desirable to describe the locations of the eigenvalues of A_n. We know that $n-N-1$ of the eigenvalues are 1 where $N = \lfloor \log n \rfloor$ and there is a dominant eigenvalue at about $\sqrt{n}$ and another at about $-\sqrt{n}$. In quite extensive calculations of the eigenvalues by Wayne Barret, and others, the remaining $N-1$ "non-trivial" eigenvalues always appear in the unit circle. Thus it is plausible to conjecture that the non-trivial eigenvalues lie there. It is known (Vaughan, On the eigenvalues of Redheffer's matrix, II, J. Austral. Math. Soc.(Series A) 60(1996), 260-273.) that there are a few eigenvalues very close to 1, but if it could be shown that most non-trivial eigenvalues λ satisfy $|\lambda| \le 1 - (\log n)^{-\theta}$ where $0 < \theta < 1$, then one would have a bound for $M(n)$ comparable to that obtained from the theory of the Riemann zeta function and indeed if $\theta < 2/5$, then it would be superior. However the best overall result that we have is only (Vaughan, On the eigenvalues of Redheffer's matrix, I, Proc. Conf. BYU May 1991, Marcel Dekker, 1993, 283-296) that the non-trivial eigenvalues satisfy $|\lambda| \ll (\log n)^{2/5}$.

10. (Browning) Let $r(n)$ denote the number of representations of n as a sum of two squares, and set $r_0(n) = 1$ if $r(n) > 0$, $r_0(n) = 0$ otherwise. Landau showed

that

$$\sum_{|z|\le B} r_0(z) \sim c\frac{B}{\sqrt{\log B}}\,.$$

Show that

$$\sum_{\substack{(x,y,z)\in\mathbb{Z}^3_{pnm}\\ |x|,|y|,|z|\le B\\ zy^2+yz^2=x^3-xz^2}} r_0(z) = o(\sqrt{\log B})\,.$$

The cubic equation defines an elliptic curve of rank 1 over the rationals. Is the left hand side actually bounded?

11. (Brandes) Let $\psi \in \mathbb{R}[t_1, t_2, \dots, t_m]$ be homogeneous, of degree d, and positive definite. Write

$$\psi(t) = \sum_{(j_1,j_2,\dots,j_d)} n_{(j_1,j_2,\dots,j_d)} t_{j_1} t_{j_2} \cdots t_{j_d}\,.$$

Is it true that every such form is equivalent (via a linear change of variables) to a form ψ' where

$$\left|n_{(j_1,j_2,\dots,j_d)}\right| \le \left|n_{(j_1,j_1\dots,j_1)} n_{(j_2,j_2,\dots,j_2)} \cdots n_{(j_d,j_d,\dots,j_d)}\right|^{1/d}?$$

12. (Bloom) Hardy showed that

$$\Lambda(n) = \frac{n}{\phi(n)} \sum_{q=1}^{\infty} \frac{\mu(q)}{\phi(q)} c_q(n)\,.$$

However, this expansion is not absolutely convergent. Does there exist a representation

$$\Lambda(n) = F(n) \sum_{q=1}^{\infty} G(q,n)$$

where $F(n)$ is multiplicative and $G(q,n)$ is a multiplicative function of q for every fixed n, with the sum absolutely convergent?

13. (Chow) Prove or disprove that if $\mathcal{A} = \{a_1 < a_2 < \cdots\}$, then the measure of the set of $\alpha \in [0,1]$ such that

$$\#\Big\{(n,m) : 1 \le n,m \le N, n \ne m, \|\alpha(a_n - a_m)\| \le \frac{s}{N}\Big\} \to 2s$$

as $N \to \infty$ is just 0 or 1?

14. (Hanson) Suppose that we have real numbers a_i with $1 < a_1 < a_2 < \cdots$. Consider the equation

$$a_{i_1} + a_{i_2} + \cdots + a_{i_k} = a_{j_1} + a_{j_2} + \cdots + a_{j_k}.$$

If

$$\frac{a_{n+1}}{a_n} > 1 + c,$$

then the sequence $\{a_n\}$ is lacunary and estimates for the number of solutions exist, although they are not uniform in c. If the ratios

$$a_{n+1}/a_n = 1 + c$$

are fixed, then we have a geometric progression and algebraic number theory can be used, uniformly in c. My question is, what can be said when these ratios are increasing?

15. (Klurman) Suppose that $\mathcal{A} \subseteq \{1, 2, \ldots, n\}$. We say that $\mathcal{A}$ is a *multiplicative Sidon set* if $ab = cd$ with $a, b, c, d \in \mathcal{A}$, then $\{a, b\} = \{c, d\}$.
(1) The primes have this property. How big can such a set be? See literature of Erdős, Pach, ...
(2) If $\mathcal{A}$ is an arbitrary set of integers in $[1, n]$ with $|\mathcal{A}| \asymp n$, does there necessarily exist a multiplicative Sidon set $\mathcal{B} \subseteq \mathcal{A}$ such that $\mathcal{B}$ is large?

Bounds in the polynomial Szemerédi theorem

Sarah Peluse

Szemerédi's theorem [11] on arithmetic progressions states that if $A \subset [N] := \{1, \ldots, N\}$ contains no nontrivial k-term arithmetic progressions

$$x, x + y, \ldots, x + (k-1)y; \qquad y \neq 0,$$

then $|A| = o_k(N)$. Bergelson and Leibman [1] showed that the conclusion of Szemerédi's theorem still holds when the linear polynomials $y, \ldots, (k-1)y$ are replaced by arbitrary polynomials $P_1, \ldots, P_k \in \mathbb{Z}[y]$ with zero constant term. In contrast to the situation for Szemerédi's theorem, for which Gowers has proven quantitative bounds [4, 5], no bounds are known in the polynomial Szemerédi theorem in general.

Until recently, beyond Gowers's result, which deals with the case of linear polynomial progressions, bounds were only known for sets lacking two-term polynomial progressions, for which Fourier analytic methods immediately apply, and for arithmetic progressions with common difference equal to a perfect power (due to Prendiville [10]), to which Gowers's method can be adapted to apply. It was essential for the success of the density increment arguments in [4] and [5] that k-term arithmetic progressions are preserved under translation and dilation, since the inverse theorems for the Gowers norms give a density increment on an arithmetic progression whose common difference can be much larger than the length of the progression. Similarly, k-term arithmetic progressions with common difference equal to a perfect d^{th} power are preserved under translation and dilation by a perfect d^{th} power. However, the vast majority of polynomial progressions do not behave so nicely under dilation (for example, consider the progression $x, x + y, x + y^2$), and so to handle more progressions, new strategies avoiding the use of the inverse theorems for the Gowers norms were needed.

Recently, significant progress has been made on the problem of proving a quantitative version of the polynomial Szemerédi theorem, beginning with work in the

finite field setting. Let S be $[N]$ or $\mathbb{F}_p$ and let $r_{P_1,\dots,P_m}(S)$ denote the size of the largest subset of S with no nontrivial (i.e., with $y \neq 0$) progressions of the form $x, x+P_1(y), \dots, x+P_m(y)$. Bourgain and Chang [2] proved that $r_{y,y^2}(\mathbb{F}_p) \ll p^{14/15}$. I [6] proved that $r_{P_1,P_2}(\mathbb{F}_p) \ll p^{23/24}$ whenever P_1 and P_2 are affine-linearly independent over $\mathbb{Q}$, and then Dong, Li, and Sawin [3] very shortly after and independently showed improved bounds, getting $r_{P_1,P_2}(\mathbb{F}_p) \ll_{P_1,P_2} p^{11/12}$. All three of our methods, though quite different, completely avoided the use of any inverse theorems for the Gowers norms. There were serious barriers to generalizing any of the arguments in [2, 6, 3] to the integer setting or to longer progressions in the finite field setting, however.

Inventing a different technique, which we now refer to as "degree-lowering", I [8] showed that $r_{P_1,\dots,P_m}(\mathbb{F}_p) \ll p^{1-\gamma_{P_1,\dots,P_m}}$ whenever $P_1, \dots, P_m$ are affine-linearly independent. The degree-lowering method did not appear to suffer from the same obvious barriers to generalization that the arguments in [2, 6, 3] had. Sean Prendiville and I successfully carried out an adaptation to the integer setting in [9], where we showed that $r_{y,y^2}([N]) \ll N/(\log\log N)^c$ for some $c > 0$. This adaptation was far from straightforward, since the integer setting has many challenges not present in the finite field setting. The most significant of these challenges was the need for a quantitative "concatenation" result that would bound an average of Gowers box norms appearing in our argument by a Gowers uniformity norm. The first concatenation results were shown by Tao and Ziegler [12], but their results were purely qualitative, having no effective bounds. In the course of proving $r_{y,y^2}([N]) \ll N/(\log\log N)^c$, we also proved a quantitative concatenation result for the average of Gowers box norms that arises from studying the progression $x, x+y, x+y^2$.

Following this, I [7] proved bounds for subsets of the integers lacking arbitrarily long nontrivial polynomial progressions having distinct degrees. Along the way, by proving a more general quantitative concatenation result, I showed that counts of any polynomial progression can be controlled by uniformity norms.

Theorem 1. *Let $P_1, \dots, P_m \in \mathbb{Z}[y]$ be polynomials of distinct degree such that $P_i(0) = 0$ for $i = 1, \dots, m$. If $A \subset [N]$ contains no nontrivial progressions of the form*

$$x, x + P_1(y), \dots, x + P_m(y),$$

then

$$|A| \ll \frac{N}{(\log\log N)^{c_{P_1,\dots,P_m}}},$$

where $c_{P_1,\dots,P_m} > 0$ is a constant depending only on $P_1, \dots, P_m$.

For example, this theorem gives bounds for subsets of $[N]$ lacking arbitrarily long shifted geometric progressions $x, x+y, x+y^2, \dots, x+y^{k-1}$.

References

[1] V. Bergelson and A. Leibman, Polynomial extensions of van der Waerden's and Szemerédi's theorems, J. Amer. Math. Soc. 9(3):725–753, 1996.
[2] J. Bourgain and M.-C. Chang, Nonlinear Roth type theorems in finite fields, Israel J. Math. Jul 2017.
[3] D. Dong, X. Li, and W. Sawin, Improved estimates for polynomial roth type theorems in finite fields, preprint, 2017, arXiv:1709.00080.
[4] W. T. Gowers, A new proof of Szemerédi's theorem for arithmetic progressions of length four, Geom. Funct. Anal. 8(1998), 529–551.
[5] W. T. Gowers, A new proof of Szemerédi's theorem, Geom. Funct. Anal. 11(2001), 465–588.
[6] S. Peluse, Three-term polynomial progressions in subsets of finite fields, Israel J. Math. 228(2018), 379–405.
[7] S. Peluse, Bounds for sets with no polynomial progressions, preprint, 2019, arXiv:1909.00309.
[8] S. Peluse, On the polynomial Szemerédi theorem in finite fields, Duke Math. J., 168(2019), 749–774.
[9] S. Peluse and S. Prendiville, Quantitative bounds in the non-linear Roth theorem, preprint, 2019, arXiv:1903.02592.
[10] S. Prendiville, Quantitative bounds in the polynomial Szemerédi theorem: the homogeneous case, Discrete Anal. (5), 2017.
[11] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, Acta Arith. 27(1975),199–245.
[12] T. Tao and T. Ziegler, Concatenation theorems for anti-Gowers-uniform functions and Host-Kra characteristic factors, Discrete Anal., Paper No. 13, 60, 2016.

Prime number theorem for Anzai skew products

Maksym Radziwiłł

(joint work with Adam Kanigowski, Mariusz Lemanczyk)

Given an irrational α and a real-analytic 1-periodic function g with mean zero consider the map $T_{\alpha,g} : \mathbb{T}^2 \to \mathbb{T}^2$ defined by

$$(x, y) \mapsto (x + \alpha, y + g(x)).$$

Such a transformation is known as an *Anzai skew product*. One thinks of $T_{\alpha,g}$ as a "random rotation": at the nth iteration $T_{\alpha,g}$ rotates the second co-ordinate of (x, y) by $g(\{n\alpha+x\})$, and $\{n\alpha+x\}$ can be considered as a source of "deterministic randomness". See [1, 2] for further properties.

Anzai skew-products have been investigated in the context of Sarnak's conjecture by Liu-Sarnak [5] and Zhiren Wang [4], who showed that for $f : \mathbb{T}^2 \to \mathbb{R}$ continuous and all $(x, y) \in \mathbb{T}^2$,

$$\sum_{n\le N} \mu(n) f(T^n_{\alpha,g}(x, y)) = o(N) \tag{1}$$

as $N \to \infty$. We establish a prime number theorem for $T_{\alpha,g}$.

Theorem 1. *Let α be an irrational real number. Let g be a real-analytic 1-periodic function with $\int_{\mathbb{T}} g(x)dx = 0$. Suppose that $T_{\alpha,g}$ is uniquely ergodic. Then, for every*

continuous $f : \mathbb{T}^2 \to \mathbb{R}$ *and for every* $(x, y) \in \mathbb{T}^2$, *as* $N \to \infty$,

$$\frac{1}{N} \sum_{p \le N} f(T^p_{\alpha,g}(x, y)) \to \int_{\mathbb{T}^2} f(\beta, \gamma) d\beta d\gamma \tag{2}$$

This is the first example of a (dynamical) prime number theorem that holds for a natural class of smooth dynamical systems that are neither algebraic nor symbolic.

We expect that unique ergodicity of $T_{\alpha,g}$ is also necessary for (2) to hold. We note that if $T_{\alpha,g}$ is uniquely ergodic then α is non-diophantine, that is for every fixed A there are only finitely many q such that $\|q\alpha\| > q^{-A}$.

The proof depends on a thorough understanding of the dynamical structure of the problem. The number theoretic content ends up being related to Huxley's prime number theorem in almost all short intervals and a recent result of Matomäki-Shao on polynomial phases over primes in short intervals. An interesting feature of the proof is that we need to address the contribution of certain type-III sums. While we do not know how to obtain cancellations in these type-III sums we can get away with a tight sieve upper bound for their contribution, following an idea of Heath-Brown [3].

Interestingly Theorem 1 cannot hold for g that are merely continuous. In fact we construct an example of $T_{\alpha,g}$ that is uniquely ergodic, for which Sarnak's conjecture holds, and for which Theorem 1 is false.

References

[1] H. Anzai, Ergodic skew product transformations on the torus, Osaka Math. J. 3(1951), 83–99.

[2] H. Furstenberg, Strict ergodicity and transformation of the torus, Amer. J. Math. 83(1961), 573–601.

[3] D. R. Heath-Brown, The number of primes in a short interval, J. Reine Angew. Math. 389(1988), 22–63.

[4] Z. Wang, Möbius disjointness for analytic skew products, Invent. Math. 209(2017), 175–196.

[5] J. Liu & P. Sarnak, The Möbius function and distal flows, Duke Math. J. 164(2015), 1353–1399.

Squarefrees in short intervals

Brad Rodgers

(joint work with Ofir Gorodetsky, Kaisa Matomäki, Maksym Radziwiłł)

We consider counts of squarefree integers in random short intervals and sparse arithmetic progressions and prove the following estimates for their variance.

Theorem 1. *For fixed* $\delta \in (0, 1/100)$, *let* $X \ge 1$ *and* $H \le X^{6/11-\delta}$ *such that* $H \to \infty$ *with* $X \to \infty$. *Then as* $X \to \infty$,

$$\frac{1}{X} \int_X^{2X} \Big| \sum_{x \le n \le x+H} \mu(n)^2 - \frac{1}{\zeta(2)} H \Big|^2 dx \sim C\sqrt{H}, \tag{1}$$

where C is a constant given by

$$C = \frac{\zeta(3/2)}{\pi} \prod_p \Big(1 - \frac{3}{p^2} + \frac{2}{p^3}\Big).$$

On the Riemann Hypothesis this result is true in the wider range $H \le X^{2/3-\delta}$.

Theorem 2. *For fixed $\delta \in (0, 1/100)$, let q be prime and $X \ge 1$ with $X^{5/11+\delta} \le q = o(X)$, and $X \to \infty$. Then as $X \to \infty$,*

$$\sum_{(a,q)=1} \Big| \sum_{\substack{n \le x \\ n \equiv a \bmod q}} \mu(n)^2 - \Big(\frac{1}{\zeta(2)} \frac{1}{1-q^{-2}}\Big) \frac{X}{q} \Big|^2 \sim C X^{1/2} q^{1/2},$$

where C is the same constant as above. On the Generalized Riemann Hypothesis, this result is true in the wider range $X^{1/3+\epsilon} \le q = o(X)$.

One should think of X/q as being analogous to H in these theorems. Theorem 1 improves an old result of R.R. Hall, while Theorem 2 improves recent results of R.M. Nunes and P. Le Boudec. Based on a function field result, J.P. Keating and Z. Rudnick had conjectured that Theorems 1 and 2 are true in the wider range $H \le X^{1-\delta}$ and $X^\delta \le q = o(X)$, and these results give evidence that this is the case.

The proofs depend upon on the decomposition $\mu(n)^2 = \sum_{md^2=n} \mu(d)$. Using this identity, averages like (1) can, roughly speaking, be broken up into averages

$$\frac{1}{X} \int_X^{2X} \Big| \sum_{\substack{x \le md^2 \le x+H \\ d^2 \sim \omega}} \mu(d) - H \sum_{d^2 \sim \omega} \frac{\mu(d)}{d^2} \Big|^2 dx,$$

where ω ranges dyadically in between 1 and x. For

$$H^{1+\epsilon} \le \omega \le \min(X/H^{1/2+\epsilon}, (HX)^{1/2-\epsilon})$$

an asymptotic formula can be found for this quantity by using Poisson summation (or an approximate functional equation) in m, along with bounds for the number of off-diagonal terms which can possibly arise. For $\omega \ge H^{4/3}$ one may show that these quantities are negligible by converting them into mean squares of Dirichlet polynomials and using various estimates for the Riemann zeta-function. For $H \le X^{6/11-\delta}$ this allows us to handle all ω which could possibly arise.

The proof of Theorem 2 is similar, though it involves overcoming a few additional technical obstacles. In addition to the Theorems recorded here, the same ideas yield a nearly correct upper bound for essentially the complete range H and q as long as one is willing to assume the Riemann Hypothesis or the Generalized Riemann Hypothesis. Progress on the range of H and q which are admissible in Theorems 1 and 2 occurred during and after the workshop, with new ideas being incorporated into the work.

Equal sums of three d^{th} powers

Per Salberger

We presented in our talk new upper bounds for the number of rational points of bounded height on threefolds and fourfolds.

Theorem 1 (Salberger 2019)**.** *Let $Z \subset \mathbb{P}^5$ be the non-singular fourfold defined by a form*

$$a_0x_0^d + a_1x_1^d + a_2x_2^d + a_3x_3^d + a_4x_4^d + a_5x_5^d$$

with rational non-zero coefficients and let $U \subset Z$ be the complement of all closed subsets given by equations

$$a_ix_i^d + a_jx_j^d = a_kx_k^d + a_kx_k^d = a_lx_l^d + a_mx_m^d = 0$$

with six different indices. Let $H : \mathbb{P}^5(\mathbb{Q}) \to \mathbb{N}$ be the naïve multiplicative height and $Z(\mathbb{Q}, B) = \{x \in Z(\mathbb{Q}) : H(x) \leq B\}$. Then

a) $\#Z(\mathbb{Q}, B) = O_Z(B^{7/2-\delta})$ for some $\delta > 0$ for $d \geq 5$.

b) $\#U(\mathbb{Q}, B) = O_Z(B^{3-\delta})$ for some $\delta > 0$ for $d \geq 11$.

In particular, if $n_d(B)$ is the number of solutions in positive integers $x_j \leq B$ of

$$x_0^d + x_1^d + x_2^d = x_3^d + x_4^d + x_5^d,$$

then $n_d(B) = O_d(B^{7/2-\delta})$ for $d \geq 5$ and $n_d(B) = 6B^3 + O_d(B^{3-\delta})$ for $d \geq 11$.

Our upper bounds are in fact more precise with exponents decreasing with d. They improve upon estimates of Browning and Heath-Brown in [2] where a) was shown for $d \geq 25$ and b) for $d \geq 33$ and on estimates in [3] where a) was shown for $d \geq 9$ and b) for $d \geq 25$. The proofs of these earlier bounds were based on estimates of $\#(U \cap \Lambda)(\mathbb{Q}, B)$ for linear spaces $\Lambda \subset \mathbb{P}^5$ of codimension two, which in turn were obtained by Heath-Brown's p-adic determinant method.

To prove theorem 1, we reduce to estimates of $\#(U \cap \Pi)(\mathbb{Q}, B)$ for hyperplanes $\Pi \subset \mathbb{P}^5$ of height $O(B^{1/5})$. It is then not hard to control the contribution from the singular hyperplane sections as they are relatively sparse. To handle the contribution from the non-singular hyperplane sections we use a version of the following theorem for integral points in lopsided boxes.

Theorem 2 (Salberger 2019)**.** *Let $X \subset \mathbb{P}^4$ be a non-singular threefold over $\mathbb{Q}$ of degree $d \geq 5$. Then all curves on X of degree $\delta \leq d-3$ lie on a surface W of degree bounded in terms of d and we have for $U = X - W$ that*

$$\#U\mathbb{Q}, B) = O_{d,\varepsilon}(B^{g(d)+\varepsilon})$$

with $g(d) = \max\big(3f(d), 3f(d) + g_1(d), 2f(d) + g_2(d)\big)$ for $f(d) = 4/3\sqrt[3]{d}$, $g_1(d) = \max_{\delta \geq d-2} \frac{2}{\delta} - \frac{f(d)}{\delta-(d-3)}$ and $g_2(d) = \max_{\delta \geq d-2} \frac{2}{\delta} - \frac{f(d)}{\delta-(d-3)}$.

To prove theorem 2, we use the semiglobal determinant method in [4] and the Noether-Lefschetz theorem to reduce to counting problems for curves on X. These counting problems are then solved by another use of the determinant method together with new results on covering gonality in [1].

References

[1] F.Bastianelli, P. DePoi, L. Ein, R. Lazarsfeld, B.Ullery : Measures of irrationality for hypersurfaces of large degree, Compos. Math. 153 (2017), 2368-2393.

[2] T.D.Browning, R.Heath-Brown: Equal sums of three powers hypersurfaces. Inv. Math. 157(2004), 553-573.

[3] P.Salberger: Counting rational points on hypersurfaces of low dimension, Ann. Sci. Éc. Norm. Sup. 38(2005), 93-115.

[4] P.Salberger: Uniform bounds for rational points on cubic hypersurfaces, in Arithmtic and and Geometry pp..401-21, London Math Soc. Lecture Notes Ser., vol 420, Cambridge University press, Cambridge 2015.

On the Chowla conjecture over $\mathbb{F}_q[T]$

Will Sawin

(joint work with Mark Shusterman)

We resolve two open problems in number theory, except with the ring of integers $\mathbb{Z}$ replaced by the ring of polynomials $\mathbb{F}_q[T]$, under suitable assumptions on q. We first fix some notation. Define the norm of a nonzero $f \in \mathbb{F}_q[T]$ to be

$$|f| = q^{\deg(f)} = |\mathbb{F}_q[T]/(f)|. \tag{1}$$

The degree of the zero polynomial is negative ∞, so we set its norm to be 0. Our first main result covers the twin prime conjecture in its quantitative form. The latter is the 2-point prime tuple conjecture of Hardy-Littlewood, predicting for a nonzero integer h that

$$\#\{X \leq n \leq 2X : n \text{ and } n+h \text{ are prime}\} \sim \mathfrak{S}(h)\frac{X}{\log^2(X)}, \quad X \to \infty, \tag{2}$$

where

$$\mathfrak{S}(h) = \prod_p (1-p^{-1})^{-2}(1-p^{-1}-p^{-1}\mathbf{1}_{p\nmid h}), \tag{3}$$

with $\mathbf{1}_{p\nmid h}$ equals 1 if h is not divisible by p, and 0 otherwise.

For the function field analogue, we set

$$\mathfrak{S}_q(h) = \prod_P \left(1-|P|^{-1}\right)^{-2}\left(1-|P|^{-1}-|P|^{-1}\mathbf{1}_{P\nmid h}\right) \tag{4}$$

where q is a prime power, P ranges over all primes (monic irreducibles) of $\mathbb{F}_q[T]$, and $h \in \mathbb{F}_q[T]$ is nonzero.

Theorem 1. *For an odd prime number p, and a power q of p satisfying $q > 685090p^2$, the following holds. For any nonzero $h \in \mathbb{F}_q[T]$ we have*

$$\#\{f \in \mathbb{F}_q[T] : |f| = X, f \text{ and } f+h \text{ are prime}\} \sim \mathfrak{S}_q(h)\frac{X}{\log_q^2(X)} \tag{5}$$

as $X \to \infty$ through powers of q. Moreover, we have a power saving (depending on q) in the asymptotic above.

For example, the 2-point Hardy-Littlewood conjecture holds over

$$\mathbb{F}_{3^{15}}, \mathbb{F}_{5^{11}}, \mathbb{F}_{7^9}, \mathbb{F}_{11^8}, \mathbb{F}_{685093^3}. \tag{6}$$

For h a constant, the fact that the count above tends to ∞ was proven in [Hal06, Corollary 14] for $q > 3$ and in [Pol08]. This has been extended to monomial h (assuming $q > 105$) in [CHLPT15, Theorem 1.3] using an idea of Entin. The latter work builds on the recent dramatic progress on this problem over the integers, particularly [Ma15]. The strongest result known over the integers is [PM14, Theorem 16(i)], which says that for any 'admissible tuple' of 50 integers, there exists at least one difference h between two elements in the tuple such that there are infinitely many pairs of primes separated by h.

Our proof of Theorem 1 establishes also the analog of the Goldbach problem over function fields, and can be modified to treat more general linear forms in the primes. Our second main result, and the key ingredient in the proof of Theorem 1 is the proof of Chowla's k-point correlation conjecture over $\mathbb{F}_q[T]$ for some prime powers q. Over the integers, this conjecture predicts that for any fixed distinct integers $h_1, \dots, h_k$, one has

$$\sum_{n \le X} \mu(n+h_1)\mu(n+h_2)\cdots\mu(n+h_k) = o(X), \quad X \to \infty. \tag{7}$$

The only completely resolved case is $k = 1$ which is essentially equivalent to the prime number theorem.

For the function field analogue, we recall that the Möbius function of a monic polynomial f is 0 if f is not squarefree, and is otherwise given by

$$\mu(f) = \begin{cases} 1, & \#\{P : P \mid f\} \equiv 0 \bmod 2 \\ -1, & \#\{P : P \mid f\} \equiv 1 \bmod 2. \end{cases} \tag{8}$$

We denote by $\mathbb{F}_q[T]^+$ the set of monic polynomials over $\mathbb{F}_q$.

Theorem 2. *For an odd prime number p, an integer $k \ge 1$, and a power q of p satisfying $q > p^2k^2e^2$, the following holds. For distinct $h_1, \dots, h_k \in \mathbb{F}_q[T]$ we have*

$$\sum_{\substack{f \in \mathbb{F}_q[T]^+ \\ |f| \le X}} \mu(f+h_1)\mu(f+h_2)\cdots\mu(f+h_k) = o(X), \quad X \to \infty. \tag{9}$$

In fact, we obtain a power saving inversely proportional to p, and the shifts $h_1, \dots, h_k$ can be as large as any fixed power of X (the corresponding assumption on q becomes stronger as this power grows larger).

Over the integers, the $k = 2$ case of the Chowla conjecture, with logarithmic averaging, was proven in [Tao16, Theorem 3], building on earlier breakthrough work of Matomäki and Radziwiłł [MR16]. The k odd case, again with logarithmic averaging, was handled by Tao and Teräväinen [TT19]. Generalizations of some of these arguments to the function field setting are part of a work in progress by Klurman, Mangerel, and Teräväinen, discussed elsewhere in this report.

The proof of Theorem 2 relies on two key observations which are far from traditional analytic number theory, which are then used in an argument which is

very reminiscent of classical analytic number theory techniques. The first observation is that the Möbius function, when composed with the polynomial function $s \mapsto as^p + b$ (with a, b fixed), becomes a (shifted) quadratic Dirichlet character in s, with modulus $ab' - b'a$ (taking here the polynomial derivative). This relies on elementary algebra involving polynomial discriminants and resultants. The second observation is a very strong Burgess-type bound for multiplicative character sums to squarefree moduli over function fields. The traditional Burgess's bound is proved by combining algebraic geometry (Weil's bound) with an elementary analytic argument. Because a short interval over a function field is a high-dimensional vector space over a finite field, our bound can be proven using a purely geometric method. This leads to a stronger estimate, but requires the full strength of Deligne's second proof of the Weil conjectures as well as some vanishing cycles arguments.

Combining these, our strategy is to restrict the sum to subsets of the form $as^p + b$, and show cancellation in the sum over s for almost all a and b. This uses the Chinese remainder theorem to show a product of many Dirichlet characters is a single Dirichlet character to a larger modulus, as long as the moduli of the Dirichlet characters do not share common factors. Handling the common factors requires us to bound how often large common factors appear with a sieve-like argument. This sieve is efficient enough that one can get bounds essentially as strong as would be obtained if common factors never appeared (which in fact happens for special values of the shifts h).

Once a uniform variant of Theorem 2 (for $k = 2$) is established, Theorem 1 follows from arguments similar to those in [MV17]. These involve a convolution identity relating the von Mangoldt function, which can be used to count primes, to the Möbius function. This convolution identity produces a more complicated sum which can be decomposed into many different ranges. Some ranges may be handled by elementary methods (these contribute the main term), some require a uniform $k = 1$ case of Theorem 2, and some require a uniform $k = 2$ version of Theorem 2. However, there is a critical range where Theorem 2 does not apply. In this range, we are able to get power savings using a function field analogue of a result from [FM98], which we have also modified to sum over Möbius and not primes and to handle squarefree moduli and not prime moduli.

References

[Hal06] C. Hall (2006), L-functions with twisted Legendre curves, J. of Number Theory, 119, 128-147.

[Pol08] P. Pollack, An explicit approach to Hypothesis H for polynomials over a finite field, in Anatomy of integers, CRM Proc. Lecture Notes 46, 259–273. Amer. Math. Soc., Providence, RI, 2008.

[CHLPT15] A. Castillo, C. Hall, R. Lemke Oliver, P. Pollack, L. Thompson, (2015) Bounded gaps between primes in number fields and function fields, Proc. Amer. Math. Soc.143(7), 2841-2856.

[FM98] E. Fouvry, P. Michel, Sur certaines sommes d'exponentielles sur les nombres premiers, Ann. scient. Ec. Norm. Sup., 4e serie, t. 31, 1998, 93-130.

[Ma15] J. Maynard (2015), Small gaps between primes, Ann. Math. 181, 1-31.

[MR16] K. Matomäki, M. Radziwiłł (2016), Multiplicative functions in short intervals, Ann. Math 1015-1056.
[MV17] R. Murty, A. Vatwani (2017), Twin primes and the parity problem, J. Number Theory, 180, 643-659.
[PM14] Polymath, D. H. J. (2014), Variants of the Selberg sieve, and bounded intervals containing many primes, Res. Math. sci. 1(1), 12.
[Tao16] T. Tao, The logarithmically averaged Chowla and Elliott conjectures for two-point correlations, Forum of Mathematics, Pi, Vol 4, 2016, e8, Cambridge University Press.
[TT19] T. Tao, J. Teräväinen (2019), The structure of logarithmically averaged correlations of multiplicative functions, with applications to the Chowla and Elliott conjectures, Duke Math. J. 168(11), 1977-2077.

A toy problem in multiplicative chaos

Kannan Soundararajan
(joint work with Asif Zaman)

I report on joint work (in progress) with Asif Zaman which is aimed at understanding recent progress on random multiplicative functions as well as the distribution of the Riemann zeta-function in intervals of length 1 on the critical line. There has been a lot of progress in recent years (see [1, 2, 3]) on such questions, especially through the work of Harper, and our goal is to give a setting in which these ideas appear without technical difficulties.

The toy problem is as follows. Recall that a standard complex Gaussian random variable Z is of the form $X + iY$ where X and Y are independent real Gaussians with mean 0 and variance $1/2$. Equivalently the complex Gaussian Z is characterized by the moments (for non-negative integers m and n)

$$\mathbb{E}\Big[Z^m \overline{Z}^n\Big] = \begin{cases} n! & \text{if } m = n \\ 0 & \text{otherwise.} \end{cases}$$

For each natural number n let $X(n)$ denote a standard complex Gaussian random variable, with $X(n)$ chosen independently for each natural number n. Form the random power series

$$g(z) = \sum_{n=1}^{\infty} \frac{X(n)}{\sqrt{n}} z^n,$$

which converges almost surely for $|z| < 1$, but diverges almost surely on the unit circle $|z| = 1$. For non-negative integers $N \geq 0$ define random variables $a(N)$ by setting

$$f(z) = \exp(g(z)) = \sum_{N=0}^{\infty} a(N) z^N.$$

Theorem 1. *With these notations*

$$\mathbb{E}[|a(N)|^2] = 1,$$

but for large N one has

$$\mathbb{E}[|a(N)|] \asymp (\log N)^{-\frac{1}{4}}.$$

The random variable $a(N)$ may be expressed in terms of the variables $X(k)$ by the formula

$$a(N) = \sum_{\substack{k\geq 1\\ m_k\geq 0\\ \sum km_k=N}} \prod_k \Big(\frac{X(k)}{\sqrt{k}}\Big)^{m_k} \frac{1}{m_k!}$$

where the sum is over all partitions of N with the part k appearing m_k times. From this, and the independence of the variables $X(k)$, one sees that

$$\mathbb{E}[|a(N)|^2] = \sum_{\substack{k\geq 1\\ m_k\geq 0\\ \sum km_k=N}} \prod_k \frac{1}{k^{m_k} m_k!} = 1,$$

upon using the cycle-index formula. By Cauchy's inequality we must clearly have $\mathbb{E}[|a(N)|] \leq 1$, but the surprising fact is that the L^1–norm is even smaller, and indeed tends to zero as given in the theorem.

This toy problem arises if we consider random multiplicative functions in the "function field setting." Thus consider $\mathbb{F}_q[t]$ and a random completely multiplicative function $X(F)$ defined by picking $X(P)$ uniformly on the unit circle, independently for all monic irreducible polynomials P. Here one would like to understand the behavior of $\sum_{\deg(\mathrm{F})=\mathrm{N}} X(F)$ where the sum is over all monic polynomials F of degree N. Such a sum depends only on $\sum_{\deg(P)=n} X(P)$ for $n \in \mathbb{N}$. There are about q^n/n monic irreducibles of degree n, so that (at least for large n) $\sum X(P)$ behaves like a complex Gaussian with mean 0 and variance q^n/n. Since

$$\sum_{N=0}^{\infty} \sum_{\deg(F)=N} X(F) z^N = \prod_P (1 - X(P) z^{\deg(P)})^{-1} \approx \exp\Big(\sum_{n=1}^{\infty} \sum_{\deg(P)=n} X(P) z^n\Big),$$

we see that this problem is approximated by a scaled version of our toy problem.

All this is to model the behavior of random multiplicative functions in the integer setting. Choose independent random variables $X(p)$ distributed uniformly on the unit circle for prime numbers p, and use multiplicativity to define a random completely multiplicative function $X(n)$. From the definition clearly

$$\mathbb{E}\Big[\Big|\sum_{n\leq N} X(n)\Big|^2\Big] = N,$$

but, answering a conjecture of Helson, Harper has established that

$$\mathbb{E}\Big[\Big|\sum_{n\leq N} X(n)\Big|\Big] \asymp \frac{\sqrt{N}}{(\log\log N)^{\frac{1}{4}}}.$$

Our theorem is an analogue of this result, and builds upon the ideas of Harper [2] with some simplifications.

References

[1] L-P. Arguin, D. Belius, P. Bourgade, M. Radziwiłł and K. Soundararajan, Maximum of the Riemann zeta function on a short interval of the critical line, Comm. Pure Appl. Math. **72** (2019), 500–535.

[2] A. Harper, Moments of random multiplicative functions, I: Low moments, better than squareroot cancellation, and critical multiplicative chaos, Forum of Math., Pi, to appear; preprint `arXiv:1703:06654`.

[3] A. Harper, On the partition function of the Riemann zeta function, and the Fyodorov–Hiary–Keating conjecture, preprint `arXiv:1906.05783`.

Multiplicative functions in short arithmetic progressions

Joni Teräväinen

Let $f : \mathbb{N} \to \mathbb{U}$ be a multiplicative function, with $\mathbb{U}$ the unit disc of the complex plane. Sums of multiplicative functions over arithmetic progressions of the form

$$\sum_{\substack{n\leq x\\ n\equiv a \pmod q}} f(n) \tag{1}$$

have attracted a lot of interest, in particular in the case of the Möbius function $f(n) = \mu(n)$. For the Möbius function, the problem of estimating (1) is related to the corresponding problem of primes in short intervals, and in particular we have analogues of the classical theorems of Linnik, Bombieri–Vinogradov and Barban–Davenport–Halberstam for the Möbius function. Linnik's theorem handles sums of the Möbius function in arithmetic progressions for $q \leq x^{\varepsilon}$ (for all a, q, with possible secondary main terms from Siegel zeros), the Bombieri–Vinogradov theorem handles the range $q \leq x^{1/2}/(\log x)^A$ (for all a and almost all q), and the Barban–Davenport–Halberstam theorem in turn handles the range $q \leq x/(\log x)^A$ (for almost all a and almost all q). In this talk, we are interested in the regime $x^{1-\varepsilon} \leq q \leq x$ where the arithmetic progression $\{n \leq x : \ n \equiv a \pmod q\}$ is very short, and in particular we simultaneously strengthen and generalize the result of Barban, Davenport and Halberstam for multiplicative functions.

For more general multiplicative functions $f : \mathbb{N} \to \mathbb{U}$, Hooley [1] proved (as a part of a long series of papers on the topic) a Barban–Davenport–Halberstam -type theorem that works in the full range $q = o(x)$; see also [4]. This theorem roughly speaking shows that if $H = H(x)$ is any function tending to infinity with x, we have the variance estimate

$$\sum_{a \pmod q}^{*} \left| \sum_{\substack{n\leq x\\ n\equiv a \pmod q}} f(n) - \frac{\chi_1(a)}{\phi(q)} \sum_{n\leq x} f(n)\overline{\chi_1}(n) \right| = o(\phi(q)\frac{x^2}{q^2}) \tag{2}$$

for all $q \leq x/H$ apart from $\ll x/H^2$ exceptional q, with χ_1 being the character (mod q) for which $|\sum_{n\leq x} f(n)\overline{\chi}(n)|$ is the largest (Hooley actually restricted to functions f satisfying the Siegel–Walfisz criterion, so that χ can be taken to be the principal character).

The exceptional set of q in Hooley's result becomes very weak when H is slowly growing, say $H = (\log x)^{\varepsilon}$. In this talk, I discuss a new result [2], joint with O. Klurman and A. P. Mangerel, which improves the exceptional set of q in (2) to a nearly power-saving one, even for q very close to x. Roughly speaking, if we replace $= o(\phi(q)x^2/q^2)$ in (2) with $\leq \varepsilon\phi(q)x^2/q^2$ for $\varepsilon = \varepsilon(x) \in ((\log(x/Q))^{-1/200}, 1)$, then the set of exceptional $q \leq Q$ is shown to be $\ll Qx^{-\varepsilon^{200}}$. We further show that assuming GRH (or a weak version of it) the set of exceptional q is empty, and that for prime moduli q it is $\ll (\log x)^{\varepsilon^{-200}}$.

The result as well as its proof can be viewed as a q-analogue of the Matomäki–Radziwiłł theorem on multiplicative functions in short intervals from [3]. However, we also encounter some further technical obstacles in the proof coming from the fact that there are no unconditional bounds for character sums $\sum_{p\leq y}\chi(p)$ (unlike for Dirichlet polynomials) when the conductor q of χ is y^A for large A. We overcome these obstacles via zero-density estimates, the pretentious large sieve, and bounds for $L(1,\chi)$. As a result, we in fact obtain a hybrid version of the Matomäki–Radziwiłł theorem that works for sums over short intervals and arithmetic progressions simultaneously.

As an application of the method, we also consider in [2] the analogue of Linnik's theorem on the least prime in an arithmetic progression for the least E_3-number (that is, a product of exactly 3 primes) in an arithmetic progression $a \pmod q$. We show that the least E_3-number in this progression is bounded by $\ll q^{2+\varepsilon}$ for $(a,q) = 1$ and for q smooth in the sense that $p \mid q$ implies $p \leq q^{\varepsilon'}$. The exponent $2+\varepsilon$ is the same that would follow for the ordinary Linnik problem assuming GRH.

References

[1] C. Hooley, On the Barban-Davenport-Halberstam theorem. IX, Acta Arith. **83** (1998), no. 1, 17–30.

[2] O. Klurman, A. P. Mangerel and J. Teräväinen, Multiplicative functions in short arithmetic progressions, preprint. `arXiv:1909.12280`

[3] K. Matomäki and M. Radziwiłł, Multiplicative functions in short intervals, Ann. of Math. (2), **183** (2016), no. 3, 1015–1056.

[4] R. C. Vaughan, On a variance associated with the distribution of general sequences in arithmetic progressions. II, R. Soc. Lond. Philos. Trans. Ser. A Math. Phys. Eng. Sci. **356** (1998), no. 1738, 793–809.

Counting and effective rigidity in algebra and geometry

Lola Thompson

(joint work with Benjamin Linowitz, D. B. McReynolds, Paul Pollack)

In this report, we present several applications of ideas from analytic number theory to quantitative questions about objects from spectral geometry. The objects that we will be interested in studying are geodesics on hyperbolic 2- and 3-manifolds.

Two manifolds are said to be *commensurable* if they have a common finite degree covering space. Commensurability is an equivalence relation, partitioning manifolds into commensurability classes.

In 1992, Reid [6] posed the question of whether hyperbolic 2- and 3-manifolds with the same geodesic length spectra are necessarily commensurable. He subsequently answered this question affirmatively in the arithmetic setting (note that the 3-manifold version is due to Chinberg, Hamilton, Long, and Reid [1]); the non-arithmetic case remains open. In a 2018 paper [3], we give an effective version of Reid's results, showing that, if the geodesic lengths agree up to a certain bound, then a pair of arithmetic hyperbolic 2- or 3-manifolds are necessarily commensurable. In particular, there exists a nonnegative real number $\mathrm{L}(V)$ such that, if M and N are arithmetic 2- or 3-manifolds of volume at most V and have the same geodesic lengths up to $\mathrm{L}(V)$, then M and N are commensurable. We produce the following upper bounds for $L(V)$:

Theorem 1. *If M and N are arithmetic hyperbolic surfaces of area at most V then*

$$L(V) \leq c_1 e^{c_2 \log(V) V^{130}}$$

for absolute, effectively computable constants c_1 and c_2. If M and N are arithmetic hyperbolic 3-manifolds of volume at most V then

$$L(V) \leq c_3 e^{\log(V)^{\log(V)}}$$

where c_3 is an absolute, effectively computable constant.

Our result is the first to deduce commensurability from a known finite part of the geodesic length spectrum. Note that, as of this writing, the best lower bounds for $L(V)$ come from a construction of Futer and Millichap [2] that produces examples of non-commensurable non-arithmetic hyperbolic 2- and 3-manifolds that share the same geodesic lengths for the first n lengths out of any finite subset of lengths. The lower bounds for $L(V)$ that can be deduced from their construction grow linearly in V. So, at this point we can only conclude that the growth rate of $L(V)$ is somewhere between linear and super-polynomial. It is likely that Futer and Millichap's construction is missing many examples, and that the lower bound should be a great deal larger, but it is also unclear whether our upper bound is anywhere close to the truth.

In contrast to Theorem 1, we also show in [3] that there are lots of pairwise non-commensurable arithmetic hyperbolic 2-manifolds with a great deal of overlap in their geodesic lengths. We are able to count, for instance, the number of commensurability classes of arithmetic hyperbolic 2- and 3-manifolds with volume less than V which contain closed geodesics of any fixed finite set S of prescribed lengths (say, $S = \{\ell_1, \ldots, \ell_n\}$). We show that there are, very roughly, $V/\log V$ of them. More precisely, we prove:

Theorem 2. *Let $\pi(V, S)$ denote the maximum cardinality of a collection of pairwise non-commensurable arithmetic hyperbolic 2-orbifolds (or, respectively, 3-orbifolds) derived from quaternion algebras, each of which has volume less than V and*

geodesic length spectrum containing S. If $\pi(V,S) \to \infty$ as $V \to \infty$, then there are integers $1 \leq r, s \leq |S|$ and constants $c_1, c_2 > 0$ such that

$$\frac{c_1 V}{\log(V)^{1-\frac{1}{2^r}}} \leq \pi(V,S) \leq \frac{c_2 V}{\log(V)^{1-\frac{1}{2^s}}}$$

for all sufficiently large V.

One might wonder if the volumes of these orbifolds are getting farther and farther apart. In [4], we show that the answer is "no." In fact, we produce infinitely many k-tuples of these orbifolds with volumes lying in an interval of bounded length!

Theorem 3. *Let $\pi(V,S)$ be as in Theorem 2. Then, for every $k \geq 2$, there is a constant $C > 0$ such that there are infinitely many k–tuples $M_1, \ldots, M_k$ of arithmetic hyperbolic 2–orbifolds (or, respectively, 3-orbifolds) which are pairwise non-commensurable, have length spectra containing S, and volumes satisfying $|\mathrm{vol}(M_i) - \mathrm{vol}(M_j)| < C$ for all $1 \leq i, j \leq k$.*

Where does analytic number theory enter the picture? It turns out that there is a correspondence between quadratic extensions of a number field K which embed into a quaternion algebra and closed geodesics on the associated arithmetic manifolds. We can use this correspondence to translate our geometric questions into questions about counting quaternion algebras. In [3], we obtain, for any fixed number field K, integer $n \geq 2$, and prime ℓ, an asymptotic for the number of central division algebras of dimension n^2 over K for which ℓ is the smallest prime divisor of n. We also consider variants in which we count (by discriminant) higher dimensional central simple algebras or, in the quaternionic case, the number of quadratic extensions of a fixed number field with bounded discriminant which embed into a fixed quaternion algebra over that number field. In each case, we obtain an asymptotic by constructing a Dirichlet series whose coefficients count the algebras that we are interested in, and then compute the partial sums of the coefficients using a Tauberian theorem.

As commensurability classes of hyperbolic 2- and 3-manifolds are in one-to-one correspondence with quaternion algebras defined over number fields satisfying certain ramification conditions, we can use our asymptotic for the number of central division algebras of dimension n^2 over K, along with a formula for the volume of an arithmetic hyperbolic manifold, to count commensurability classes of arithmetic manifolds containing a representative with volume less than V. Similarly, if we want to count the number of commensurability classes of arithmetic hyperbolic 2- or 3-manifolds (derived from quaternion algebras) with bounded volume which contain geodesic lengths $\ell_1, ..., \ell_n$, it suffices to count the number of quaternion algebras with bounded discriminant over a number field K which admit embeddings of the corresponding quadratic extensions $L_1, ..., L_n$ of K.

Analytic number theory is also useful in our aforementioned "bounded gaps between volumes of orbifolds" result. Borel's covolume formula gives an explicit formula for the volume of an arithmetic hyperbolic 2- or 3-orbifold. The formula depends on two parameters: its field of definition and the (norms of the) primes at

which the quaternion algebra ramifies. This means that, if two orbifolds have the same field of definition but their associated quaternion algebras ramify at different primes, then their volumes will differ by some function of the norm of the primes that ramify. So, primes with bounded gaps between them produce orbifolds with volumes lying in bounded length intervals. Recall that we want these orbifolds to have length spectra containing prescribed geodesic lengths $\ell_1, ..., \ell_n$. This will happen if and only if the corresponding quadratic extensions $L_1, ..., L_n$ of K embed into the quaternion algebras. One can arrange this by choosing primes (ramifying in the quaternion algebras) that lie in certain appropriately-chosen Chebotarev sets. Consequently, our problem of producing bounded gaps between volumes of certain orbifolds reduces to showing that there are bounded gaps between primes in Chebotarev sets. We accomplish this by generalizing the work of Thorner [7], who obtained such a result for Chebotarev sets where the corresponding Galois group is defined over $\mathbb{Q}$. We show that his result can be extended to Chebotarev sets with Galois groups defined over any number field. All of these results on Chebotarev sets rely crucially on the seminal work of Maynard [5] and Tao on small gaps between primes.

In this report, we have seen several examples of quantitative results in spectral geometry that have been obtained using tools from analytic number theory. Indeed, there are already many interesting papers in the spectral geometry literature that rely heavily on number theoretic ideas. This begs the question: are there interesting number theoretic results that one can prove using tools from spectral geometry?

References

[1] T. Chinburg, E. Hamilton, D. D. Long, A. W. Reid, Geodesics and commensurability classes of arithmetic hyperbolic 3-manifolds, Duke Math. J. 145 (2008), 25–44.

[2] D. Futer and C. Millichap, Spectrally similar incommensurable 3-manifolds, Proc. London Math. Soc. (3)115 (2017), 411–447.

[3] B. Linowitz, D. B. McReynolds, P. Pollack, and L. Thompson, Counting and effective rigidity in algebra and geometry, Invent. Math. 213 (2018), 697 – 758.

[4] B. Linowitz, D. B. McReynolds, P. Pollack, and L. Thompson, Bounded gaps between primes and the length spectra of arithmetic hyperbolic 3-orbifolds, C. R. Math. Acad. Sci. Paris. 355 (2017), 1121–1126.

[5] J. Maynard, Small gaps between primes, Ann. Math. 181 (2015), 383 – 413.

[6] A. W. Reid, Isospectrality and commensurability of arithmetic hyperbolic 2- and 3-manifolds, Duke Math. J. 65, 215–228 (1992).

[7] J. Thorner, Bounded gaps between primes in Chebotarev sets, Res. Math. Sci. 1, no. 4 (2014).

On quadratic forms over restricted sets of integers

Lilu Zhao

We consider quadratic forms over restricted sets of integers. Let $f(x_1,\dots,x_n)\in\mathbb{Z}[x_1,\dots,x_n]$ be a quadratic form in $n\geqslant 9$ variables.

Our first result is as follows. The non-degenerate quadratic form $f(x_1,\dots,x_n)$ has zeros in prime variables provided that $f(x_1,\dots,x_n)$ has zeros over $\mathbb{U}_p$ for all p, where $\mathbb{U}_p$ denotes the set of p-adic units in $\mathbb{Z}_p$ for primes p and $\mathbb{U}_\infty=\mathbb{R}^+$. Indeed, we are able to establish the asymptotic formula for the number of solutions. We define

$$N_{f,t}(X)=\sum_{\substack{1\leqslant x_1,\dots,x_n\leqslant X\\ f(x_1,\dots,x_n)=t}}\prod_{j=1}^{n}\Lambda(x_j),$$

where $\Lambda(\cdot)$ is the von Mangoldt function.

We introduce the singular series $\mathfrak{S}(f,t)$ defined as

$$\mathfrak{S}(f,t)=\sum_{q=1}^{\infty}B_{f,t}(q),$$

where $B_{f,t}(q)$ is given by

$$B_{f,t}(q)=\frac{1}{\phi^n(q)}\sum_{\substack{a=1\\(a,q)=1}}^{q}e\Big(-\frac{at}{q}\Big)\sum_{\substack{1\leqslant\mathbf{h}\leqslant q\\(\mathbf{h},q)=1}}e\Big(f(\mathbf{h})\frac{a}{q}\Big).$$

We define the singular integral

$$\mathfrak{I}_{f,t}(X)=\int_{-\infty}^{\infty}\Big(\int_{[0,X]^n}e\big(\beta f(\mathbf{x})\big)d\mathbf{x}\Big)e(-t\beta)d\beta.$$

Theorem 1. *Suppose that $f(x_1,\dots,x_n)$ is non-degenerate with $n\geqslant 9$, and that K is an arbitrary large real number. Let $t\in\mathbb{Z}$. Then we have*

$$N_{f,t}(X)=\mathfrak{S}(f,t)\mathfrak{I}_{f,t}(X)+O(X^{n-2}\log^{-K}X),$$

where the implied constant depends on f and K.

The second result is to consider the translation invariant quadratic forms over dense subset of integers. Let $f(x_1,\dots,x_n)$ be a translation invariant quadratic form in $n\geqslant 9$ variables. Let $\mathcal{A}\subseteq\mathbb{N}$. Denote

$$\mathcal{A}(x)=|\{1\leqslant a\leqslant x:\ a\in\mathcal{A}\}|.$$

Theorem 2. *If f has only trivial solutions on $\mathcal{A}$, then $\mathcal{A}(x)\ll_f x(\log x)^{-c_f}$ for some constant $c_f>0$.*

This improves upon the result of Keil who proved if a translation invariant quadratic form in $n\geqslant 17$ variables has only trivial solutions in $\mathcal{A}$, then $\mathcal{A}(x)\ll_f x(\log\log x)^{-c}$ for some absolute constant $c>0$.

Indeed, for a wide class of translation invariant quadratic forms in $n \geqslant 9$ variables, we can obtain the density estimate $\mathcal{A}(x) \ll_f x(\log x)^{-c}$ for some absolute constant $c > 0$. To state the above result precisely, we introduce the definition of the *exceptional* symmetric square matrix. Let $A \in M_{n,n}(\mathbb{R})$ be a symmetric square matrix. We call A is *exceptional* if for some $1 \leqslant r \leqslant 4$, there exist $2r$ columns of A with rank at most r. For a quadratic form $f(\mathbf{x}) = \mathbf{x}^T A\mathbf{x}$, we say f is *exceptional* if the symmetric square matrix A is exceptional.

Theorem 3. *Let $f(x_1, \dots, x_n)$ be a translation invariant indefinite quadratic form in $n \geq 9$ variables. Suppose that f is not exceptional. If $f(x_1, \dots, x_n) = 0$ has only trivial solutions when the variables are restricted in $\mathcal{A} \subseteq \{1, 2, \dots, N\}$, then there exists an absolute constant $c > 0$ such that*

$$\mathcal{A}(x) \ll_f N(\log N)^{-c}.$$

To establish the above theorem, we need to develop the argument of partial diagonalization. This is based on works of Liu [3] and Keil [2].

If f is exceptional, then we turn to solve a system of translation invariant linear equations. We apply the method of Roth [4, 5] and Heath-Brown [1] on 3-term arithmetic progressions to establish the density estimate $\mathcal{A}(x) \ll_f N(\log N)^{-c_f}$, where the constant $c_f > 0$ may depend on the coefficients.

References

[1] D. R. Heath-Brown, Integer sets contaning no arithmetic progressions, J. London Math. Soc. (2)35(1987), 385–394.
[2] E. Keil, Translation invariant quadratic forms in dense sets, arXiv:1308.6680.
[3] J. Liu, Integral points on quadrics with prime coordinates, Monatsh. Math. 164(2011), 439–465.
[4] K. F. Roth, On certain sets of integers, J. London Math. Soc. 28(1953), 104–109.
[5] K. F. Roth, On certain sets of integers (II), J. London Math. Soc. 29(1954), 20–26.
[6] L. Zhao, The quadratic form in 9 prime variables, Nagoya Math. J. 223(2016), 21–65.
[7] L. Zhao, On translation invariant quadratic forms in dense sets, IMRN 4(2019), 961–1004.

Reporter: Robert C. Vaughan

Participants

Dr. Sandro Bettin
Dipartimento di Matematica
Università di Genova
Via Dodecaneso 35
16146 Genova
ITALY

Prof. Dr. Manjul Bhargava
Department of Mathematics
Princeton University
Fine Hall
Washington Road
Princeton, NJ 08544-1000
UNITED STATES

Dr. Kirsti Biggs
School of Mathematics
University of Bristol
Fry Building
Woodland Road
Bristol BS8 1UG
UNITED KINGDOM

Prof. Dr. Valentin Blomer
Mathematisches Institut
Universität Bonn
Endenicher Allee 60
53115 Bonn
GERMANY

Dr. Thomas Frederik Bloom
Department of Pure Mathematics
and Mathematical Statistics
University of Cambridge
Wilberforce Road
Cambridge CB3 0WB
UNITED KINGDOM

Dr. Jonathan W. Bober
School of Mathematics
University of Bristol
Fry Building
Woodland Road
Bristol BS8 1UG
UNITED KINGDOM

Dr. Julia Brandes
Department of Mathematics
Chalmers University of Technology
and University of Gothenburg
412 96 Göteborg
SWEDEN

Prof. Dr. Timothy D. Browning
Institute of Science and
Technology Austria (IST Austria)
Am Campus 1
3400 Klosterneuburg
AUSTRIA

Prof. Dr. Jörg Brüdern
Mathematisches Institut
Georg-August-Universität Göttingen
Bunsenstrasse 3-5
37073 Göttingen
GERMANY

Dr. Sam Chow
Mathematics Institute
University of Warwick
Gibbet Hill Road
Coventry CV4 7AL
UNITED KINGDOM

Prof. Dr. Brian Conrey
American Institute of Mathematics
600 E. Brokaw Road
San Jose, CA 95112
UNITED STATES

Prof. Dr. Régis De La Bretèche
UFR de Mathématiques
Université Paris Diderot
Bâtiment Sophie Germain
75205 Paris Cedex 13
FRANCE

Prof. Dr. Rainer Dietmann
Department of Mathematics
Royal Holloway
University of London
Egham, Surrey TW20 0EX
UNITED KINGDOM

Dr. Alexandra Florea
Department of Mathematics
Columbia University
2990 Broadway
New York NY 10027
UNITED STATES

Prof. Dr. Etienne Fouvry
Laboratoire de Mathématiques
Université Paris Sud (Paris XI)
Bâtiment 307
91405 Orsay Cedex
FRANCE

Dr. Christopher Frei
Department of Mathematics
The University of Manchester
Oxford Road
Manchester M13 9PL
UNITED KINGDOM

Prof. Dr. John B. Friedlander
Department of Mathematics
University of Toronto
Bahen Centre; Room 6290
40 St. George Street
Toronto ONT M5S 2E4
CANADA

Prof. Dr. Ayla R. Gafni
Department of Mathematics
University of Mississippi
P.O. Box 1848
University, MS 38677
UNITED STATES

Luca Ghidelli
Department of Mathematics and Statistics
University of Ottawa
140 Louis-Pasteur Street
Ottawa ON K1N 6N5
CANADA

Prof. Dr. Ben J. Green
Mathematical Institute
University of Oxford
Andrew Wiles Building
Radcliffe Observatory Quarter
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM

Lasse P. Grimmelt
Mathematisch Instituut
Universiteit Utrecht
Budapestlaan 6
P. O. Box 80.010
3508 TA Utrecht
NETHERLANDS

Dr. Brandon W. Hanson
Department of Mathematics
University of Georgia
624 Boyd
Athens, GA 30602
UNITED STATES

Prof. Dr. Roger Heath-Brown
Mathematical Institute
Oxford University
Andrew Wiles Building
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM

Prof. Dr. Harald A. Helfgott
Mathematisches Institut
Universität Göttingen
Bunsenstrasse 3-5
37073 Göttingen
GERMANY

Prof. Dr. Henryk Iwaniec
Department of Mathematics
Rutgers University
Hill Center, Busch Campus
110 Frelinghuysen Road
Piscataway, NJ 08854-8019
UNITED STATES

Prof. Dr. Jerzy Kaczorowski
Faculty of Mathematics and Computer Science
A. Mickiewicz University
ul. Umultowska 87
61-614 Poznań
POLAND

Dr. Oleksiy Klurman
Department of Mathematics
KTH Royal Institute of Technology
10044 Stockholm
SWEDEN

Prof. Dr. Dimitris Koukoulopoulos
Department of Mathematics and Statistics
University of Montreal
CP 6128, succ. Centre Ville
Montreal QC H3C 3J7
CANADA

Prof. Dr. Youness Lamzouri
INRIA Lorraine - IECN
Campus Scientifique
Université de Nancy 1
B.P. 239
54506 Vandoeuvre-lès-Nancy Cedex
FRANCE

Prof. Dr. Yu-Ru Liu
Department of Pure Mathematics
University of Waterloo
200 University Avenue West
Waterloo ON N2L 3G1
CANADA

Dr. Kaisa Matomäki
Department of Mathematics and Statistics
University of Turku
20014 University of Turku
FINLAND

Dr. James A. Maynard
Mathematical Institute
Oxford University
Andrew Wiles Building
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM

Prof. Dr. Micah B. Milinovich
Department of Mathematics
The University of Mississippi
P.O. Box 1848
University, MS 38677
UNITED STATES

Prof. Dr. Hugh L. Montgomery
Department of Mathematics
University of Michigan
530 Church Street
Ann Arbor, MI 48109-1043
UNITED STATES

Dr. Simon L. R. Myerson
Mathematisches Institut
Georg-August-Universität Göttingen
Bunsenstrasse 3-5
37073 Göttingen
GERMANY

Dr. Siddhi Pathak
Department of Mathematics
Penn State University
217 McAllister Building
State College PA 16802
UNITED STATES

Sarah Peluse
Mathematical Institute
University of Oxford
Andrew Wiles Building
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM

Prof. Alberto Perelli
Dipartimento di Matematica
Università di Genova
Via Dodecaneso 35
16146 Genova
ITALY

Prof. Dr. Lillian Beatrix Pierce
Department of Mathematics
Duke University
P.O.Box 90320
Durham, NC 27708-0320
UNITED STATES

Prof. Dr. Paul Pollack
Department of Mathematics
University of Georgia
Athens, GA 30602
UNITED STATES

Prof. Dr. Maksym Radziwill
Department of Mathematics
California Institute of Technology
Pasadena CA 91125
UNITED STATES

Dr. Brad Rodgers
Department of Mathematics and
Statistics
Queen's University
Jeffery Hall
Kingston ON K7L 3N6
CANADA

Prof. Dr. Per Salberger
Department of Mathematics
Chalmers University of Technology and
University of Gothenburg
412 96 Göteborg
SWEDEN

Dr. Will Sawin
Department of Mathematics
Columbia University
2990 Broadway
New York, NY 10027
UNITED STATES

Dr. Damaris Schindler
Mathematisch Instituut
Universiteit Utrecht
Hans Freudenthal Gebouw
Budapestlaan 6
3584 CD Utrecht
NETHERLANDS

Dr. George Shakan
Mathematical Institute
University of Oxford
Andrew Wiles Building
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM

Prof. Dr. Kannan Soundararajan
Department of Mathematics
Stanford University
Stanford, CA 94305-2125
UNITED STATES

Dr. Joni P. Teräväinen
Mathematical Institute
Oxford University
Andrew Wiles Building
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM

Prof. Dr. Lola Thompson
Mathematics Department
Oberlin College
173 W. Lorain Street
Oberlin OH 44074
UNITED STATES

Dr. Caroline L. Turnage-Butterbaugh
Department of Mathematics and Statistics
Carleton College
One North College Street
Northfield MN 57707
UNITED STATES

Prof. Dr. Robert C. Vaughan
Department of Mathematics
Pennsylvania State University
335 McAllister Building
University Park, PA 16802-6401
UNITED STATES

Prof. Dr. Trevor D. Wooley
Department of Mathematics
Purdue University
150 N. University Street
West Lafayette IN 47907-2067
UNITED STATES

Dr. Lilu Zhao
School of Mathematics
Shandong University
27 Shanda Nanlu
Jinan, Shandong 250 100
CHINA