Mathematisches Forschungsinstitut Oberwolfach

Report No. 53/2016

DOI: 10.4171/OWR/2016/53

Analytic Number Theory

Organised by
Jörg Brüdern, Göttingen
Hugh L. Montgomery, Ann Arbor
Robert C. Vaughan, State College
Trevor D. Wooley, Bristol

6 November – 12 November 2016

Abstract. Analytic number theory has flourished over the past few years, and this workshop brought together world leaders and young talent to discuss developments in various branches of the subject.

Mathematics Subject Classification (2010): 11xx.

Introduction by the Organisers

Analytic number theory is on the roll for quite some time now, with spectacular discoveries year after year. Thus, the timing was perfect for an exciting week, but the overload of talent and the vast activities in various subbranches of the field made it challenging to select an appropriate mix of participants. However, we feel that we could not have done better: during the workshop, we experienced a typical Oberwolfach atmosphere, open, collaborative and productive.

We tried to keep the schedule moderate, with ample time for work and discussion after lunch and in the evening. The programme included a round table discussion on recent advances with the circle method on Tuesday evening, and a problem session on Thursday evening. The problems posed are included at the end of this report.

Many important results have been announced during the week. Rather than making an attempt to highlight the truly outstanding contributions, we let the collection of abstracts speak for itself.

Finally, it is our great pleasure to record the warm-hearted hospitality and excellent support by the local staff during a great event.

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-1049268, "US Junior Oberwolfach Fellows".

Workshop: Analytic Number Theory

Table of Contents

Valentin Blomer
Epstein zeta-functions, subconvexity, and the purity conjecture 2979

Thomas Bloom (joint with Olof Sisak)
On Roth's theorem on arithmetic progressions 2980

Andriy Bondarenko, Kristian Seip
Extreme values of the Riemann zeta function 2981

Régis de la Bretèche (joint with Daniel Fiorilli)
Mean value and variance of arithmetical sequences using Vaughan-type major arcs approximation 2982

Tim Browning (joint with Efthymios Sofos)
Pairs of quadrics and Nair's theorem 2984

Alina-Carmen Cojocaru (joint with Árpád Tóth, José Felipe Voloch)
Squarefree orders for the reductions of an elliptic curve over a function field 2985

Brian Conrey (joint with Jon Keating)
Statistics of L-functions 2987

Rainer Dietmann
Systems of cubic forms 2989

Alexandra Florea
Moments of L–functions in function fields 2991

Étienne Fouvry (joint with V. Blomer, E. Kowalski, Ph. Michel, D. Milićević and W. Sawin)
Moments of L–functions at the central point 2992

Christopher Frei (joint with Daniel Loughran and Efthymios Sofos)
Divisor sums and rational points on conic bundle surfaces 2994

Brandon Hanson
Sums of squares and combinatorial geometry 2996

Adam J Harper
Character sums and point counting 2997

Roger Heath-Brown
Iteration of quadratic polynomials over finite fields 2998

Harald Andrés Helfgott
The sieve of Eratosthenes in less space 2999

Jerzy Kaczorowski, Alberto Perelli
New results on the Selberg class 3000

Dimitris Koukoulopoulos (joint with Andrew Granville and James Maynard)
Sieve weights and their smoothings 3001

Pierre Le Boudec
Height of rational points on random Fano varieties 3004

Robert J. Lemke Oliver (joint with Kannan Soundararajan)
Unexpected biases in the distribution of consecutive primes 3006

Oscar Marmon (joint with Pankaj Vishe)
Rational points on quartic hypersurfaces 3006

Kaisa Matomäki (joint with James Maynard and Xuancheng Shao)
Vinogradov's three primes theorem with primes from special sets 3008

James Maynard
Primes with restricted digits 3009

Micah B. Milinovich (joint with William Banks, Greg Martin, Nathan Ng)
Linear relations of zeros of the zeta function 3011

Simon L. Rydin Myerson
Real and rational system of forms 3013

Lillian B. Pierce (joint with M. M. Wood and C. Turnage-Butterbaugh)
On ℓ-torsion in class groups of number fields of arbitrary degree 3015

Paul Pollack (joint with Abbey Bourdon, Pete L. Clark)
Torsion of CM elliptic curves over number fields 3016

Maksym Radziwill (joint with Florin Boca)
Eigenvalues of the large sieve matrix 3017

Brad Rodgers
Arithmetic functions in short intervals and function field analogues 3017

Zeev Rudnick
Quantum chaos, eigenvalue statistics and the Fibonacci sequence 3019

Per Salberger
Counting rational points on cubic curves 3020

Kannan Soundararajan
Equidistribution of zeros of polynomials 3020

Problem session 3022

Abstracts

Epstein zeta-functions, subconvexity, and the purity conjecture

Valentin Blomer

Let Z be a symmetric, positive definite n-by-n matrix with real entries, and let Q be the associated quadratic form. The Epstein zeta-function associated with Z is given by

$$E(Z,s) = \sum_{\mathbf{x}\in\mathbb{Z}^n\setminus\{0\}} Q(\mathbf{x})^{-ns/2}.$$

As a function of s, it is a Dirichlet series with a functional equation relating s to $1-s$ with Gamma factor $\Gamma(ns/2)$, but no Euler product in general. As a function of Z, it is essentially a maximally degenerate Eisenstein series: the function $z \mapsto E(zz^\top, s)$ lives on $X_n := \mathrm{SL}_n(\mathbb{Z})\backslash\mathrm{SL}_n(\mathbb{R})/\mathrm{SO}_n(\mathbb{R})$ and is an eigenfunction of all invariant differential operators and all Hecke operators. In particular, its Laplace eigenvalue for $s = 1/2 + it$ is $\lambda(t) = \frac{1}{24}(n^3-n) + \frac{1}{2}n(n-1)t^2 \asymp 1 + t^2$.

The first result bounds $E(Z,s)$ on the critical line $s = 1/2 + it$ and provides, for arbitrary $n \geq 2$, a result that is better than what can be obtained from the functional equation by a convexity argument: we have the *subconvexity* bound

$$E(Z, 1/2 + it) \ll (1 + |t|)^{\frac{n}{4} - \delta_n + \varepsilon}$$

for any $\varepsilon > 0$, where $\delta_2 = 1/6$, $\delta_3 = 1/4$, $\delta_n = 1/2$ for $n \geq 4$, and the implied constant is uniform in Z as long as Z varies in a fixed compact domain. The proof uses results of Götze [Go].

The second result shows that the previous bound is best possible for $n \geq 4$: we have the lower bound

$$E(\mathrm{id}_n, 1/2 + it) = \Omega\left((1 + |t|)^{\frac{n}{4} - \frac{1}{2}}\right)$$

for $n \geq 4$. The proof starts with an application of Siegel's mass formula, and for odd n exploits the rich structure of multiple Dirichlet series.

Taken together, these bounds imply for fixed compact domain $\mathrm{id}_n \in \mathcal{D} \subseteq X_n$ the relation

$$\lim_{t\to\infty} \frac{\log \|E(., 1/2 + it)|_{\mathcal{D}}\|_\infty}{\log t^2} = \frac{n}{8} - \frac{1}{4} \tag{1}$$

for $n \geq 4$.

This can be interpreted in the context of Sarnak's purity conjecture [Sa]: if X is a compact, arithmetic, irreducible locally symmetric space and $\{f_j \mid j = 1, 2, \ldots\}$ is any L^2-normalized sequence of eigenfunctions for all Hecke operators and all invariant differential operators with Laplacian eigenvalue $\lambda_j \to \infty$, then

$$\text{accumulation points}\left\{\frac{\log \|f_j\|_\infty}{\log \lambda_j} \mid j = 1, 2, \ldots\right\} \subseteq \mathbb{Z}/4 \cap \left[0, \frac{\dim(X) - \mathrm{rank}(X)}{4}\right).$$

To the author's knowledge, no single accummulation point has been determined in any non-trivial example, but the conjecture is consistent with all known upper and lower bounds for sup-norms (see e.g. [RS]).

While the above example of Eisenstein series do not exactly meet the assumptions of Sarnak's purity conjecture (X_n is not compact and $E(.,1/2+it)$ is not L^2-integrable), the denominator 8 in (1) is an interesting feature that indicates that there may occur unexpected phenomena to be explored.

References

[Go] F. Götze, *Lattice point problems and values of quadratic forms*, Invent. Math. **157** (2004), 195–226

[RS] Z. Rudnick, P. Sarnak, *The behavior of eigenstates of arithmetic hyperbolic manifolds*, Comm. Math. Phys. **161** (1994), 195–213

[Sa] P. Sarnak, Letter to Morawetz `http://www.math.princeton.edu/sarnak`

On Roth's theorem on arithmetic progressions

Thomas Bloom

(joint work with Olof Sisak)

Let $r(N)$ denote the size of the largest subset of $\{1,\dots,N\}$ that contains no (non-trivial) three term arithmetic progression; that is, three numbers of the form $x, x+d, x+2d$ with $d \neq 0$, or, equivalently, a solution to $x+y-2z=0$ with $x \neq y$.

In 1953, answering a question of Erdős and Turán, Roth showed that $r(N) = o(N)$. In fact, introducing a stunning new variant on the circle method, he gave the quantitative estimate $r(N) \ll N/\log\log N$. This estimate has seen a succession of improvements, leading to the bound of $r(N) \ll N/\log N^{1-o(1)}$ due to Sanders, also achieved by the speaker via an alternative method.

In this talk we present a recent result, due to the speaker and Olof Sisask, that $r(N) \ll N/(\log N)^{1+c}$ for some absolute constant $c > 0$. In particular, for the first time the so-called 'log barrier' has been broken, allowing this statement to have implications for sets such as the primes on density grounds alone. It also gives the first non-trivial case of a conjecture of Erdős, that a set $A \subset \mathbb{Z}$ such that $\sum_{n\in A} \frac{1}{n} = \infty$ must contain arbitrarily long arithmetic progressions.

This result mirrors a 2010 result of Bateman and Katz, who obtained a similar bound of $3^n/n^{1+c}$ for the analogous problem over $\mathbb{F}_3^n$. This bound has recently seen a vast improvement by Ellenberg and Gijswijt, using the new polynomial method of Croot, Lev, and Pach, which so far has not been applicable to the integer setting.

The methods of Bateman and Katz, however, build directly on the classical density increment method initiated by Roth, and thus are more amenable to translation. Our proof follows a similar strategy to theirs, incorporating a number of refinements.

The main idea of Roth is, that if $A \subset \{1, \dots, N\}$ contains few arithmetic progressions, then it has increased density on some smaller Bohr set, and the argument can then be iterated until the density is sufficiently large. The increment comes from a careful analysis of the large spectrum, the set of large Fourier coefficients of the characteristic function of A. The goal is to find many such coefficients which have many additive relations between them, allowing for a large increase in density without reducing the size of the Bohr set too much.

The key advance of Bateman and Katz was to study the large spectrum using combinatorial methods; in particular, showing that either the spectrum has an unusual amount of additive energy, or else it has a structural decomposition.

Our proof builds on such ideas. We must first adapt the argument to the more technically forbidding realm of Bohr sets in the integers. We then give a more powerful structural result that is necessary in this setting, using entirely elementary arguments. Finally, we find a more efficient way to exploit the structure thus obtained – roughly speaking, we use elementary arguments to perform a lifting argument, showing that either the large spectrum itself is additively structured, or else there is a set of even larger Fourier coefficients which is additively structured. In either case, we obtain an efficient density increment which, when iterated, leads to the result.

Extreme values of the Riemann zeta function

Andriy Bondarenko, Kristian Seip

We presented the basic ideas used in the proof of the following theorem.

Theorem. *Let $0 < \beta < 1$ be given and let c be a positive number less than $\sqrt{\min(1/2, 1-\beta)}$. If T is sufficiently large, then there exists a t, $T^\beta \le t \le T$, such that*

$$\left|\zeta\Big(\frac{1}{2}+it\Big)\right| \ge \exp\left(c\sqrt{\frac{\log T \log\log\log T}{\log\log T}}\right).$$

The best lower estimate for extreme values of $|\zeta(1/2+it)|$ known previously was obtained in 2008 by Soundararajan [5] who proved that

$$\left|\zeta\Big(\frac{1}{2}+it\Big)\right| \ge \exp\left((1+o(1))\sqrt{\frac{\log T}{\log\log T}}\right)$$

holds for some t, $T \le t \le 2T$, if T is large enough. In 1977, Montgomery [4] had proved, assuming the Riemann Hypothesis, that there exist arbitrarily large t such that

$$\left|\zeta\Big(\frac{1}{2}+it\Big)\right| \gg \exp\left(c\sqrt{\frac{\log t}{\log\log t}}\right)$$

with $c = 1/20$. This result was proved unconditionally at the same time by Balasubramanian and Ramachandra with a larger value of c (see [1] and [5]).

The proof of Theorem 1 uses the resonance method introduced by Soundararajan [5]. The main new ingredient of the proof is a special multiplicative function associated with a large greatest common divisor (GCD) sum. The idea behind the construction of this function is inspired by our recent work [2]. In the latter paper, we found that there exists an absolute constant A less than 7 such that

$$\sum_{k,\ell=1}^{N} \frac{\gcd(n_k, n_\ell)}{\sqrt{n_k n_\ell}} \leq N \exp\left(A\sqrt{\frac{\log N \log\log\log N}{\log\log N}}\right) \tag{1}$$

for arbitrary integers $1 \leq n_1 < \cdots < n_N$ and N sufficiently large. We show in [3] that (1) is optimal in the sense that it does not hold if $A < 1$.

References

[1] R. Balasubramanian and K. Ramachandra, *On the frequency of Titchmarsh's phenomenon for $\zeta(s)$. III*, Proc. Indian Acad. Sci. Sect. A **86** (1977), 341–351.

[2] A. Bondarenko and K. Seip, *GCD sums and complete sets of square-free numbers*, Bull. London Math. Soc. **47** (2015), 29–41.

[3] A. Bondarenko and K. Seip, *Large GCD sums and extreme values of the Riemann zeta function*, Duke Math. J., to appear; arXiv:1507.05840.

[4] H. L. Montgomery, *Extreme values of the Riemann zeta function*, Comment. Math. Helv. **52** (1977), 511–518.

[5] K. Soundararajan, *Extreme values of zeta and L-functions*, Math. Ann. **342** (2008), 467–486.

Mean value and variance of arithmetical sequences using Vaughan-type major arcs approximation

Régis de la Bretèche

(joint work with Daniel Fiorilli)

In order to study the distribution of arithmetical sequences $\mathcal{A} = \{f(n)\}_{n\geq 1}$ in progressions of large moduli, we consider

$$\sum_{x/2N<q\leq x/N} \sum_{a=1}^{q} \Big(\sum_{\substack{a<n\leq x \\ n\equiv a \bmod q}} f(n) - E(x,q,a)\Big)^2,$$

where $E(x,q,a)$ is chosen so that

$$\sum_{x/2N<q\leq x/N} \Big(\sum_{\substack{a<n\leq x \\ n\equiv a \bmod q}} f(n) - E(x,q,a)\Big)$$

is small.

We will consider arithmetical sequences $\mathcal{A} = \{f(n)\}_{n\geq 1}$ satisfying two hypotheses. The first is analogous to a standard sieve hypothesis, and the second describes the equidistribution of $\mathcal{A}$ in arithmetic progressions.

1 — There exists an integer $J \geq 0$, arithmetical functions h_j and monotonic smooth functions $u_j : \mathbb{R}_{\geq 0} \to \mathbb{R}$ with $0 \leq j < J$ such that uniformly for $1 \leq d \leq x$ we have

$$\mathcal{A}_d(x) := \sum_{\substack{n \leq x \\ d \mid n}} f(n) = \sum_{0 \leq j < J} \frac{h_j(d)}{d} U_j(x) + O\left(\frac{U_0(x)}{L(x)(\log Q(x))^2}\right),$$

where $U_j(x) := \int_0^x u_j$.

2 — For $x \geq 1$ we have the bound

$$\sum_{q \leq Q(x)} \max_{y \leq x} \max_{1 \leq a \leq q} \Big| \sum_{\substack{n \leq y \\ n \equiv a \bmod q}} f(n) - \frac{1}{\phi(q/(q,a))} \sum_{\substack{n \leq y \\ (n,q) = (a,q)}} f(n) \Big| \ll \frac{U_0(x)}{L(x)}.$$

These hypotheses are satisfied by Λ [1], μ [3], τ_k the k iterated divisor functions, to name a few. The approximation $E(x, q, a)$ will be determined in terms of the data in the first hypothesis. In order to do so, we extract the major arcs from a heuristic application of the circle method. The resulting expression is

$$F_R(n) := \sum_{0 \leq j < J} u_j(n) \sum_{r \leq R} \frac{(h_j * \mu)(r)}{\phi(r/(r,n))} \mu\Big(\frac{r}{(r,n)}\Big);$$

we then define the Vaughan-type approximation

$$E(x, q, a) := \sum_{\substack{n \leq y \\ n \equiv a \bmod q}} F_R(n).$$

The goal of our study is to estimate the mean M_1 and the variance M_2 with

$$M_1 := \sum_{x/2N < q \leq x/N} \Big(\sum_{\substack{a < n \leq x \\ n \equiv a \bmod q}} \Delta_R(n) \Big),$$

$$M_2 := \sum_{x/2N < q \leq x/N} \sum_{a=1}^{q} \Big(\sum_{\substack{a < n \leq x \\ n \equiv a \bmod q}} \Delta_R(n) \Big)^2,$$

where $\Delta_R(n) := f(n) - F_R(n)$. We show that, under Hypotheses 1 and 2 that M_1 is small and M_2 can be approximated by

$$\#\{x/2N < q \leq x/N\} \sum_{n \leq x} \Delta_R(n)^2.$$

We recover Fiorilli's result [1] and Vaughan's result [6] when $f = \Lambda$.

For $f = \tau_k$ and $k \geq 2$, we obtain the existence of an absolute constant $\eta > 0$ such that for every $k \geq 2$ and in the range $N \leq R \leq x^{\eta/k}$ we have

$$\sum_{n \leq x} \Delta_R(n)^2 = C_k x \frac{(\log x)^{k^2-1}}{(k^2-1)!} \Big(1 - \Big(\frac{\log R}{\log x}\Big)^{(k-1)^2} P_k\Big(\frac{\log R}{\log x}\Big) + O\Big(\frac{1}{\log x}\Big)\Big), \tag{1}$$

where P_k are polynomials of degree $2k-2$ and

$$C_k := \prod_p \Big(1-\frac{1}{p}\Big)^{k^2}\Big(\sum_{\nu\geq 0}\frac{\tau_k(p^\nu)^2}{p^\nu}\Big).$$

Defining

$$\gamma_k(c) := \frac{1}{k!G(k+1)^2}\int_{[0,1]^k}\delta(w_1+...+w_k-c)\Delta(w)^2 d^k w,$$

where δ is the Dirac delta-function, $\Delta(w) := \prod_{i<j}(w_i-w_j)$ is the Vandermonde determinant, and $G(k+1) = (k-1)!(k-2)!\cdots 1!$, we observe that

$$\frac{(\log x)^{k^2-1}}{(k^2-1)!}\Big(1-\Big(\frac{\log R}{\log x}\Big)^{(k-1)^2}P_k\Big(\frac{\log R}{\log x}\Big)\Big) = (\log(x/R))^{k^2-1}\gamma_k\Big(\frac{\log x}{\log(x/R)}\Big).$$

The function γ_k has already appeared in [4] and [5].

References

[1] D. Fiorilli, *On Vaughan's approximation: the first moment*, (2015), preprint, https://arxiv.org/pdf/1508.07309.pdf

[2] R. de la Bretèche, D. Fiorilli, *Major arcs and moments of arithmetical sequences*, (2016), preprint, http://arxiv.org/pdf/1611.08312v1.pdf.

[3] C. Hooley, *On the Barban-Davenport-Halberstam theorem. III. J. London Math. Soc.* (2) **10** (1975), 249–256.

[4] J. Keating, B. Rodgers, E. Roditty-Gershon, Z. Rudnick, *Sums of divisor functions in $\mathbb{F}_q[t]$ and matrix integrals*, *arXiv:1504.07804 [math.NT]*

[5] B. Rodgers, K. Soundararajan *The variance of divisor sums in arithmetic progressions*, arxiv.org/abs/1610.06900 (2016).

[6] R. C. Vaughan, *Moments for primes in arithmetic progressions. I. Duke Math. J.* **120** (2003), no. 2, 371–383.

Pairs of quadrics and Nair's theorem

Tim Browning

(joint work with Efthymios Sofos)

A quartic del Pezzo surface X over $\mathbb{Q}$ is a smooth projective surface in $\mathbb{P}^4$ cut out by a pair of quadrics defined over $\mathbb{Q}$. Let $U \subset X$ be the Zariski open set obtained by deleting the 16 lines from X and consider the counting function $N(B) = \#\{x \in U(\mathbb{Q}) : H(x) \leq B\}$, for $B \geq 1$, where H is the standard height function on $\mathbb{P}^4(\mathbb{Q})$. Note that $\#\{x \in (X\setminus U)(\mathbb{Q}) : H(x) \leq B\}$ has order B^2 as soon as one of the lines is defined over $\mathbb{Q}$. The Batyrev–Manin conjecture [2] predicts the existence of a constant $c \geq 0$ such that $N(B) \sim cB(\log B)^{\rho-1}$, as $B \to \infty$, where ρ is the rank of the Picard group of X. To date, as worked out by de la Bretèche and Browning [1], the only example for which this conjecture has been settled is the surface

$$x_0x_1 - x_2x_3 = x_0^2 + x_1^2 + x_2^2 - x_3^2 - 2x_4^2 = 0.$$

Our main result gives expected upper and lower bounds for any conic bundle quartic del Pezzo surface over $\mathbb{Q}$. Thus, assuming only that $X(\mathbb{Q}) \neq \emptyset$ and that X contains a conic defined over $\mathbb{Q}$, we show that there exist constants $c_1, c_2 > 0$, depending on X, such that

$$c_1 B(\log B)^{\rho-1} \leq N(B) \leq c_2 B(\log B)^{\rho-1}.$$

Our proof makes essential use of [5], where detector functions are worked out for the fibres with $\mathbb{Q}$-rational points. Combining this with height machinery and a uniform estimate for the number of rational points of bounded height on a conic, in the generic case the problem is reduced to finding optimal bounds for divisor sums of the shape

$$\sum_{s,t \leq x} \sum_{d \mid \Delta(s,t)} \left(\frac{G(s,t)}{d} \right),$$

for forms $\Delta, G \in \mathbb{Z}[s,t]$ such that Δ is irreducible and $2 \mid \deg G$. Thus far, such sums have only been examined in the special case that G is constant. The extension to general G draws on pioneering work of Shiu [4] and Nair–Tenenbaum [3].

References

[1] R. de la Bretèche and T. D. Browning, Manin's conjecture for quartic del Pezzo surfaces with a conic fibration. *Duke Math. J.* **160** (2011), 1–69.

[2] J. Franke, Y. I. Manin and Y. Tschinkel, Rational points of bounded height on Fano varieties. *Invent. Math.* **95** (1989), 421–435.

[3] M. Nair and G. Tenenbaum. Short sums of certain arithmetic functions. *Acta Math.* **180** (1998), 119–144.

[4] P. Shiu, A Brun–Titchmarsh theorem for multiplicative functions. *J. reine angew. Math.* **313** (1980), 161–170.

[5] E. Sofos, Serre's problem on the density of isotropic fibres in conic bundles. *Proc. London Math. Soc.* **113** (2016), 1–28.

Squarefree orders for the reductions of an elliptic curve over a function field

Alina-Carmen Cojocaru

(joint work with Árpád Tóth, José Felipe Voloch)

Let K be a global field of characteristic p and constant field $\mathbb{F}_q$. We denote by V_K the set of places of K; for $v \in V_K$, we denote by k_v the residue field of K at v and by $\deg v := [k_v : \mathbf{F}_q]$ the degree of v. Let E/K be an elliptic curve over K and set

$$\begin{aligned} V_{E/K} &:= \{v \in V_K : E_v/k_v \text{ is smooth}\}, \\ V_{E/K}(x) &:= \{v \in V_{E/K} : \deg v = x\}, \\ \left|\overline{V}_{E/K}\right| &:= \sum_{v \in V_K \setminus V_{E/K}} \deg v. \end{aligned}$$

We report on progress towards the following claim: assuming $p \geq 5$ and $j_E \notin \mathbb{F}_q$, for each sufficiently large integer x there exists $\delta(E,x) \in \mathbb{Q} \cap [0,\infty)$ such that

$$(1) \quad \#\left\{v \in V_{E/K}(x) : E_v(k_v) \text{ has squarefree order}\right\} = \delta(E,x)\pi_K(x) + \emptyset\left(\frac{q^x}{x}\right),$$

where $\pi_K(x) := \#\{v \in V_K : \deg v = x\}$.

Claim (1) may be viewed as a function field analogue of the following asymptotic formula, proposed and investigated by Cojocaru in the early 2000s (see [Co1], also [Co2], [Co3]):

Squarefree Order Conjecture [Co1]
Let $E/\mathbb{Q}$ be an elliptic curve over $\mathbb{Q}$, of conductor N_E. For a prime p not dividing N_E, let $E_p/\mathbb{F}_p$ be the reduction of E modulo p. Then there exists an explicit constant $\delta(E) \geq 0$ satisfying, as $x \to \infty$,

$$(2) \qquad \#\{p \leq x : E_p(\mathbb{F}_p) \text{ has squarefree order}\} \sim \delta(E)\ \pi(x),$$

where $\pi(x)$ denotes the number of primes $p \leq x$.

We recall that, while (2) is known in the case $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \not\simeq \mathbb{Z}$ (see [Co3, Thm. 1.1, p. 588]) and is supported by average results (see [Ge] and [AkDaHaTh]), it remains open in the case $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$.

The principal tools in our approach towards (1) are:

- results concerning the frequency with which $q^{\deg v} + 1 - |E_v(k_v)|$ equals a given integer, due to A. Pacheco and R. Schoof;
- classical estimates of class numbers of imaginary quadratic fields;
- arithmetic / algebraic properties of the division fields and of the function fields of Igusa curves, associated to E/K, due to J-I. Igusa and N.M. Katz and B. Mazur;
- effective versions of the Chebotarev density theorem for global function fields, due to V.K. Murtya and J. Scherk (and based on A. Weil).

References

[AkDaHaTh] S. Akhtari, C. David, H. Hahn, L. Thompson, *Distribution of squarefree values of sequences associated with elliptic curves,* Contemporary Math. 606, 2013, pp. 171–188.

[BaLoVi] A. Bandini, I. Longhi and S. Vigni, *Torsion points on elliptic curves over function fields and a theorem of Igusa*, Expositiones Mathematicae 27, 2009, pp. 175–209.

[Co1] A.C. Cojocaru, *Cyclicity of elliptic curves modulo p* , PhD thesis, 2002, Queen's University, Canada.

[Co2] A.C. Cojocaru, *Questions about the reductions modulo primes of an elliptic curve*, Number Theory, CRM Proc. Lecture Notes 36, Amer. Math. Soc., Providence, RI, 2004, pp. 61–79.

[Co3] A.C. Cojocaru, *Square-free orders for CM elliptic curves modulo p*, Math. Ann. vol. 342, no 3, 2008, pp. 587–615.

[CoHa] A.C. Cojocaru and C. Hall, *Uniform results for Serre's theorem for elliptic curves*, Int. Mat. Res. Not. 2005, no. 50, pp. 3065–3080.

[CoTo] A.C. Cojocaru and Á. Tóth, *The distribution and growth of the elementary divisors of the reductions of an elliptic curve over a function field*, Journal of Number Theory 132, 2012, pp. 953–965.

[DuTo] W. Duke and Á. Tóth, *The splitting of primes in division fields of elliptic curves,* Experimental Math. 11, 2002, no. 4, pp. 555–565.

[Er] M. Erdélyi, *The distribution and density of cyclic groups of the reductions of an elliptic curve over a function fields,* preprint 2016.

[FuHa] W. Fulton and J. Harris, *Representation theory*, Springer Science & Business Media, vol. 129, 1991.

[Ge] E.-U. Gekeler, *Statistics about elliptic curves over finite prime fields,* Manuscripta Math. 127, 2008, no. 1, pp. 55–67.

[HaRi] H. Halberstam and H-E. Richert, *Sieve methods,* Dover Publications Inc, Mineola, New York, 2011.

[HaVo] C. Hall and J.F. Voloch, *Towards Lang-Trotter for elliptic curves over function fields*, Pure Appl. Math. Q. 2, no. 1, part 1, 2006, pp. 163–178.

[Ig] J-I. Igusa, *Fibre systems of Jacobian varieties (III. Fibre systems of elliptic curves)*, Amer. J. Math. 81, 1959, pp. 453–476.

[Ig2] J-I. Igusa, *On the algebraic theory of elliptic modular functions* J. Math. Soc. Japan 20, 1968, pp 96–106.

[MuSc] V.K. Murty and J. Scherk, *Effective versions of the Chebotarev density theorem for function fields*, C.R. Acad. Sci. Paris, t. 319, Série I, 1994, pp. 523–528.

[Pa] A. Pacheco, *Distribution of the traces of Frobenius on elliptic curves over function fields*, Acta Arithmetica 106.3 (2003), pp. 255–263.

[Ro] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics **201**, Springer-Verlag, New York, 2002.

[Sc] R. Schoof, *Nonsingular plane cubic curves over finite fields*, Journal of Combinatorial Theory, Series A 46, 1987, pp. 183–211.

[Si] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.

[Vo1] J.F. Voloch, *A note on elliptic curves over finite fields*, Bulletin de la S.M.F., tome 116, no 4 (1988), pp. 455–458.

[Vo2] J.F. Voloch, *Primitive points on constant elliptic curves over function fields*, Bol. Soc. Bras. Mat., Vol. 21, no. 1, 1990, pp. 91–94.

[Wa] E. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. 2, 1969, pp. 521–560.

[We] A. Weil, *Courbes algébriques et variétés abéliennes*, Paris, Hermann, 1971.

Statistics of L-functions

Brian Conrey
(joint work with Jon Keating)

The value distribution, especially large values, of L-functions in families can be determined to a certain extent by averages or moments of the L-functions in the family. Similarly, small values and zero statistics can be ascertained by averages of the ratio of products of L-functions. In recent years precise conjectures for moments and for ratios of L-functions have been developed especially using random matrix theory as a guide. These conjectures agree with theory whenever the theory is known, and have also been extensively tested numerically and found to be in good agreement. These conjectures have been developed by Conrey, Farmer, Keating, Rubinstein, and Snaith and by Conrey, Farmer, and Zirnbauer. An alternate approach to moments is due to Friedberg, Goldfeld, and Hoffstein.

What has been missing from this picture is a way to develop these conjectures through arithmetic means. In particular for the Riemann zeta-function how can one obtain the moments conjectures from shifted divisor problems? The purpose of this talk is to explain a method developed by Conrey and Keating to do this.

Typically when one thinks about the $2k$th moment

$$\int_T^{2T} |\zeta(1/2+it)|^{2k}\ dt$$

for $k > 2$ one assumes that the number theory needed to input is a conjectural formula for the shifted divisor problem

$$\sum_{n\leq x} d_k(n)d_k(n+h).$$

However, we now realize that this is not sufficient. In fact, in the terminology developed in the recipe of [CFKRS], this arithmetic information will only give rise to the "one-swap" terms of the recipe.

What is needed to recover the "two-swap" terms is to solve a problem like

$$\sum_{mn\leq x} d_j(m)d_j(m+h_1)d_\ell(n)d_\ell(n+h_2)$$

where $j+\ell = k$, which could be described as "a convolution of two shifted divisor problems." In general, one needs to solve "a k-fold convolution of shifted divisor problems", at least on average, to recover all of the terms in the recipe for the $2k$th moment of ζ.

The original incarnation of this idea is in a couple of papers of Bogomolny and Keating on correlations of zeros of the Riemann zeta-function in which they show formally how to get the n-correlation of zeros of $\zeta(s)$ from the Hardy-Littlewood conjectures for prime pairs $\sum_{n\leq x}\Lambda(n)\Lambda(n+2k)$.

This new convolution of shifted divisor problems bears some resemblance to phenomena in the study of rational points on complicated varieties. There are known examples where the circle method does not register all of the main terms within the study of the major arcs. An example of this, pointed out by Trevor Wooley, occurs in the study of equal sums of three fourth powers:

$$x_1^4 + x_2^4 + x_3^4 = y_1^4 + y_2^4 + y_3^4$$

with $|x_i|, |y+i| \leq N$. Here the circle method predicts a main term of size $\approx N^2$. But the diagonal terms $x_i = y_j$ give a term of size N^3. And the terms on the subvariety with $x_1 = x_2 + x_3$, $y_1 = y_2 + y_3$ give a term of size $\approx N^2 \log N$. So, care is needed in handling this equation!

In our zeta-function moment we are also counting lattice points

$$x_1 \dots x_k = y_1 \dots y_k + h.$$

Ostensibly there should be no other terms. And in a certain regime the circle method (or delta-method) apparently no longer gives all of the main terms and

one needs to forcibly consider counting lattice points on, for example,

$$Mx_1 \dots x_j = Ny_1 \dots y_j + h_1 \qquad Nt_1 \dots t_\ell = Mu_1 \dots u_\ell + h_2$$

for small parameters M and N.

The complete stratification becomes combinatorially quite complicated. But in the end one can recover all of the main terms with the geometric and arithmetic weights which appear in the recipe.

Systems of cubic forms

Rainer Dietmann

Let $\gamma(r)$ be the smallest non-negative integer such than whenever $C_1, \dots, C_r \in \mathbb{Q}[X_1, \dots, X_s]$ are cubic forms with $s > \gamma(r)$, then the system $C_i(\mathbf{x}) = 0 \quad (1 \leq i \leq r)$ has a solution $\mathbf{x} \in \mathbb{Q}^s \backslash \{\mathbf{0}\}$. The best known bounds at present are $\gamma(1) \leq 13$ ([4]), $\gamma(2) \leq 654$ ([2], [4]), and $\gamma(r) < (10r)^5$ ([8]) in general. It is that latter case of large r which we want to focus on. To state results more precisely, let us first generalize Davenport and Lewis' definition of the h-invariant ([3]) to systems of cubic forms in the following way: Let K be a field and $C_1, \dots, C_r \in K[X_1, \dots, X_s]$ be cubic forms, then define $h_K(C_1, \dots, C_r)$ to be the smallest non-negative integer h such that there exist linear forms $L_1, \dots, L_h \in K[X_1, \dots, X_s]$ and quadratic forms $Q_1^{(j)}, \dots, Q_h^{(j)} \in K[X_1, \dots, X_s] \quad (1 \leq j \leq r)$ such that

$$C_j = \sum_{i=1}^{h} L_i Q_i^{(j)} \quad (1 \leq j \leq r).$$

It is easy to see that $s - h_K(C_1, \dots, C_r)$ is the dimension of the largest K-linear space on which $C_1, \dots, C_r$ simultaneously vanish.

Using the circle method, one can show that if $C_1, \dots, C_r \in \mathbb{Z}[X_1, \dots, X_s]$ are cubic forms such that each form C in the $\mathbb{Q}$-rational pencil of $C_1, \dots, C_r$ satisfies $h_{\mathbb{Q}}(C) > 8r^2 + 8r$, then an asymptotic formula for the number of simultaneous integer zeros of $C_1, \dots, C_r$ in an expanding box holds true. The bottleneck is to show that the singular series is positive. Schmidt ([5], [6], [7]) developed an approach combining reduction theory and exponential sums showing that if the system $C_1, \dots, C_r$ is 'ω-bottomed' for $\omega > 1764(3r+1)^2$, then its singular series is positive. However, his argument for 'bottomless' systems was more wasteful, and it is here that we introduce new ideas: If $C_1, \dots, C_r$ is not ω-bottomed, then one can show that there is a form C in the $\overline{\mathbb{Q}}$-rational pencil of $C_1, \dots, C_r$ such that

$$h_{\overline{\mathbb{Q}}}(C) < 3\omega r. \tag{1}$$

The main new ingredient is now our following result ([1]).

Theorem 1. *Let $\alpha_1, \dots, \alpha_q \in \overline{\mathbb{Q}}$ be $\mathbb{Q}$-linearly independent, and let $C_1, \dots, C_q \in \mathbb{Z}[X_1, \dots, X_s]$ be cubic forms. Then*

$$h_{\mathbb{Q}}(C_1, \dots, C_q) \leq 6q h_{\overline{\mathbb{Q}}}(\alpha_1 C_1 + \dots + \alpha_q C_q) + 1.$$

Applying this in the situation (1) from above, one finds that there are linearly independent cubic forms $C_1, \dots, C_q$ in the $\mathbb{Q}$-rational pencil of $C_1, \dots, C_r$ having

$$h_{\mathbb{Q}}(C_1, \dots, C_q) \le 400000qr^3,$$

hence simultaneously vanishing on a $\mathbb{Q}$-linear space V of dimension at least $s - 400000qr^3$. This way, substituting V into the remaining cubic forms, one can inductively reduce the number of equations and obtains the following improvement over Schmidt's result:

Theorem 2. *We have*

$$\gamma(r) \le 400000r^4.$$

The proof of Theorem 1 makes use of Schmidt's subspace theorem: Suppose that

$$\sum_{i=1}^{q} \alpha_i C_i(\mathbf{x}) = \sum_{i=1}^{h} L_i(\mathbf{x}) Q_i(\mathbf{x}) \tag{2}$$

for cubic forms $C_i \in \mathbb{Z}[X_1, \dots, X_s]$, linear forms $L_i \in \mathbb{C}[X_1, \dots, X_s]$ and quadratic forms $Q_i \in \mathbb{C}[X_1, \dots, X_s]$. Choosing $\mathbf{x} \in \mathbb{Z}^s \setminus \{\mathbf{0}\}$, such that simultaneously all $|L_i(\mathbf{x})|$ are small, one can force the right hand side of (2) to be small, whereas by the subspace theorem, and $\mathbb{Q}$-linear independence of $\alpha_1, \dots, \alpha_q$, the left hand side can only be small if all integers $C_i(\mathbf{x})$ are simultaneously zero. This idea can be generalized to finding a $\mathbb{Q}$-linear space of common rational zeros of $C_1, \dots, C_q$ and this way leads to a bound of $h_{\mathbb{Q}}(C_1, \dots, C_q)$ in terms of $h_{\overline{\mathbb{Q}}}(\alpha_1 C_1 + \dots + \alpha_q C_q)$.

References

[1] Dietmann, R. On the h-invariant of cubic forms, and systems of cubic forms, to appear in *Q. J. Math.*

[2] Dietmann, R. & Wooley, T. Pairs of cubic forms in many variables, *Acta Arith.* **110** (2003), 125–140.

[3] Davenport, H. & Lewis, D. J. Non-homogeneous cubic equations, *J. London Math. Soc.* **39** (1964), 657–671.

[4] Heath-Brown, D. R. Cubic forms in 14 variables, *Invent. Math.* **170** (2007), 199–230.

[5] Schmidt, W. M. On cubic polynomials. I. Hua's estimate of exponential sums, *Monatsh. Math.* **93** (1982), 63–74.

[6] Schmidt, W. M. On cubic polynomials. II. Multiple exponential sums, *Monatsh. Math.* **93** (1982), 141–168.

[7] Schmidt, W. M. On cubic polynomials. III. Systems of p-adic equations, *Monatsh. Math.* **93** (1982), 211–223.

[8] Schmidt, W. M. On cubic polynomials. IV. Systems of rational equations, *Monatsh. Math.* **93** (1982), 329–348.

Moments of L–functions in function fields

Alexandra Florea

This report is concerned with moments in the family of quadratic Dirichlet L–functions over function fields. Fix $\mathbb{F}_q[x]$, with q a prime with $q \equiv 1 \pmod 4$. We are interested in obtaining asymptotic formulas for

$$\sum_{D \in \mathcal{H}_{2g+1}} L(\tfrac{1}{2}, \chi_D)^k,$$

where $\mathcal{H}_{2g+1}$ denotes the ensemble of monic, square-free polynomials of degree $2g+1$ with coefficients in $\mathbb{F}_q$, when the genus $g \to \infty$. Using the "recipe" method developed by Conrey, Farmer, Keating, Rubinstein and Snaith to predict moments for different families of L–functions over number fields, Andrade and Keating made the following conjecture.

Conjecture 1. *For q fixed, we have*

$$\sum_{D \in \mathcal{H}_{2g+1}} L(\tfrac{1}{2}, \chi_D)^k = q^{2g+1}\Big(P_k(2g+1) + o(1)\Big),$$

where P_k is a polynomial of degree $k(k+1)/2$ with explicit coefficients.

The first moment was computed by Andrade and Keating, with an error term of size $O(q^{\frac{3g}{2}+\epsilon g})$. In the same setting, I computed an extra term, of size approximately the cube root of the main term.

Theorem 1. *For q, fixed, we have that*

$$\sum_{D \in \mathcal{H}_{2g+1}} L(\tfrac{1}{2}, \chi_D) = q^{2g+1}P_1(2g+1) + q^{\frac{2g+1}{3}}Q_1(2g+1) + O(q^{\frac{g}{2}(1+\epsilon)}),$$

where P_1 and Q_1 are linear polynomials with explicit coefficients.

The proof relies on using a Poisson summation formula over function fields which leads to three terms: a diagonal term, an off-diagonal term arising from the dual parameter in the Poisson summation formula being a square, and an off-off diagonal contribution from non-square polynomials. By identifying the off-diagonal term, as in the work of Soundararajan on the second and third moments of quadratic L–functions in number fields, and by using a matching argument, one can show that this term partly cancels out with the error arising from the diagonal term, and then contributes a lower order term of size $q^{\frac{2g+1}{3}}g$.

In the case of the second and third moments, we prove the following.

Theorem 2. *For q fixed and $k = 2, 3$, we have that*

$$\sum_{D \in \mathcal{H}_{2g+1}} L(\tfrac{1}{2}, \chi_D)^k = q^{2g+1}P_k(2g+1) + O(q^{\frac{kg}{2}(1+\epsilon)}).$$

For the second moment, it is believed that the true size of the error term should be $O(q^{g(1+\epsilon)})$, while for the third moment in the number field setting, by using multiple Dirichlet series, Diaconu, Goldfeld and Hoffstein conjectured the existence

of a term of size $X^{\frac{3}{4}}$ (which translates to $q^{\frac{3g}{2}}$ in the function field setting) in the asymptotic formula. In light of these conjectures, the error terms obtained in the theorem above are sharp. Both of these terms arise from the off-off diagonal contribution of non-square polynomials, which can be related to another shifted moment-type expression. Obtaining the upper bound relies on using the Lindelöf bound for L–functions.

The fourth moment is more delicate to compute, and we cannot obtain the full degree 10 polynomial conjectured by Andrade and Keating. However, we can obtain an asymptotic formula with the first few leading terms. Specifically, we have the following result.

Theorem 3. *For q fixed,*

$$\sum_{D\in\mathcal{H}_{2g+1}} L(\tfrac{1}{2},\chi_D)^4 = q^{2g+1}\Big(a_{10}g^{10}+a_9g^9+a_8g^8\Big)+O\Big(q^{2g+1}g^{7+\frac{1}{2}+\epsilon}\Big),$$

where a_{10}, a_9, a_8 are arithmetic factors which can be written down explicitly.

The proof of the theorem above entails obtaining first an upper bound of the correct order of magnitude for the fourth moment (as in the work of Soundararajan and Harper on moments of the Riemann-zeta function). Using upper bounds for moments allows us to obtain the first leading term in the asymptotic formula. By truncating the Dirichlet polynomial coming from the approximate functional equation and using a recursive argument, one can compute the g^9 and the g^8 terms as well.

Moments of L–functions at the central point

Étienne Fouvry

(joint work with V. Blomer, E. Kowalski, Ph. Michel, D. Milićević and W. Sawin)

In 2011 M. Young proved the following asymptotic formula [6]

$$\frac{1}{q-2}\sum_{\chi \bmod q}^{*}\Big|L(\chi,1/2)\Big|^4 = P_4(\log q)+O\big(q^{-\frac{1}{80}(1-2\theta)+\varepsilon}\big), \tag{1}$$

where $q\geq 3$ is prime, where the sum is over all primitive characters modulo q, where P_4 is a real polynomial with degree 4, and where θ is any constant, such that the inequality $|\lambda_f(n)|\leq d(n)n^\theta$, ($d$ usual divisor function) holds for any $n\geq 1$, for any cuspidal Hecke eigenform, holomorphic or not. Recall that the value $\theta=7/64$ is correct (Kim–Sarnak) and it is conjectured that $\theta=0$ is also correct (Ramanujan–Petersson conjecture).

The purpose of our work has two aspects: extend the left–hand side of (1) and improve the error term. Here are our three results (see [1], [2], [4]).

Let f be a cuspidal Hecke eigenform with level 1, *holomorphic or not. Then there exist three polynomials P_4, P_0 and P_1, with degrees* 4, 0 *and* 1 *respectively,*

such that, for any $\varepsilon > 0$, for any prime $q \geq 3$, we have the equalities

$$\frac{1}{q-2}\sum_{\chi \bmod q}^{*} \Big|L(\chi, 1/2)\Big|^4 = P_4(\log q) + O_\varepsilon\big(q^{-\frac{1}{20}+\varepsilon}\big), \tag{2}$$

(and the exponent $1/20$ is improved in $1/16$ if $\theta = 0$)

$$\frac{1}{q-2}\sum_{\chi \bmod q}^{*} L(f\otimes\chi, 1/2)\,\overline{L(\chi, 1/2)}^2 = P_0(\log q) + O_\varepsilon\big(q^{-\frac{1}{68}+\varepsilon}\big), \tag{3}$$

$$\frac{1}{q-2}\sum_{\chi \bmod q}^{*} \Big|L(f\otimes\chi, 1/2)\Big|^2 = P_1(\log q) + O_\varepsilon\big(q^{-\frac{1}{144}+\varepsilon}\big), \tag{4}$$

In the above formulas, $L(f\otimes\chi, s)$ is the classical Dirichlet twist of a modular L–function: $L(f\otimes\chi, s) = \sum \lambda_f(n)\chi(n)n^{-s}$. Remark, that if we consider, for instance the sum treated in (4) but with f replaced by the Eisenstein series E, we recover the sum appearing in (1) and (2). The problem of giving asymptotic formulas of the sums presented in (2), (3) and (4) (with a power saving in the error term) is more and more difficult. The reason is essentially due to the fact that the sums we are creating in the proof, are more and more rigid: the function d, seen as a Fourier coefficient of an Eisenstein series, is present in (1) and (2) and introduces more flexibility.

Compared with (1), our improvements are essentially based on a better treatment of the shifted convolution problems and also new results concerning bilinear sums of Kloosterman sums. For q prime, we denote by $\mathrm{Kl}_2(a;q)$ the normalized Kloosterman sum $\mathrm{Kl}_2(a;q) := (1/2\sqrt{q})\sum \exp(2\pi i(x+ay)/q)$, where the sum is over all (x, y) modulo q such that $xy = 1$. By Weil, we know the inequality $|\mathrm{Kl}_2(a;q)| \leq 1$. We are searching for deeper cancellations by exploiting the oscillations of the signs of Kl_2 in bilinear sums of the shape

$$\mathcal{B}(M, N) := \sum_{m\in\mathcal{M}}\sum_{n\in\mathcal{N}} \alpha_m\beta_n \mathrm{Kl}_2(mn;q),$$

where $\mathcal{M}$ and $\mathcal{N}$ are intervals modulo q, with cardinalities M and N, and where α_m and β_n are coefficients less than 1 in modulus. Our aim is to go below the trivial bound $\mathcal{B}(M, N) = O(MN)$ for M and N as small as possible when compared with the prime q going to infinity.

We treat $\mathcal{B}(M, N)$ under different angles: Cauchy–Schwarz and independence of Kloosterman sheaves ([1]), by trace functions techniques, or opening Kloosterman sums ([5], [2]), Karatsuba shift by ab and bounds for exponential sums over some varieties ([1]),...

The recent bound (see [4]) $\mathcal{B}(M, N) \ll MNq^{-\delta}$ for M and $N \geq q^{\frac{1}{2}-\gamma}$ where δ and γ are some specified constants certainly is the achievment of all these techniques and seems to be essential in the proof of (4).

The combination of (2), (3) or (4) with now standard techniques of analytic number theory (amplification, mollification, resonator,...) leads to various results on the existence of special behaviour of these L–functions at the central point.

For instance we prove that if f is a fixed Hecke cuspidal newform, there exists a positive proportion of Dirichlet twists $L(f\otimes\chi, 1/2)$ with modulus greater $1/(\log q)$ when χ belongs to the set of a characters modulo the prime q going to infinity (see [3]).

References

[1] V. Blomer, E. Fouvry, E. Kowalski, Ph. Michel and D. Milićević, *On moments of twisted L–functions*, Amer. J. Math. (to appear), see arXiv:1411.4467.

[2] V. Blomer, E. Fouvry, E. Kowalski, Ph. Michel and D. Milićević, *Some applications of smooth bilinear sums of Kloosterman sums*, Special issue of the Proceedings of the Steklov Institute of Mathematics dedicated to the 125th anniversary of I. M. Vinogradov (to appear), see arXiv:1604.07664.

[3] V. Blomer, E. Fouvry, E. Kowalski, Ph. Michel, D. Milićević and W. Sawin, *Non–vanishing of twisted L–functions*, (work in progress).

[4] E. Kowalski, Ph. Michel and W. Sawin, *Bilinear forms with Kloosterman sums and applications*, (submitted), see arXiv:1511.01636.

[5] I.E. Shparlinski and T.P. Zhang, *Cancellations amongst Kloosterman sums*, Acta Arith. (to appear), see arXiv:1501.05123

[6] M. Young , *The fourth moment of Dirichlet L–functions*, Ann. of Math. (2) **173** (2011), no. 1, 1–50.

Divisor sums and rational points on conic bundle surfaces

Christopher Frei

(joint work with Daniel Loughran and Efthymios Sofos)

A *conic bundle surface* over a number field K is a smooth projective surface X over K with a dominant morphism $\pi : X \to \mathbb{P}^1_K$, such that each fibre of π is isomorphic to a plane conic. It can be defined inside a $\mathbb{P}^2$-bundle over $\mathbb{P}^1$ by an equation

$$Q(s,t;x_0,x_1,x_2) := \sum_{0\le i,j\le 2} a_{ij}(s,t)x_ix_j = 0,$$

with binary forms $a_{ij} \in \mathcal{O}_K[s,t]$. In particular, every del Pezzo surface is a conic bundle surface if the base field K is large enough. The height machine provides us with a height function H on the rational points $X(K)$ relative to the anticanonical divisor $-K_X$ of X. If $-K_X$ is big, then X has an open subset U satisfying the Northcott property, i.e.,

$$N_{U,H}(B) := \#\{x \in U(K) \mid H(x) \le B\} < \infty$$

for all $B > 0$. If moreover $X(K)$ dense in X, versions of Manin's conjecture predict an asymptotic formula

$$N_{U,H}(B) \sim cB(\log B)^{\rho_X - 1},$$

where $c > 0$ and ρ_X is the rank of the Picard group of X. Our results concern (conjecturally) sharp asymptotic lower bounds for $N_{U,H}(B)$ for a wide range of conic bundle surfaces and arbitrary open subsets U thereof. To each conic bundle surface $\pi : X \to \mathbb{P}^1_K$, we associate a *generalized divisor sum* $D_\pi(B)$ over the values

of certain binary forms. For simplicity, let us restrict to the case $K = \mathbb{Q}$. Then our divisor sums take the rough shape

$$D(B) := \sum_{\substack{(s,t)\in(\mathbb{Z}\cap[-B,B])^2\\ F_i(s,t)\neq 0\\ (s,t)\equiv(\sigma,\tau) \bmod q}} \prod_{i=1}^{n} (1*f)(F_i(s,t)) \Bigg(\sum_{\substack{d_i\in\mathbb{N}\\ d_i \text{ odd}\\ d_i \mid F_i(s,t)}} \left(\frac{G_i(s,t)}{d_i}\right)\Bigg).$$

Here, σ, τ, q, are positive integers, f is a small arithmetic function, the integer binary forms G_i have even degree, and the forms F_i are irreducible and coprime to G_i and each other. For such divisor sums, one would expect lower bounds (and even asymptotics) of the order of maginitude

$$D(B) \gg B(\log B)^{\mathrm{rk}(D)}, \tag{1}$$

where $\mathrm{rk}(D) := \#\{1 \le i \le n \mid G_i(s,1) \text{ is a square mod } F_i(s,1)\}$, assuming that no F_i is proportional to t. The divisor sum $D_\pi(B)$ corresponding to a conic bundle surface π has the irreducible factors of the discriminant $\Delta(s,t) := \det(a_{ij}(s,t))$ as the forms F_i and certain detector functions deciding the splitting properties of singular fibres as the forms G_i. The main result of [1] shows that a lower bound as in (1) for $D_\pi(B)$ implies a lower bound

$$N_{U,H}(B) \gg B(\log B)^{\rho_X - 1}$$

for the number of rational points in any non-empty open subset U of X, which is sharp according to Manin's conjecture. In [2], we prove the validity of (1) for all divisor sums D of *complexity*

$$c(D) := \sum_{\substack{1\le i\le n\\ G_i(s,1)\not\equiv \square \bmod F_i(s,1)}} \deg F_i \le 3$$

over all number fields, under some technical hypotheses. The sum in the definition of $c(D)$ runs over all i such that $G_i(s,1)$ is no square modulo $F_i(s,1)$. These bounds translate back to sharp lower bounds for conic bundle surfaces π of *complexity*

$$c(\pi) := \sum_{\substack{p\in\mathbb{P}^1_K\\ X_p \text{ non-split}}} [K(p):K] \le 3,$$

leading to remarkable consequences in particular for del Pezzo surfaces. Recall that every del Pezzo surface has a *degree* $d \in \{1,\dots,9\}$, defined as the self-intersection number $d = K_X \cdot K_X$. Manin's conjecture is known to hold for del Pezzo surfaces of degree $d \ge 6$, so we restrict to $d \le 5$.

Theorem 1. *Let X be a del Pezzo surface of degree $d \le 5$ over K. Then*

$$N_{U,H}(B) \gg B(\log B)^{\rho_X - 1}$$

holds after a base extension of degree bounded by $n_d < \infty$.

Theorem 2. *Let X be a del Pezzo surface of degree $d \leq 5$ over K with $X(K) \neq \emptyset$. Then*

$$N_{U,H}(B) \gg B(\log B)^{\rho_X - 1}$$

as soon as $\rho_X \geq r_d$.

The constants n_d, r_d in Theorems 1 and 2 are given explicitly as follows.

d	5	4	3	2	1
n_d	5	80	432	4032	138240
r_d	3	4	4	5	6

References

[1] C. Frei, D. Loughran and E. Sofos, *Rational points of bounded height on general conic bundle surfaces*, preprint, arXiv:1609.04330.

[2] C. Frei and E. Sofos, *Generalised divisor sums of binary forms over number fields*, preprint, arXiv:1609.04002.

Sums of squares and combinatorial geometry

Brandon Hanson

The numbers which can be represented as a sum of squares are of classical importance to number theory. Laundau gave an asymptotic formula for the number of such integers up to x. From an additive combinatorial point of view, the fact that the number of such integers is even $o(x)$ is perhaps surprising. Why should the squares have any additive structure at all. A simple modification of the large sieve can be used to explain this. On the other hand, this small amount of additive structure is conjectured to be the most any collection of squares has. Namely, if S is any finite set of perfect squares, then a conjecture of Rudin states that $|S+S| \gg |S|^{2-\epsilon}$ should hold for any positive ϵ (at the cost of an implicit constant). This conjecture is wide open, and even $|S+S| \gg |S|^{1+\delta}$ for some positive δ is not known. Here, the assumption that S consists of squares of integers is essential. We prove that for difference sets, i.e. sets of the form $D = A - A$ where A is a set of real numbers, a similar phenomenon holds: $|D^2 + D^2| \gg |D|^{1+\delta}$. This provides a certain rigid structure to the endpoint case of the famous Erdos Distinct Distances Problem for point sets which are cartesian products.

Character sums and point counting

Adam J Harper

Let q be a large prime, and let $\chi \neq \chi_0$ be a non-principal Dirichlet character mod q. The behaviour of character sums $\sum_{n\in I}\chi(n)$, where I is an interval, is a classical topic of study in analytic number theory. In my talk I reported on work in progress on the behaviour of the sums

$$S(x) = S(x;q,\chi,H) := \sum_{x<n\leq x+H}\chi(n),$$

where $H = H(q) \geq 0$ is some length function, and where $x \in \{0,1,...,q-1\}$ is chosen uniformly at random. This statistical question has been the subject of work by Davenport and Erdős [1] and by Lamzouri [2], amongst others.

Since χ is periodic modulo q, we may restrict attention to length functions satisfying $0 \leq H \leq q$. Moreover, when $H \asymp q$ it turns out that the behaviour of $S(x)$ has special structure (e.g. when $H = q$ we have $S(x) \equiv 0$, by orthogonality), and for bounded H the question of the distribution of $S(x)$ essentially reduces to the distribution of values of the character χ itself. Therefore we restrict to the case where $H(q) \to \infty$ but $H(q) = o(q)$ as $q \to \infty$. In this setting, and for *real* χ, and *assuming in addition that* $(\log H)/\log q \to 0$, Davenport and Erdős [1] proved that

$$\frac{S(x)}{\sqrt{H}} \xrightarrow{d} N(0,1) \quad \text{as } q \to \infty.$$

Recall that the object on the left is a random variable for each q (as x is chosen at random), and the result of Davenport and Erdős is the convergence in distribution of this sequence of random variables (as $q \to \infty$) to the standard real Gaussian $N(0,1)$. Lamzouri [2] extended the result of Davenport and Erdős to allow complex characters χ, now with a complex Gaussian limit distribution, but still under the extra assumption that $(\log H)/\log q \to 0$ as $q \to \infty$.

Lamzouri [2] also made a conjecture about what should happen when the assumption $(\log H)/\log q \to 0$ is removed. More precisely, he conjectured that provided $H(q) \to \infty$ and $H(q) = o(q/\log q)$ one should see the same Gaussian limit distributions. This conjecture was based on the analogy with a model problem where one fixes an interval $[y, y+z(y)]$ (with $y \to \infty$ at the end), and looks at the distribution of the sum on this *fixed* interval of a *random* multiplicative function.

The results I described in my talk were as follows. Firstly, Lamzouri's conjecture is not correct, since for any fixed $A > 0$ one can take $H(q) = q/\log^A q$ and find a sequence of characters χ mod q for which one doesn't see the desired limit distributions. But secondly, Lamzouri's conjecture is correct on the range $q^{1-o(1)} \leq H(q) = o(q)$, provided one only asks for the result for "almost all" characters. In particular, one doesn't need the extra restriction $H(q) = o(q/\log q)$ posited by Lamzouri for an "almost all" result (and the result is false if one wants it for all characters).

The disproof of Lamzouri's conjecture works by looking at the Fourier expansion of $S(x)$, and observing that this closely resembles a sum of χ over an interval of

length $q/H = \log^A q$. Thus it turns out one can rule out the posited Gaussian limits by using characters whose sum over such an interval is "highly biased". The positive "almost all" result is proved using a moment calculation with this Fourier expansion, which reduces to a point counting problem.

References

[1] H. Davenport, P. Erdős, *The distribution of quadratic and higher residues*, Publ. Math. Debrecen **2** (1952), 252–265.

[2] Y. Lamzouri, *The distribution of short character sums*, Math. Proc. Cambridge Philos. Soc. **155**, no. 2 (2013), pp 207–218.

Iteration of quadratic polynomials over finite fields

Roger Heath-Brown

Let $f(X) \in \mathbb{F}_q[X]$ and define the iterates $f_j(X)$ by setting $f_0(X) = X$ and $f_{j+1}(X) = f(f_j(X))$. Let $m \in \mathbb{F}_q$, and consider the sequence of values $f_0(m)$, $f_1(m)$, $f_2(m), \ldots$. Since the field $\mathbb{F}_q$ is finite, the sequence eventually recurs, and one enters a closed cycle. We are interested in the questions:- How long is it before one enters the cycle? How long is the cycle?

The standard model assumes that the values $f_i(m)$ form a random walk. They should then typically recur after $O(\sqrt{q})$ steps. However the polynomials $f(X) = X^2$ and $f(X) = X^2 - 2$ do not behave in this way. If $q = 2r + 1$ and $r = 2l + 1$ with q, r, l all prime and $l \equiv 1 (\mathrm{mod}\ 4)$, then the first of these produces a period of length $(q - 3)/2$ if the starting value m is a primitive root of q. Similarly, the second will produce a cycle of length $\gg q$ for many initial values m.

Things also appear to go wrong for $f(X) = X^3 + 1$ when $q \equiv 5 (\mathrm{mod}\ 6)$ is prime. Here f induces a permutation on $\mathbb{F}_q$, and if this were a random permutation we would expect cycles of length $\gg q$ in a positive proportion of cases. The numerical evidence seems to support this model.

In contrast we prove:

For $f(X) = X^2 + 1$ the sum of all cycle lengths is $O(q/(\log\log q))$. Moreover, every trajectory $f_0(m), f_1(m), \ldots$ recurs after $O(q/(\log\log q))$ steps.

The proof proof works for most quadratic polynomials but requires (among other conditions) that

$$\frac{f_a(X) - f_a(Y)}{f_b(X) - f_b(Y)}$$

is absolutely irreducible for all positive integers $a > b$; and one can see that this fails for X^2 and $X^2 - 2$.

The sieve of Eratosthenes in less space

Harald Andrés Helfgott

The sieve of Eratosthenes is a procedure for constructing all primes up to N. More generally, such a sieve can be used for computing all values $f(n)$, $n \leq N$, for many arithmetical functions f that depend on the factorization of integers. For instance, one can take $f = \mu$, the Möbius function, or $f = \lambda$, the Liouville function.

The point of the sieve of Eratosthenes is that it can be carried out in time close to linear on N, even though determining whether an individual integer is prime, let alone factorizing it, takes much more than constant time with current methods. Though a very naïve implementation of the sieve would take space proportional to N, it is not hard to see how to implement the sieve in space $O(\sqrt{N})$, simply by applying the sieve to intervals of length $O(\sqrt{N})$ at a time; the time taken is still essentially linear on N. (One could take shorter intervals, but the algorithm would then become much less efficient.) This is called the "segmented sieve"; see [Sin69] for an early reference.

Galway [Gal00] found a way to sieve using space $O(N^{1/3})$ and essentially linear time. Like the sieve in [AB04], on which it is based, Galway's sieve is specific to finding prime numbers.

I have managed to find a way to implement a sieve of Eratosthenes in space $O(N^{1/3})$ and essentially linear time.

Theorem 1. *We can construct all primes $p \leq N$ in space $O(N^{1/3})$ and time $O(N)$. We can also compute all values $\mu(n)$ and $\lambda(n)$ with $n \leq N$, in space $O\left(N^{1/3}(\log N)^{2/3}\right)$ and time $O(N \log N)$.*

Moreover, we can construct all primes in an interval $[N-\Delta, N+\Delta)$ and compute all values $\mu(n)$, $\lambda(n)$ therein in time $O(\Delta \log x)$ for $\Delta \geq N^{1/3}(\log N)^{2/3}$.

The main ideas come from basic number theory. In order for us to be able to apply the sieve to an interval I of length $O(N^{1/3})$ without large time inefficiencies, we need to be able to tell in advance which primes (or integers) d up to $\sqrt{N}$ divide at least one integer in I, without testing each d individually. We can do this by Diophantine approximation, a local linear approximation to the function $x \mapsto n/x$ for n fixed, and by the solution to what amounts to a linear equation mod1.

The idea of using Diophantine approximation combined with a local linear approximation is already present in [TCH12], where it was used to compute $\sum_{n \leq x} \tau(n)$ in time $O(x^{1/3}(\log x)^{O(1)})$. The basic underlying idea in [Gal00] may be said to be the same: we are speaking of an Diophantine idea that stems ultimately from Voronoï's work on the circle problem (in the case of [Gal00]) and the Dirichlet divisor problem. For that matter, [Gal00, §5] already suggests that Voronoï's work on the Dirichlet divisor problem could be used to make the sieve of Eratosthenes in space $O(N^{1/3})$ and essentially linear time.

The main difference is that the relation to Voronoï in Galway's work is much more direct, in that he literally dissects a region between two circles, much as Voronoï does. In the case of the present work, we can speak of a main idea that

originated in the context of giving elementary estimates for a quantity in analytic number theory and is now used to carry out an exact computation.

References

[AB04] A. O. L. Atkin and D. J. Bernstein. Prime sieves using binary quadratic forms. *Math. Comp.*, 73(246):1023–1030 (electronic), 2004.

[Gal00] William F. Galway. Dissecting a sieve to cut its need for space. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 297–312. Springer, Berlin, 2000.

[Sin69] Richard C. Singleton. Algorithm 357: an efficient prime number generator. *Communications of the ACM*, 12:563–564, 1969. URL: `http://cr.yp.to/bib/entries.html#1969/singleton-357`.

[TCH12] Terence Tao, Ernest Croot, III, and Harald Helfgott. Deterministic methods to find primes. *Math. Comp.*, 81(278):1233–1246, 2012.

New results on the Selberg class

Jerzy Kaczorowski, Alberto Perelli

Part I - *The functional equation of the standard twists of certain L-functions.*
The standard twist of an L-function $F(s)$ satisfying a general Riemann-type functional equation

$$\Lambda(s) = \omega\overline{\Lambda(1-\overline{s})}, \qquad \Lambda(s) = Q^s \prod_{j=1}^{r} \Gamma(\lambda_j s + \mu_j) F(s) \tag{1}$$

is defined as

$$F(s,\alpha) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s} e(-\alpha n^{1/d}), \tag{2}$$

where $\alpha > 0$, $e(x) = e^{2\pi i x}$ and $a(n)$ (resp. $d = 2\sum_{j=1}^{r} \lambda_j$) are the coefficients (resp. the degree) of $F(s)$. The standard twist is a useful tool in the study of L-functions (in particular in the Selberg class theory), and its basic analytic properties (meromorphic continuation, polar structure and order of growth on vertical strips) are known.

In view of the characterization of the degree 1 L-functions, in such a case $F(s,\alpha)$ reduces to a certain combination of Hurwitz-Lerch zeta functions, and hence satisfies a Hurwitz-Lerch type functional equation. One may therefore ask if the standard twist has a functional equation for general degrees $d \geq 2$. Recently we proved that if $F(s)$ satisfies (1) with a special choice of Γ-factors, then $F(s,\alpha)$ has a functional equation reflecting s to $1-s$.

Examples of such a choice of Γ-factors can be produced for any integer degree $d \geq 2$. In particular, for $d = 2$ our method applies to the classical case of the Hecke L-functions associated with cusp forms of half-integral weight. As a consequence, in such a case $F(s,\alpha)$ satisfies, in addition to the above reported properties, a functional equation which may be regarded as a degree 2 analog of the Hurwitz-Lerch functional equation. Moreover, information about trivial and non-trivial

zeros of $F(s,\alpha)$ can be deduced. We are currently investigating how to enlarge the choice of admissible Γ-factors.

Part II - *Converse theorems for degree* 2*, conductor* 1 *L-functions from the Selberg class.*

Converse theorems are statements identifying known L-functions by their analytic properties. We focus our attention on degree 2 L-functions from the Selberg class of conductor 1. It is expected that the only primitive L-functions of this type are those coming from holomorphic and non-holomorphic eigenforms with respect to the full modular group $\Gamma_0(1)$. The theorems below yield strong evidence supporting these expectations.

For $F(s)$ from the Selberg class S we denote by d and q the degree and the conductor of $F(s)$, respectively. Moreover, let $\xi = 2\sum_{j=1}^{r}(\mu_j - \frac{1}{2})$, $H(2) = 2\sum_{j=1}^{r} B_2(\mu_j)\lambda_j^{-1}$ (here $B_2(X) = X^2 - X + 1/6$ denotes the second Bernoulli polynomial) and $\delta(F) = \inf|\Re(\omega' - \omega)|$, where the infimum is taken over different trivial zeros of $F(s)$ with $\Im(\omega) = \Im(\omega')$. The following theorems hold.

Theorem 1. *If $F \in S$ has $d = 2$, $q = 1$ and a pole at $s = 1$, then $F(s)$ is the square of the Riemann zeta function: $F(s) = \zeta^2(s)$.*

Theorem 2. *If $F \in S$ has $d = 2$, $q = 1$, $\xi = k - 2$ ($k \geq 12$, even integer) and $H(2) = 2B_2((k-1)/2)$, and all its trivial zeros are simple, then there exists a holomorphic eigenform $f \in S_k(\Gamma_0(1))$ such that $F(s) = L(s + \frac{k-1}{2})$.*

Theorem 3. *Let $F \in S$ be such that $d = 2$, $q = 1$, $\xi \in \{-2, 0\}$, $H(2) = \frac{4}{3} - 2\kappa^2$, where $\kappa^2 + \frac{1}{4}$ is an eigenvalue of the hyperbolic Laplacian, and $\delta(F) > 1$. Then there exists a weight 0 Maass eigenform for $\Gamma_0(1)$ corresponding to the eigenvalue $\kappa^2 + \frac{1}{4}$ such that $F(s) = L(s, f)$. Moreover, f is even if $\xi_F = -2$ and odd if $\xi_F = 0$.*

Sieve weights and their smoothings

Dimitris Koukoulopoulos
(joint work with Andrew Granville and James Maynard)

Inclusion-exclusion tells us that

$$\mathbf{1}_{(a,m)=1} = \sum_{d|(a,m)} \mu(d). \tag{1}$$

Here we think of a as belonging some set $\mathcal{A}$ from which we are trying to extract primes, and m as the product of some primes with which we are sifting $\mathcal{A}$. However, the divisors d in the right hand side of (1) become too large for this formula to be useful in practice. Modern sieve methods can be thought of as an attempt of replacing the right hand side of (1) with weights that correlate sufficiently strongly with the left hand side. In the combinatorial sieve, this is done using combinatorial

tools. In Selberg's sieve though, one replaces the right hand side of (1) by

$$\left(\sum_{d|(a,m)} \lambda_d\right)^2, \tag{2}$$

where the λ_d's are some real numbers to be chosen in an optimal way. If $\lambda_1 = 1$, then the expression in (2) always majorizes $\mathbf{1}_{(a,m)=1}$. To guarantee that the support of the sum in (2) is small enough, we assume that $\lambda_d = 0$ for $d > R$. If $m = \prod_{p \le R}$ and we impose some reasonable assumptions on the set $\mathcal{A}$ we are sieving, we find that the optimal choice in Selberg's sieve is given by

$$\lambda_d \approx c \cdot \mu(d) \cdot \left(\frac{\log(R/d)}{\log R}\right)^{\kappa} \cdot \mathbf{1}_{d \le R},$$

where κ is a certain invariant of the sieving problem called the *dimension* and c is a normalizing factor. What is important to notice here is as κ increases, the truncation at $d = R$ is done in a smoother and smoother way.

More generally, we can consider the Selberg-style sieve weight

$$M_f(n; R) = \sum_{d|n} \mu(d) f\left(\frac{\log d}{\log R}\right),$$

where f is supported on $(-\infty, 1]$. Such weights and their higher-dimensional analogues play a crucial role in the study of small gaps between primes [6, 8, 10, 11]. In [7], we investigate the role of the smoothness of f in these weights. As it turns out, the effect of the smoothing can be seen more explicitly when taking high moments of $M_f(n; R)$. In the special but important case when $f(x) = f_A(x) := \mathbf{1}_{x<1} \cdot (1-x)^A$, we proved the following result:

Theorem 1. *For fixed integers $k \ge 1$ and $A \ge 0$, there is a constant $c_{k,A} > 0$ such that*

$$\frac{1}{x} \sum_{n \le x} M_f(n; R)^{2k} = c_{k,A} \cdot (\log R)^{\mathcal{E}_{k,A}} + O((\log R)^{\mathcal{E}_{k,A}-1}) \quad (x \ge R^{2k} \log R),$$

where $\mathcal{E}_{k,A} := \max\{\binom{2k}{k} - 2k(A+1), -1\}$. In particular, $\mathcal{E}_k = \mathcal{E}_{k,0} = \binom{2k}{k} - 2k$. Additionally, we find that there is a constant $c'_k > 0$ such that for $R^{2k} \le x$ we have

$$\frac{1}{x} \sum_{n \le x} \Big(\sum_{\substack{d|n \\ R/2 < d \le R}} \mu(d) \Big)^{2k} = c'_k (\log R)^{\binom{2k}{k}-2k} + O\left((\log R)^{\binom{2k}{k}-2k-1}\right).$$

All implied constants depend at most on k and A.

In particular, we see that $2k$-th power of $M_{f_A}(n; R)$ behaves like a sieve weight only when $A > \binom{2k}{k}/(2k) - 1$. The above theorem improves upon [1, 3] when $A = 0$.

We also studied analogous questions in the ring $\mathbb{F}_q[t]$, where q is a prime. Precisely, we considered the sum

$$\mathrm{Poly}_q(n,m;k) := \frac{1}{q^n} \sum_{\substack{N\in\mathbb{F}_q[t]\\ \deg N=n}} \Big| \sum_{\substack{M|N\\ \deg M=m}} \mu(M)\Big|^{2k}.$$

Part of our motivation for studying this analogy was to get a better understanding of the unexpected exponent $\mathcal{E}_{k,0} = \binom{2k}{k} - 2k$ in the unsmoothed cased. However, it turns out that there is a discrepancy between $\mathbb{Z}$ and $\mathbb{F}_q[t]$, a rare occurrence:

Theorem 2. *For integers $k, m \geq 1$ and $n \geq 2mk$, and a prime power q that is large enough in terms of m and k, we have that*

$$\mathrm{Poly}_q(n,m;k) \asymp_{m,k} 1 + m^{2^{2k-1}-2k-1}.$$

We explained this discrepancy by observing that it is rooted in the fact that the Möbius function $\mu(M)$ can be replaced here by $(-1)^{\deg(M)}\mu(M)$, which is zero on average over irreducible polynomials. An analogous example of a real-valued multiplicative function over $\mathbb{Z}$ is a real, non-principal Dirichlet character χ, and the analogous quantity is

$$\mathcal{D}(x;R) := \frac{1}{x}\sum_{n\leq x}\Big(\sum_{\substack{d|n\\ R/2<d\leq R}} \chi(d)\Big)^{2k}.$$

We proved that $\mathcal{D}(x;R)$ behaves like the finite field analogy for R large enough in terms of χ. However, if $L(s,\chi)$ has a Siegel zero, so that $\chi(n)$ *pretends to be* $\mu(n)$ for small n, then $\mathcal{D}(x;R)$ behaves like the same sum with χ replaced by μ for small R.

References

[1] M. Balazard, M. Naimi and Y.-F. S. Pétermann, *Étude d'une somme arithmétique multiple liée à la fonction de Möbius*, Acta Arith. **132** (2008), 245–298.

[2] R. de la Bretèche, *Estimation de sommes multiples de fonctions arithmétiques*, Compos. Math. **128** (2001), 261–298.

[3] F. Dress, H. Iwaniec and G. Tenenbaum, *Sur une somme liée à la function de Möbius*, J. Reine Angew. Math. **340** (1983), 53–58.

[4] K. Ford, *The distribution of integers with a divisor in a given interval*, Ann. of Math. 168, (2008), 367–433.

[5] J. Friedlander and H. Iwaniec, *Opera de cribro*. American Mathematical Society Colloquium Publications, 57. American Mathematical Society, Providence, RI, 2010.

[6] A. Goldston, J. Pintz and C. Y. Yıldırım, *Primes in tuples. I.* Ann. of Math. (2) 170 (2009), no.2, 819–862.

[7] A. Granville, D. Koukoulopoulos, J. Maynard, *Sieve weights and their smoothings.* Preprint (2016), arXiv:1606.06781

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

[9] A. Selberg, *Collected papers. II*, Springer Collected Works in Mathematics, Springer, Heidelberg, 2014.

[10] T. Tao, *Polymath8b: Bounded intervals with many primes, after Maynard*, Blog note. https://terrytao.wordpress.com/2013/11/19/polymath8b-bounded-intervals-with-many-primes-after-maynard/
[11] Y. Zhang, *Bounded gaps between primes*, Ann. of Math. (2) 179 (2014), no. 3, 1121–1174.

Height of rational points on random Fano varieties

Pierre Le Boudec

The goal of this note is to report on forthcoming work of the author [5] investigating the distribution of the height of the lowest rational point on a variety V in terms of the height of V, as V runs over families of Fano complete intersections.

We let $n \geq 3$, $r \geq 1$ and $d_1, \dots, d_r \geq 2$ be fixed. Moreover, we set $\mathbf{d} = (d_1, \dots, d_r)$ and $d = d_1 + \cdots + d_r$ and we assume that $n + 1 - d > 0$. Finally, for $e \geq 1$, we let $N(e, n)$ be the number of monomials of degree e in $n + 1$ variables.

Ordering monomials using the lexicographical order, smooth complete intersections in $\mathbb{P}^n$ of codimension r and multidegree $\mathbf{d}$ defined over $\mathbb{Q}$ are naturally parametrized by a subset $\mathbb{V}_{\mathbf{d},n}$ of $\mathbb{P}^{N(d_1,n)-1}(\mathbb{Q}) \times \cdots \times \mathbb{P}^{N(d_r,n)-1}(\mathbb{Q})$. From now on, we thus view the above varieties as elements of this product of projective spaces.

Note that the assumption $n + 1 - d > 0$ implies that the elements of $\mathbb{V}_{\mathbf{d},n}$ are Fano varieties.

We define the exponential height $H_n : \mathbb{P}^n(\mathbb{Q}) \to \mathbb{R}_{>0}$ by choosing coordinates $(x_0, \dots, x_n) \in \mathbb{Z}^{n+1}$ satisfying $\gcd(x_0, \dots, x_n) = 1$ and by setting

$$H_n(x_0 : \cdots : x_n) = \max\{|x_0|, \dots, |x_n|\}.$$

Let $V \in \mathbb{V}_{\mathbf{d},n}$. Recall that the anticanonical height $H : V(\mathbb{Q}) \to \mathbb{R}_{>0}$ on V is defined by

$$H(x_0 : \cdots : x_n) = H_n(x_0 : \cdots : x_n)^{n+1-d}.$$

Our goal is to investigate the quantity $\mathfrak{M}(V)$ defined by

$$\mathfrak{M}(V) = \min\{H(\mathbf{x}), \mathbf{x} \in V(\mathbb{Q})\},$$

if $V(\mathbb{Q}) \neq \emptyset$ and by $\mathfrak{M}(V) = \infty$ if $V(\mathbb{Q}) = \emptyset$.

We now introduce an ordering of $\mathbb{V}_{\mathbf{d},n}$ by defining the height of an element V of $\mathbb{V}_{\mathbf{d},n}$. For $V = (\mathbf{a}_1, \dots, \mathbf{a}_r)$, we set

$$\mathfrak{H}(V) = \max_{1 \leq i \leq r} H_{N(d_i,n)-1}(\mathbf{a}_i)^r.$$

Finally, for $A \geq 1$, we let

$$\mathbb{V}_{\mathbf{d},n}(A) = \{V \in \mathbb{V}_{\mathbf{d},n}, \mathfrak{H}(V) \leq A\}.$$

In [5], the author introduces a probabilistic model which provides a prediction for the distribution of $\mathfrak{M}(V)$ in terms of $\mathfrak{H}(V)$ as V runs over $\mathbb{V}_{\mathbf{d},n}$. This model leads in particular to the following conjecture.

Conjecture 1. *For $t \in (0,1)$, we have the upper bound*

$$\limsup_{A\to\infty} \frac{\#\{V \in \mathbb{V}_{\mathbf{d},n}(A), \mathfrak{M}(V) \leq t\mathfrak{H}(V)\}}{\#\mathbb{V}_{\mathbf{d},n}(A)} \ll t.$$

We define

$$\delta_{\text{global}} = \lim_{A\to\infty} \frac{\#\{V \in \mathbb{V}_{\mathbf{d},n}(A), V(\mathbb{Q}) \neq \emptyset\}}{\#\mathbb{V}_{\mathbf{d},n}(A)},$$

if this limit exists. It is important to note here that we expect $\delta_{\text{global}} > 0$, which is the reason why Conjecture 1 is pertinent. Indeed, let

$$\delta_{\text{local}} = \lim_{A\to\infty} \frac{\#\{V \in \mathbb{V}_{\mathbf{d},n}(A), V(\mathbf{A}_{\mathbb{Q}}) \neq \emptyset\}}{\#\mathbb{V}_{\mathbf{d},n}(A)},$$

if this limit exists and where $V(\mathbf{A}_{\mathbb{Q}})$ denotes the set of adèles of V. In the case $r = 1$, Poonen and Voloch conjectured (see [6, Conjecture 2.2]) that $\delta_{\text{global}} = \delta_{\text{local}}$ and they showed (see [6, Theorem 3.6]) that $\delta_{\text{local}} > 0$. Moreover, they proved (see [6, Proposition 3.4]) that the equality $\delta_{\text{global}} = \delta_{\text{local}}$ follows from the conjecture of Colliot-Thélène (see [4] and [3]) asserting that the Brauer-Manin obstruction to the Hasse principle is the only one for smooth Fano hypersurfaces. In addition, Browning recently generalized (see [1, Theorem A]) their results to the case $r > 1$.

The main results established in [5] are the following.

Theorem 1. *If $r \leq n + 1 - d$ then Conjecture 1 holds.*

It is worth stressing that Theorem 1 implies in particular that Conjecture 1 holds if $r = 1$.

Corollary 1. *Assume that $r \leq n + 1 - d$. Let $\psi : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ be such that $\psi(u) = o(u)$ as $u \to \infty$. We have the equality*

$$\lim_{A\to\infty} \frac{\#\{V \in \mathbb{V}_{\mathbf{d},n}(A), \mathfrak{M}(V) > \psi(\mathfrak{H}(V))\}}{\#\mathbb{V}_{\mathbf{d},n}(A)} = 1.$$

The probabilistic model introduced in [5] leads to the expectation that $\mathfrak{M}(V)$ and $\mathfrak{H}(V)$ should typically have comparable size. Therefore, Corollary 1 is expected to be optimal.

The topics addressed in [5] have not been much studied. However, we note that Brüdern and Dietmann have investigated the case of diagonal hypersurfaces, which is of course much harder. They have obtained the analog of Conjecture 1 for these families under the assumption that $n + 1 - d \geq d$ (see [2, Theorem 1.4]) but unfortunately, the case $n + 1 - d = 1$ seems to be far out of reach.

References

[1] Browning, T. D., How often does the Hasse principle hold?, Preprint,2016.

[2] Brüdern, J. and Dietmann, R.,Random Diophantine equations, I, Adv. Math., 256, 2014, 18–45.

[3] Colliot-Thélène, J.-L., Points rationnels sur les fibrations, Higher dimensional varieties and rational points (Budapest, 2001), Bolyai Soc. Math. Stud., 12,171–221, Springer, Berlin, 2003.

[4] Colliot-Thélène, J.-L. and Swinnerton-Dyer, P., Hasse principle and weak approximation for pencils of Severi-Brauer and similar varieties, J. Reine Angew. Math., 453, 1994, 49–112.
[5] Le Boudec, P., Height of rational points on random Fano varieties, Preprint, 2017.
[6] Poonen, B. and Voloch, J. F., Random Diophantine equations, Arithmetic of higher-dimensional algebraic varieties (Palo Alto, CA, 2002), Progr. Math., 226, 175–184, with appendices by J.-L. Colliot-Thélène and N. M. Katz, Birkhäuser Boston, Boston, MA, 2004.

Unexpected biases in the distribution of consecutive primes

Robert J. Lemke Oliver
(joint work with Kannan Soundararajan)

While the sequence of primes is very well distributed in the reduced residue classes (mod q), the distribution of pairs of consecutive primes among the permissible pairs of reduced residue classes (mod q) is surprisingly erratic. We propose a conjectural explanation for this phenomenon, based on the Hardy-Littlewood conjectures, which fits the observed data very well. This conjecture has certain surprising consequences. For example, it follows from the conjecture that the distribution of triples or longer patterns of consecutive primes (mod q) is not Markovian. Another interesting consequence is a slight refinement of our conjecture which predicts that the number of occurrences of switching patterns always outnumbers the number of repeats among pairs of consecutive primes (mod 3) and (mod 4).

We also study the distribution of the terms predicted by the conjecture, which proves to be subtle and related to quantities of classical interest in analytic number theory. In particular, the terms predicted by the conjecture (mod q) are closely related to the Fourier transform of the Dedekind sums (mod q). We show that both have distribution functions. Moreover, these quantities are also related to an Omega-result on the error in $\sum_{n\leq x}\phi(n)$, which error we prove also possesses a distribution function.

Rational points on quartic hypersurfaces

Oscar Marmon
(joint work with Pankaj Vishe)

Let $F \in \mathbb{Z}[x_1, \dots, x_n]$ be a non-singular form of degree d, defining a hypersurface $X \subset \mathbb{P}^{n-1}$. By a classical result of Birch [1], X satisfies the Hasse principle provided that

$$n \geq 2^d(d-1)+1.$$

In the cubic case $d = 3$, this has been improved by Heath-Brown [4] to $n \geq 10$, and subsequently by Hooley [6] to $n \geq 9$. In the quartic case $d = 4$, Browning and Heath-Brown [2] showed that 41 variables suffice, and this was improved by Hanselmann [3] to $n \geq 40$. Our main result improves the situation further for quartic hypersurfaces. The Hasse principle is expressed in a quantitative form, in terms of the counting function

$$N(F,P) = \#\{\mathbf{x} \in \mathbb{Z}^n \cap [-P,P]^n \mid F(\mathbf{x}) = 0\}.$$

Theorem. Let $d = 4$ and $n \geq 37$. Then if $X(\mathbb{A}_{\mathbb{Q}}) \neq \emptyset$, there exist constants P_0 and $c > 0$ (depending on F) such that

$$N(F, P) \geq cP^{n-4} \quad \text{for } P \geq P_0.$$

(We have proved a result for general quartic forms, but in this talk we restrict to the case when F is non-singular.)

Our starting point for estimating $N(F, P)$ is the δ-version of the circle method, as developed by Heath-Brown in [5]. For a smoothly weighted version of our counting function

$$N_W(F, P) = \sum_{\substack{\mathbf{x} \in \mathbb{Z}^n \\ F(\mathbf{x})=0}} W(P^{-1}\mathbf{x})$$

and the corresponding weighted exponential sum

$$S(\alpha) = \sum_{\mathbf{x} \in \mathbb{Z}^n} W(P^{-1}\mathbf{x}) e(\alpha F(\mathbf{x})),$$

our version of the δ-method produces the following result.

Lemma. Given $Q \geq 1$ and $\theta > 0$, we have

$$N_W(F, P) = \sum_{q=1}^{Q} \int_{|z| < (qQ)^{-1+\theta}} p_q(z) \left(\sideset{}{^*}\sum_{a=1}^{q} S(a/q + z) \right) dz + O_{N,\theta}(P^n Q^{-N\theta}),$$

for any $N \geq 0$, where $p_q(z)$ is a smooth function satisfying

$$p_q(z) \ll 1$$

and

$$p_q(z) = 1 + O_N\left((q/Q)^N\right) \quad \text{for } |z| < Q^{-2}.$$

This formula resembles what could have been obtained from an application of the circle method. It may be thought of as an exact Kloosterman refinement, in that it allows for potential cancellation in the sum over residue classes $a \pmod q$.

Our treatment, like that of Browning and Heath-Brown [2], involves van der Corput differencing and Poisson summation, but in contrast to their treatment, we apply this to the sum

$$S(q, z) := \sideset{}{^*}\sum_{a=1}^{q} S(a/q + z)$$

rather than to each individual term separately. After the Poisson summation step, one is lead to estimate sums

$$\sum_{\mathbf{v} \in \mathbb{Z}^n} S_{\mathbf{h}}(q, \mathbf{v}) I_{\mathbf{h}}(z, q^{-1}\mathbf{v})$$

for varying $\mathbf{h} \in \mathbb{Z}^n$. The quantities $I_{\mathbf{h}}(z, q^{-1}\mathbf{v})$ are exponential integrals containing only cubic polynomials, which is essential for the analysis to work. The exponential sums $S_{\mathbf{h}}(q, \mathbf{v})$, on the other hand, are quartic in nature (in contrast to the situation in [2]). It turns out that bounding the exponential sums $S_{\mathbf{h}}(p, \mathbf{v})$ for prime moduli

p, using results by Katz, requires knowledge of the dimension, $s_p(\mathbf{h}, \mathbf{v})$ say, of the singular locus of the projective variety defined over $\mathbb{F}_p$ by the equations

$$F(\mathbf{x}) = \mathbf{h}.\nabla F(\mathbf{x}) = \mathbf{v}.\mathbf{x} = 0,$$

as p, $\mathbf{h}$ and $\mathbf{v}$ vary.

We believe that the number of variables needed in the theorem can be reduced below 37, and this is the subject of ongoing work.

References

[1] B. J. Birch. Forms in many variables. *Proc. Roy. Soc. Ser. A*, 265:245–263, 1961/1962.

[2] T. D. Browning and D. R. Heath-Brown. Rational points on quartic hypersurfaces. *J. Reine Angew. Math.*, 629:37–88, 2009.

[3] Markus Andreas Hanselmann. *Rational points on quartic hypersurfaces*. PhD thesis, Ludwig-Maximilians-Universität München, 2012.

[4] D. R. Heath-Brown. Cubic forms in ten variables. *Proc. London Math. Soc. (3)*, 47(2):225–257, 1983.

[5] D. R. Heath-Brown. A new form of the circle method, and its application to quadratic forms. *J. Reine Angew. Math.*, 481:149–206, 1996.

[6] Christopher Hooley. On nonary cubic forms. *J. Reine Angew. Math.*, 386:32–98, 1988.

Vinogradov's three primes theorem with primes from special sets

Kaisa Matomäki

(joint work with James Maynard and Xuancheng Shao)

Vinogradov showed in 1937 that every large enough odd integer can be represented as a sum of three primes. One may ask what if these primes are restricted to some subset of the primes. In general, if the set is badly distributed in congruence classes or Bohr sets, the result does not necessarily hold. Examples of such badly distributed sets include $\{p \in \mathbb{P}\colon p \equiv 1 \pmod 5\}$ and $\{p \in \mathbb{P}\colon \|\sqrt{2}p\| < 1/6 - \varepsilon\}$, where $\|x\|$ denotes the distance from x to the nearest integer.

In the talk I discuss two "transference type" results [1, 2] aimed to show that these are only sort of obstructions. As applications of the transference principles we show that Vinogradov's three primes theorem holds for Chen's primes (i.e. primes p for which $p + 2$ has at most two prime factors) and for almost equal primes (i.e., for any $\theta > 0.55$, every large enough odd integer N can be represented as $N = p_1 + p_2 + p_3$, where $|p_i - N/3| < N^\theta$ for each i).

References

[1] K. Matomäki and X. Shao, *Vinogradov's three primes theorem with almost twin primes*, pre-print (2015) available at arXiv.org as arXiv:1512.03213 [math.NT]

[2] K. Matomäki, J. Maynard and X. Shao *Vinogradov's theorem with almost equal summands*, pre-print (2016) available at arXiv.org as arXiv:1610.02017 [math.NT]

Primes with restricted digits

James Maynard

We present the following result, which shows there are infinitely many primes with no digit 7 in their decimal expansion.

Theorem 1. *Let $X \geq 4$ and $\mathcal{A} = \{\sum_{i\geq 0} n_i 10^i < X : n_i \in \{0,\dots,9\}\backslash\{7\}\}$ be the set of numbers less than X with no digit in their decimal expansion equal to 7. Then we have*

$$\#\{p \in \mathcal{A}\} \asymp \frac{\#\mathcal{A}}{\log X} \asymp \frac{X^{\log 9/\log 10}}{\log X}.$$

There are $\phi(10)\kappa_2\#\mathcal{A}/10$ elements of $\mathcal{A}$ which are coprime to 10, and there are $(10+o(1))X/\phi(10)\log X$ primes less than X which are coprime to 10. Thus if the properties 'being in $\mathcal{A}$' and 'being prime' where independent for integers $n < X$ coprime to 10, we would expect $(\kappa_2 + o(1))\#\mathcal{A}/\log X$ primes in $\mathcal{A}$. Theorem 1 shows such a heuristic guess is within a constant factor of the truth.

Our argument is fundamentally based on an application of the circle method. Assume X is a power of 10 for convenience. The number of primes in $\mathcal{A}$ is

$$\#\{p \in \mathcal{A}\} = \frac{1}{X}\sum_{0\leq a<X} S_{\mathcal{A}}\Big(\frac{a}{X}\Big)S_{\mathbb{P}}\Big(\frac{-a}{X}\Big),$$

where

$$S_{\mathcal{A}}(\theta) = \sum_{a\in\mathcal{A}} e(a\theta), \qquad S_{\mathbb{P}}(\theta) = \sum_{p<X} e(p\theta).$$

We then separate the contribution from the a in the 'major arcs' which give our expected main term for $\#\{p \in \mathcal{A}\}$, and the a in the 'minor arcs' which we bound for an error term.

We expect that $S_{\mathbb{P}}(\theta)$ is large only when θ is close to a rational with small denominator, and $S_{\mathcal{A}}(\theta)$ is large when θ has a decimal expansion containing many 0's or 9's. Thus we expect the product to be large only when both of these conditions hold, which is essentially when θ is well approximated by a rational whose denominator is a small power of 10. By standard techniques one can verify that amongst a in the major arcs $\mathcal{M}$ we obtain our expected main term, and this comes from when a/X is well-approximated by a rational with denominator 10.

It turns out that the Fourier transform $S_{\mathcal{A}}(\theta)$ has some somewhat remarkable features which cause it to typically have *better* than square-root cancellation. (A closely related phenomenon is present and crucial in the work of Mauduit and Rivat [2] and Bourgain [1], which have many similarities with our work.) Indeed, we establish the ℓ^1 bound

$$\sum_{0\leq a<X}\Big|S_{\mathcal{A}}\Big(\frac{a}{X}\Big)\Big| \ll \#\mathcal{A}\, X^{0.36}. \tag{1}$$

which shows that for 'generic' a we have $S_{\mathcal{A}}(a/X) \ll \#\mathcal{A}/X^{0.64} \ll X^{0.32}$. This gives us a (small) amount of room for a possible successful application of the circle method to this binary problem. We actually get good asymptotic control over all

moments (including fractional ones) of $S_{\mathcal{A}}(a/X)$ rather than just the first. By making a suitable approximation to $S_{\mathcal{A}}(\theta)$, we can re-interpret moments of this approximation as the average probability of restricted paths in a Markov process, and obtain asymptotic estimates via a finite eigenvalue computation.

By combining an ℓ^2 bound for $S_{\mathbb{P}}(a/X)$ with an $\ell^{1.526}$ bound for $S_{\mathcal{A}}(a/X)$, we are able to show that it is indeed the case that 'generic' $a < X$ make a negligible contribution, and that we may restrict ourselves to $a \in \mathcal{E}$, some set of size $O(X^{0.36})$.

Thus we are left to show when $a \in \mathcal{E}\backslash\mathcal{M}$, the product $S_{\mathcal{A}}(a/X)S_{\mathbb{P}}(-a/X)$ is small on average. By using an expansion of the indicator function of the primes as a sum of bilinear terms (similar to Vaughan's identity), we are led to bound expressions such as

$$\sum_{a_1,a_2\in\mathcal{E}\backslash\mathcal{M}} \Big|S_{\mathcal{A}}\Big(\frac{a_1}{X}\Big)S_{\mathcal{A}}\Big(\frac{a_1}{X}\Big)\Big| \sum_{n_1,n_2\leq N} \min\Big(\frac{X}{N}, \Big\|\frac{a_1n_1-a_2n_2}{X}\Big\|^{-1}\Big). \tag{2}$$

The double sum over n_1, n_2 in (2) is of size $O(N^2)$ for 'typical' pairs a_1, a_2, and if it is noticeably larger than this then (a_1, a_2) must share some Diophantine structure. We find that (a_1, a_2) must lie close to the projection from $\mathbb{Z}^3$ to $\mathbb{Z}^2$ of some low height plane or low height line if this quantity is large, where the arithmetic height of the line or plane is bounded by how large the double sum is.

This restricts the number and nature of pairs (a_1, a_2) which can give a large contribution. By using the explicit description of such pairs (a_1, a_2) we succeed in obtaining such a superior bound on the sum over these pairs. It is vital here that we are restricted to a_1, a_2 lying in the small set $\mathcal{E}$ (for points on a line) and outside of the set $\mathcal{M}$ of major arcs (for points in a lattice).

This ultimately allows us to get suitable bounds for (2) provided $N \in [X^{0.36}, X^{0.425}]$. If this range were larger, we would obtain an asymptotic estimate for $\#\{p \in \mathcal{A}\}$. Unfortunately our range is not large enough to do this. Instead we work with a minorant for the indicator function of the primes throughout our argument, which is chosen such that it is essentially a combination of bilinear expressions which do fall into this range. Such a minorant is constructed via Harman's sieve. This gives a lower bound

$$\#\{p \in \mathcal{A}\} \geq (c + o(1))\frac{\#\mathcal{A}}{\log X}$$

for some constant c. We use numerical integration to verify that we (just) have $c > 0$, and so we obtain our asymptotic lower bound for $\#\{p \in \mathcal{A}\}$.

References

[1] Jean Bourgain. Prescribing the binary digits of primes, II. *Israel J. Math.*, 206(1):165–182, 2015.

[2] Christian Mauduit and Joël Rivat. Sur un problème de Gelfond: la somme des chiffres des nombres premiers. *Ann. of Math. (2)*, 171(3):1591–1646, 2010.

Linear relations of zeros of the zeta function

Micah B. Milinovich
(joint work with William Banks, Greg Martin, Nathan Ng)

The *Linear Independence Conjecture* (LIC) predicts that the positive ordinates of the nontrivial zeros of Riemann zeta-function, $\zeta(s)$, are linearly independent over the rational numbers. There are a number of important consequences of LIC. For instance, it implies the Riemann Hypothesis (since if there is a nontrivial zero of $\zeta(s)$ off the critical line then there are two zeros with the same ordinate) and it implies that the zeros of $\zeta(s)$ are all simple. In addition, if $M(x) = \sum_{n\le x} \mu(n)$ where $\mu(n)$ is the Möbius function, then Ingham [3] showed that LIC implies that

$$\limsup_{x\to\infty} \frac{M(x)}{\sqrt{x}} = +\infty \quad \text{and} \quad \liminf_{x\to\infty} \frac{M(x)}{\sqrt{x}} = -\infty.$$

In particular, LIC implies that Mertens' conjecture is false (in a strong sense).

There seem to be very few results in the literature that study LIC directly, even in the simplest case of one linear relation. Fixing $\alpha > 0$, we seek a lower bound for the size of the set

$$\mathcal{S}_\alpha(T) := \left\{0 < \gamma \le T : \zeta(\tfrac{1}{2}+i\gamma) = 0 \text{ and } \zeta\left(\tfrac{1}{2}+i\alpha\gamma\right) \ne 0\right\}.$$

We henceforth assume the Riemann Hypothesis (RH). Then LIC predicts that

$$\#\mathcal{S}_\alpha(T) = \#\left\{0 < \gamma \le T : \zeta(\tfrac{1}{2}+i\gamma) = 0\right\} = \frac{T}{2\pi}\log\frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T)$$

as $T \to \infty$ for every positive $\alpha \in \mathbb{Q} \setminus \{1\}$. Moreover, for $\alpha \notin \mathbb{Q}$, we expect that $\zeta(\frac{1}{2} + it)$ and $\zeta(\frac{1}{2} + i\alpha t)$ should simultaneously vanish at only finitely many t. Therefore this asymptotic formula should hold for all positive $\alpha \ne 1$ as well. A straightforward counting argument shows that $\#\mathcal{S}_\alpha(T) \ge \left(\frac{1-\alpha}{2\pi} + o(1)\right) T\log T$ when $0 < \alpha < 1$. For rational values of α in a certain range, we are able to prove the following result in the more difficult case where $\alpha > 1$.

Theorem. *Assume RH. Let $\alpha \in \mathbb{Q}$ with $1 < \alpha \le 2$, and let $\varepsilon > 0$ be arbitrary. Then $\#\mathcal{S}_\alpha(T) \gg_{\varepsilon,\alpha} T^{1-\varepsilon}$ as $T \to \infty$.*

It is likely that this inequality can be improved slightly using ideas in [4] and [5], and we are investigating this possibility. Using different methods (and ideas from the proof of the Piatetski–Shapiro prime number theorem), we are also trying to prove that $\#\mathcal{S}_\alpha(T) \gg_\alpha T\log T$, a positive proportion result, for all real $\alpha \in (1, 1+\delta)$ for some small $\delta > 0$. Moreover, we are in the process of extending these ideas to other L-functions and to more general linear combinations of zeros.

Let $\alpha \in \mathbb{Q} \cap (1, 2]$. The proof of the theorem begins with the observation that if $H(s)$ is an analytic function which is bounded on the critical line, then

$$\left|\sum_{0<\gamma\le T} H(\tfrac{1}{2}+i\gamma)\,\zeta\left(\tfrac{1}{2}+i\alpha\gamma\right)\right| \ll \sum_{0<\gamma\le T} \left|\zeta\left(\tfrac{1}{2}+i\alpha\gamma\right)\right|. \tag{1}$$

For various choices of $H(s)$, we can use explicit formula methods (which relate sums over zeros of $\zeta(s)$ to sums over primes) and stationary phase techniques to

estimate the sum on the left-hand side of (1). We have to choose $H(s)$ in such a way that we can simultaneously handle the stationary phase estimates and ensure that the sum remains as large as possible. This idea is inspired by two papers from the 1980s that studied simple zeros of degree two L-functions [1, 2].

Let $\alpha = a/q$ with $(a,q) = 1$, and let $\mathcal{A} = \{n \in \mathbb{N} : n = k^q \text{ with } k \in \mathbb{N}\}$. For the choice $H(s) = \chi(1-s)$ where $\zeta(s) = \chi(s)\zeta(1-s)$, we show that

$$\Big| \sum_{0<\gamma\le T} H\big(\tfrac{1}{2}+i\gamma\big)\,\zeta\big(\tfrac{1}{2}+i\alpha\gamma\big)\Big| \;=\; \Big| \sum_{mn^\alpha \le \frac{T}{2\pi}} \Lambda(m) n^{(\alpha-1)/2} e\big(mn^\alpha\big)\Big| + o_\alpha(T)$$

as $T \to \infty$, where $\Lambda(m)$ is the von Mangoldt function and $e(x) = e^{2\pi i x}$. (This estimate is slightly different when $\alpha = 2$.) The terms with $n \in \mathcal{A}$ in the sum on the right-hand side of the above equation contribute an amount that is $\sim \frac{T}{2\pi}\zeta\big(\frac{a+q}{2}\big)$. The remaining terms contribute an amount that is $o(T)$. We show this by splitting the remaining sum into $O(\log^2 T)$ dyadic sums of the form

$$\sum_{\substack{M<m\le 2M\\ N<n\le 2N}}{\sum}^{\star} \Lambda(m) n^{(\alpha-1)/2} e\big(mn^\alpha\big)$$

where the superscript $\star$ indicates the sum is restricted to $n \notin \mathcal{A}$. If M is small, we estimate these sums trivially. If M is large, say $T/(\log T)^c \le M \le T$ for some $c > 0$, then we estimate these sums using Vaughan's identity for sums of the von Mangoldt function and the Diophantine nature of the sequence $\{n^\alpha\}$ as n varies.

This analysis allows us to conclude that the sum on the right-hand side of (1) is $\gg T$. On the other hand, this sum is $\ll T^\varepsilon \cdot \#\mathcal{S}_\alpha(T)$ for any $\varepsilon > 0$ since there are $\#\mathcal{S}_\alpha(T)$ nonzero terms in the sum and $|\zeta(\frac{1}{2}+it)| \ll_\varepsilon (|t|+1)^\varepsilon$ (under RH). Combining these two estimates, the theorem follows.

References

[1] J. B. Conrey, A. Ghosh, *Simple zeros of the Ramanujan τ-Dirichlet series*, Invent. Math. **94** (1988), no. 2, 403–419.

[2] J. B. Conrey, A. Ghosh, S. M. Gonek, *Simple zeros of the zeta function of a quadratic number field. I.*, Invent. Math. **86** (1986), no. 3, 563–576.

[3] A. E. Ingham, *On two conjectures in the theory of numbers*, Amer. J. Math. **64**, (1942). 313–319.

[4] M. B. Milinovich, N. Ng, *Simple zeros of modular L-functions*, Proc. Lond. Math. Soc. (3) **109** (2014), no. 6, 1465–1506.

[5] K. Soundararajan, *Moments of the Riemann zeta function*, Ann. of Math. (2) **170** (2009), no. 2, 981–993.

Real and rational system of forms

Simon L. Rydin Myerson

Let $\boldsymbol{f}(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]^R$ be a system of R homogeneous forms of the same degree $d \geq 2$, with integer coefficients, in n variables. Define the counting function

$$N(P) \stackrel{\text{def}}{=} \#\left\{\boldsymbol{x} \in \mathbb{Z}^n : \boldsymbol{f}(\boldsymbol{x}) = \boldsymbol{0},\, |\boldsymbol{x}|_\infty \leq P\right\}.$$

A classic result of Birch estimates $N(P)$ when the number of variables n is sufficiently large and $\boldsymbol{f}$ is suitably nonsingular. In particular, his work implies:

Theorem 1 (Birch [1])**.** *If $V(\boldsymbol{f}) \subset \mathbb{P}^{n-1}$ is smooth with dimension $n-R-1$, and*

$$n \geq R(R+1)(d-1)2^{d-1} + R \tag{$\star$}$$

then the equation $\boldsymbol{f}(\boldsymbol{x}) = \boldsymbol{0}$ satisfies the Hasse principle, and

$$N(P) \sim \nu P^{n-dR}$$

as $P \to \infty$, for some real constant $\nu \geq 0$.

The proof uses the circle method. Birch's work has been very widely generalised, for example to systems of forms with differing degrees by Browning and Heath-Brown [2], to linear spaces of solutions by Brandes [3], to bihomogeneous forms by Schindler [4], and to function fields by Lee [5].

Despite this, improvements in the condition ($\star$) have until now been confined to the case $R = 1$, with the exception of the case $(d, R) = (2, 2)$ where ($\star$) has been improved from $n \geq 14$ to $n \geq 11$ by Munshi [6].

In a series of forthcoming papers [7, 8, 9] I prove the following result.

Theorem 2 (RM)**.** *If either $d \leq 3$, or $\boldsymbol{f}$ is in general position, we may replace the condition ($\star$) in Birch's result with*

$$n \geq d2^d R + R. \tag{$\dagger$}$$

This improves on ($\star$) in each of the following three cases: either $d = 2$ and $R \geq 4$, or $d = 3$ and $R \geq 3$, or $d \geq 4$ and $R \geq 2$. The "general position" condition can be made explicit, and is in some sense a nonsingularity condition.

According to the "square-root cancellation" heuristic, in place of ($\star$) one would expect the condition $n \geq 2dR + 1$ to suffice. Since ($\star$) is linear in R, it brings us within a constant factor of square-root cancellation if $d \geq 2$ is held fixed.

I also give a generalisation of Theorem 1 to systems of forms with real coefficients. Let $\boldsymbol{g}(\boldsymbol{x}) \in \mathbb{R}[\boldsymbol{x}]^R$ be a system of R forms in n variables of degree $d \geq 2$ with real coefficients. Define

$$M_{\boldsymbol{g}}(P, Q) \stackrel{\text{def}}{=} \#\left\{\boldsymbol{x} \in \mathbb{Z}^n : |\boldsymbol{g}(\boldsymbol{x})|_\infty \leq Q,\, |\boldsymbol{x}|_\infty \leq P\right\}.$$

We say $\boldsymbol{g}(\boldsymbol{x})$ is *irrational* if there is no $\boldsymbol{\alpha} \in \mathbb{R}^R \setminus \{\boldsymbol{0}\}$ for which $\sum_i \alpha_i g_i(\boldsymbol{x}) \in \mathbb{Z}[\boldsymbol{x}]$ has integral coefficients. In [10] I prove

Theorem 3 (RM). *If $d \le 3$ let $V(\boldsymbol{g})$ be smooth of dimension $n - R - 1$. If $d \ge 4$ let $\boldsymbol{g}$ be in general position. Let $\rho \in [0, d-1)$, and if $\rho = 0$ let $\boldsymbol{g}$ be irrational. Suppose $V(\boldsymbol{g})$ has a real point and*

$$n \ge (d-\rho)2^d R + R.$$

Then for some real constant $\nu_\infty > 0$, we have in the limit as $P \to \infty$ that

$$M(P, P^\rho) \sim \text{measure}\,\{\boldsymbol{x} \in \mathbb{R}^n : |\boldsymbol{g}(\boldsymbol{x})|_\infty \le P^\rho,\ |\boldsymbol{x}|_\infty \le P\} \sim \nu_\infty P^{n-(d-\rho)R}.$$

The case $d = 2$ of this result is essentially due to Müller [11], or to Bentkus and Götze [12] when $R = 1$.

Note that when $\rho > 0$, Theorem 3 applies to systems of forms with either real or rational coefficients. Only in the case $\rho = 0$ is it necessary to impose an irrationality condition. This is because an inequality of the form $|f(\boldsymbol{x})| \ll 1$, where f has integral coefficients, would lead to p-adic conditions on the variables $\boldsymbol{x}$ and the asymptotic formula in Theorem 3 would need to be modified accordingly.

The strategy of proof for Theorems 2 and 4 reduces the problem to an upper bound for the number of solutions to a system of multilinear auxiliary inequalities described in [7].

When $d = 2$ these inequalities are linear and the required upper bound is not difficult. When $d = 3$ a strategy of Davenport [13] can be used to treat the problem.

The case $d \ge 4$ seems more difficult, but when $\boldsymbol{f}$ is in general position the auxiliary inequalities cannot be very singular and consequently an upper bound can be obtained by elementary means. It might be hoped that one could generalise Davenport's approach to $d \ge 4$, and so remove the "general position" condition from Theorems 2 and 3.

References

[1] B. J. Birch. Forms in many variables. *Proc. Roy. Soc. Ser. A*, 265:245–263, 1961/1962.
[2] T. Browning and D. Heath-Brown. Forms in many variables and differing degrees. *Journal of the European Mathematical Society*, 12 2014.
[3] J. Brandes. Forms representing forms and linear spaces on hypersurfaces. *Proc. Lond. Math. Soc. (3)*, 108(4):809–835, 2014.
[4] D. Schindler. Bihomogeneous forms in many variables. *J. Théor. Nombres Bordeaux*, 26(1):483–506, 2014.
[5] S.-l. A. Lee. Birch's theorem in function fields. *ArXiv e-prints*, Sept. 2011. arXiv:1109.4953.
[6] R. Munshi. Pairs of quadrics in 11 variables. *Compos. Math.*, 151(7):1189–1214, 2015.
[7] S. L. Rydin Myerson. Systems of quadratic forms. *ArXiv e-prints*, Dec. 2015. arXiv:1512.06003.
[8] S. L. Rydin Myerson. Systems of cubic forms. In preparation.
[9] S. L. Rydin Myerson. Systems of forms of the same degree. In preparation.
[10] S. L. Rydin Myerson. Diophantine inequalities in many variables. In preparation.
[11] W. Müller. Systems of quadratic Diophantine inequalities and the value distribution of quadratic forms. *Monatsh. Math.*, 153(3):233–250, 2008.
[12] V. Bentkus and F. Götze. Lattice point problems and distribution of values of quadratic forms. *Ann. of Math. (2)*, 150(3):977–1027, 1999.
[13] H. Davenport. Cubic forms in sixteen variables. *Proc. Roy. Soc. Ser. A*, 272:285–303, 1963.

On ℓ-torsion in class groups of number fields of arbitrary degree

Lillian B. Pierce
(joint work with M. M. Wood and C. Turnage-Butterbaugh)

Let K be an extension of $\mathbb{Q}$ of degree n, with absolute discriminant $D_K = |\mathrm{Disc} K/\mathbb{Q}|$. The ideal class group Cl_K is a finite abelian group, and for any integer $\ell \geq 1$, we may consider the ℓ-torsion subgroup of Cl_K given by

$$\mathrm{Cl}_K[\ell] := \{[\mathfrak{a}] \in \mathrm{Cl}_K : [\mathfrak{a}]^\ell = \mathrm{Id}\}.$$

It is natural to ask about the cardinality of the ℓ-torsion subgroup, either for a fixed field K, or as K varies within a family of fields of fixed degree. It is conjectured that for every K and every integer $\ell \geq 1$, $|\mathrm{Cl}_K[\ell]| \ll_{\varepsilon,\ell,n} D_K^{\varepsilon}$. This conjecture has been recorded by Brumer and Silverman, who were motivated by counting elliptic curves with fixed conductor; by Duke, who was motivated by the discriminant multiplicity conjecture, which asserts that given $D \geq 1$, at most D^{ε} fields of any fixed degree can have discriminant D; and by S. Zhang, who was motivated by questions about CM points on Shimura varieties; it is also related to the heuristics of Cohen and Lenstra. In almost all cases, the best known unconditional result is still the trivial bound $|\mathrm{Cl}_K[\ell]| \leq |\mathrm{Cl}_K| \ll_{n,\varepsilon} D_K^{1/2+\varepsilon}$. The most universally applicable nontrivial bound is conditional on GRH, and takes the form

$$|\mathrm{Cl}_K[\ell]| \ll_{n,\ell,\varepsilon} D_K^{\frac{1}{2}-\frac{1}{2\ell(n-1)}+\varepsilon}. \tag{1}$$

This is due to Ellenberg and Venkatesh, and arises from the provision (under GRH) of sufficiently many small rational primes that split completely in K.

In our forthcoming work, by studying $|\mathrm{Cl}_K[\ell]|$ as K varies over an appropriate family of number fields, we can recover the bound (1) for all but a possible zero-density subfamily, without assuming GRH, although for certain families we must assume other well-known conjectures. The families we study are defined in terms of the Galois group of the Galois closure, and certain ramification restrictions on all primes that ramify tamely in K. We mention here two examples of our results.

A first result, for cyclic number fields, is completely unconditional. Let G be a cyclic group of order $n \geq 2$. Let $\mathcal{F}(X)$ be the family of Galois extensions $K/\mathbb{Q}$ with $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$ as a permutation group and with $D_K \in (0, X]$ and such that all rational primes ramifying in K are totally ramified. Then $|\mathcal{F}(X)|$ grows like a power of X, while at most $O(X^{\varepsilon})$ fields in the family can possibly violate (1).

As a second result, let $n \geq 2$ be fixed and let $\mathcal{F}(X)$ be the family of degree n extensions $K/\mathbb{Q}$ with square-free $D_K \in (0, X]$ such that the Galois closure $\tilde{K}$ has $\mathrm{Gal}(\tilde{K}/\mathbb{Q}) \simeq S_n$ as a permutation group. Then assuming the Malle-Bhargava principle, the strong Artin conjecture, and the discriminant multiplicity conjecture, $|\mathcal{F}(X)|$ grows like a power of X, while at most $O(X^{\varepsilon})$ fields in the family can possibly violate (1).

Other results of a similar nature are obtained for G a simple group, or a dihedral group. This work represents the first time that a nontrivial bound for ℓ-torsion has been exhibited for infinite families of high degree fields, for all integers $\ell \geq 1$.

Torsion of CM elliptic curves over number fields

Paul Pollack
(joint work with Abbey Bourdon, Pete L. Clark)

A remarkable theorem of Merel [5] asserts that if E is an elliptic curve defined over a number field F of degree d, then $\#E(F)[\mathrm{tors}] \leq T(d)$, where $T(d)$ is a constant depending only on d. While explicit admissible values of $T(d)$ are known, these grow (at least) exponentially with d. By contrast, it is widely conjectured that one can take $T(d)$ to grow polynomially in d. This conjecture is known for certain special families of elliptic curves. For instance, if E is an elliptic curve defined over a number field F of degree $d \geq 2$, and $j(E)$ is an algebraic integer, then Hindry and Silverman [4] have shown that

$$T(d) \leq 1977408 \cdot d \log d.$$

Elliptic curves with complex multiplication always have integral j-invariant, and so the Hindry–Silverman bound applies immediately to such curves. In this talk, we report on work with Clark [3] establishing a sharper result in this case. Specifically, if E is a CM elliptic curve defined over a degree d number field F, then

$$\#E(F)[\mathrm{tors}] \ll d \log\log d,$$

where the implied constant is absolute and effectively computable. This bound is best possible (up to the constant), as shown by a construction of Breuer [2]. Our proof uses the classical theory of complex multiplication, a recent theorem of Bourdon and Clark allowing one to reduce to the case when the CM order is maximal, and an estimate for the partial Euler products of $L(1, \chi)$, where χ is a quadratic Dirichlet character.

We also report on related statistical results obtained in joint work with Bourdon and Clark [1]. Let $T_{\mathrm{CM}}(d)$ denote the largest size of a torsion subgroup of a CM elliptic curve over a degree d number field. (Thus, the result of [3] is precisely that $T_{\mathrm{CM}}(d) \ll d \log\log d$.) We discuss estimates for the lower, average, and typical order of the function $T_{\mathrm{CM}}(d)$.

References

[1] A. Bourdon, P. L. Clark, P. Pollack, *Anatomy of torsion in the CM case*, Math Z. (to appear).
[2] F. Breuer, *Torsion bounds for elliptic curves and Drinfeld modules*, J. Number Theory **130** (2010), 1241–1250.
[3] P. L. Clark, P. Pollack, *The truth about torsion in the CM case*, Comptes Rendus Mathematique **353** (2015), 683–688.
[4] M. Hindry, J. Silverman, *Sur le nombre de points de torsion rationnels sur une courbe elliptique*, Comptes Rendus Mathematique **329** (1999), 97–100.
[5] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), 437–449.

Eigenvalues of the large sieve matrix

Maksym Radziwill
(joint work with Florin Boca)

The famous large sieve inequality is equivalent to the statement that the largest eigenvalue of the positive definite symmetric matrix

$$A^\star A := \Big(\sum_{\theta \in \mathcal{F}_Q} e((n-m)\theta) \Big)_{1 \le n,m \le N}$$

is $\le N + Q^2 - 1$. One would like to be able to refine the large sieve inequality to an asymptotic equality. For special sequences this has been (essentially) accomplished in the paper on the "Asymptotic Large Sieve" by Conrey, Iwaniec, Soundararajan. In the general case, a first step would be to understand the distribution of the eigenvalues of $A^\star A$ in the bulk (and not just the largest eigenvalue). In the regimes when $N/Q^2 \to 0$ or $N/Q^2 \to \infty$ the limiting behavior of the eigenvalues of $A^\star A$ is well understood (they all accumulate at one point). However in the remaining regime $N \sim \alpha Q^2$ (with $\alpha > 0$) Ramare conjectured that the eigenvalues, scaled by $1/N$, admit a non-trivial limiting distribution. I've discussed joint work with Florin Boca in which we settle Ramare's conjecture. We moreover gave an explicit description of the moments of the limiting measure and showed the continuity of the moments as α varies.

Arithmetic functions in short intervals and function field analogues

Brad Rodgers

1. We are interested in the variance of sums of arithmetic functions over random short intervals. An example of what we mean by this is the classical conjecture of Goldston and Montgomery on the variance of counts of primes over short intervals [2]; that for $H = X^\delta$ with $\delta \in (0,1)$ fixed,

$$\mathrm{Var}_{x \in [X,2X]} \Big(\sum_{x \le n \le x+H} \Lambda(n) \Big) \sim H(\log X - \log H).$$

Here variance may be understood in the usual sense:

$$\mathrm{Var}_{x \in [X,2X]} \Big(\sum_{x \le n \le x+H} \Lambda(n) \Big) := \frac{1}{X} \int_X^{2X} \Big(\sum_{x \le n \le n+H} \Lambda(n) - \mu_{X,H} \Big)^2 dx,$$

with

$$\mu_{X,H} := \frac{1}{X} \int_X^{2X} \Big(\sum_{x \le n \le x+H} \Lambda(n) \Big) dx \sim H.$$

One way to get a better understanding of conjectures of this sort is to consider analogues in a function field setting; this was done for the Goldston-Montgomery Conjecture in the not-too-distant-past by Keating and Rudnick [4], who proved an analogue in which the integers are replaced by the ring $\mathbb{F}_q[T]$, and $q \to \infty$.

2. We consider some variants of this conjecture, first with $\Lambda(n)$ replaced by $d_k(n)$, the k-fold divisor function.

Conjecture 1 (Keating – Rodgers – Roditty-Gershon – Rudnick [5])**.** *For* $\frac{\log H}{\log X} \to \delta$ *with* $\delta \in (0, 1 - 1/k)$,

$$\mathrm{Var}_{x\in[X,2X]}\Big(\sum_{x\le n\le x+H} d_k(n)\Big) \sim a_k H P_k(\delta)(\log X)^{k^2-1},$$

where a_k *is a certain arithmetic constant, and* $P_k(\delta)$ *is a certain piecewise-polynomial with 'phases' on the intervals*

$$\Big(0, \frac{1}{2}\Big),\ \Big(\frac{1}{2}, \frac{2}{3}\Big),\ \dots,\ \Big(\frac{k-2}{k-1}, \frac{k-1}{k}\Big),$$

and phase-changes in between.

Of particular interest are the at first surprising phase changes in the polynomial $P_k(\delta)$, which appear when $H = X^\delta$ grows at different orders.

Some justification for this conjecture is given by a function field analogue, proved in [5]: for fixed $0 \le h \le n-5$, as $q \to \infty$

$$\mathrm{Var}_{f\in\mathcal{M}_n}\Big(\sum_{g\in I(f;h)} d_k(g)\Big) \sim q^{h+1} p_k(n,h),$$

where $p_k(n,h)$ is a certain piecewise-polynomials in n and h satisfying

$$p_k(n,h) \sim P_k(\delta) n^{k^2-1} \quad \text{as} \quad \frac{h}{n} \to \delta.$$

Here we take the variance over random $f \in \mathcal{M}_n$, which denotes the collection of all monic degree n elements f of $\mathbb{F}_q[T]$. Likewise $I(f;h)$ is a short-interval around f, defined by $I(f;h) := \{g \in \mathbb{F}_q[T] :\ \deg(f-g) \le h\}$.

Additional evidence for the conjecture for certain ranges of δ includes the recent work: [6], [3], [8], [1].

3. Another variant considers $\omega(n)$, the number of distinct prime factors of n. In this case a function field analogy, proved in [7], once again leads us to speculate the following: that for $H = X^\delta$ with $\delta \in (0,1)$ fixed,

$$\mathrm{Var}_{x\in[X,2X]}\Big(\sum_{x\le n\le n+H} \omega(n)\Big) = O_\delta(H).$$

Such a result would be at least slightly surprising, since a different probabilistic model based upon the independence of $\omega(n)$ and $\omega(n+h)$ for random n and fixed h might lead one to expect that the variance is instead asymptotically $H \log\log X$.

4. We observe finally that in a function field setting, some of the behavior we have discussed above in evaluating the variance of short-interval sums of arithmetic functions can be illuminated by the following combinatorial observation, explained in greater depth in [7]: arithmetic functions such as Λ, d_k and ω can in each case be decomposed into a sum of functions $u+v$, where u is a regular enough arithmetic

function that the variance of its sum over short intervals is negligible, while v is oscillatory, and the variance of its sum over short intervals is given entirely by diagonal contributions. This decomposition changes based upon the size of the short-interval, elucidating the sometimes surprising changes seen in the variance evaluations above.

References

[1] R.de la Bretèche and D. Fiorilli. "Major arcs and moments of arithmetical sequences." *Preprint.* arXiv:1611.08312

[2] D.A. Goldston, and H.L. Montgomery. "Pair correlation of zeros and primes in short intervals." *Progress in Math* 70 (1987): 183–203.

[3] A. J. Harper, and K. Soundararajan. "Lower bounds for the variance of sequences in arithmetic progressions: primes and divisor functions." *Q.J. Math.*, to appear, 2016.

[4] J.P. Keating, and Z. Rudnick. "The variance of the number of prime polynomials in short intervals and in residue classes," *Int. Math. Res. Not.* 2014, no. 1 (2014): 259–288.

[5] J.P. Keating, B. Rodgers, E. Roditty-Gershon, and Z. Rudnick. "Sums of divisor functions in $\mathbb{F}_q[t]$ and matrix integrals," *Preprint.* arXiv:1404.3080

[6] S. Lester. "On the variance of sums of divisor functions in short intervals." *Proc. Amer. Math. Soc.* 144, no. 12 (2016): 5015–5027.

[7] B. Rodgers. "Arithmetic functions in short intervals and the symmetric group." *Preprint.* arXiv:1609.02967

[8] B. Rodgers, and K. Soundararajan. "The variance of divisor sums in arithmetic progressions." *Preprint.* arXiv:1610.06900

Quantum chaos, eigenvalue statistics and the Fibonacci sequence

Zeev Rudnick

One of the outstanding insights obtained by physicists working on "Quantum Chaos" is a conjectural description of local statistics of the energy levels of simple quantum systems according to crude properties of the dynamics of classical limit, such as integrability, where one expects Poisson statistics, versus chaotic dynamics, where one expects GOE statistics. I will describe in general terms what these conjectures say and discuss recent joint work with Valentin Blomer, Jean Bourgain and Maksym Radziwill, in which we study the size of the minimal gap between the first N eigenvalues for one such simple integrable system, a rectangular billiard having irrational squared aspect ratio. For certain quadratic irrationalities, such as the golden ratio, we show that the minimal gap is about $1/N$, consistent with Poisson statistics. In the case of the golden ratio, the problem involves some curious properties of the Fibonacci sequence. Just before the start of the workshop, the case of a general quadratic irrationality was done by Dan Carmon. We also give related results for a generic set of rectangles of full measure. The proofs use a variety of ideas of an arithmetical nature, involving Diophantine approximation, the theory of continued fractions, and results in analytic number theory.

Counting rational points on cubic curves

Per Salberger

Let C be an irreducible plane curve defined over Q of degree d and $N(C;B)$ the number of rational points of height at most B on C. It was then proved by Heath-Brown in 2002 that $N(C;B) = O_{d,\varepsilon}(B^{2/d+\varepsilon})$. The estimate is uniform in the sense that the implicit constant only depends on d and ε. In 2005 Ellenberg and Venkatesh obtained a slightly sharper estimate for curves of positive genus. For non-singular plane cubics they showed in particular that $N(C;B) = O(B^{2/3-405})$. This was then improved by Heath-Brown and Testa to $N(C;B) = O_\varepsilon(B^{2/3-1/110+\varepsilon})$. The aim of our talk was to present a proof of the following uniform estimate.

Theorem 1. *Let C be a non-singular irreducible plane cubic curve defined over Q. Then*

$$N(C;B) = O_\varepsilon(B^{2/3-1/84+\varepsilon}).$$

The proof follows the same basic strategy as in the previous papers. But there is one important new ingredient. Let $S \subset C \times C \times C$ be the surface of all points (P,Q,R) on $C \times C \times C$ such that the secant of P and Q intersects C in a third point lying on the tangent line of C at R. We then have the following result.

Lemma 1. *Let $N(S;B)$ be the number of rational points (P,Q,R) on S such that P and Q are of height at most B. Then $N(S;B) = O_\varepsilon(B^{2/3+\varepsilon})$.*

The proof of this lemma is difficult and uses a global version of Heath-Brown's p-adic determinant method developed by the author. The Riemann-Roch theorem for threefolds is also used in the proof. From this lemma, the inequality of Cauchy-Schwarz and descent theory one deduces the following result.

Lemma 2. *Let C be an irreducible plane curve defined by a non-singular ternary cubic form F over Q. Let $H(F)$ be the height of F. Then*

$$N(C;B) = O_\varepsilon(H(F)^3 B^{1/3+\varepsilon}).$$

The theorem follows from this lemma and the estimate

$$N(C;B) = O_\varepsilon(B^{2/3+\varepsilon}/H(F)^{1/9})$$

of Ellenberg-Venkatesh.

Equidistribution of zeros of polynomials

Kannan Soundararajan

Given a polynomial $P(z) = a_N z^N + a_{N-1} z^{N-1} + \ldots + a_0$ of degree N with complex coefficients (and $a_0 a_N \neq 0$), a classical theorem of Erdős and Turán [2] shows that if the values of the polynomial (suitably normalized) are small on the unit circle then the zeros cluster around the unit circle and are evenly distributed in argument. A more recent theme, with the work of Bilu [1] (with earlier work by

Langevin), has been to study the zeros of irreducible polynomials with integer coefficients, and replace conditions on the size of the polynomial by bounds on the Mahler measure. In this situation, a key role is played by the discriminant of the polynomial P, which is a non-zero integer, and therefore at least 1 in size. In my talk, I described a simplified proof of Bilu's theorem, which leads to better explicit quantified versions, as well as giving refinements of recent work of Pritsker, and refinements of work of Mignotte, Amoroso, and Dubickas on bounding resultants of polynomials in terms of their Mahler measure.

To state some sample results, we need a little notation. Let $P(z) \in \mathbb{C}[z]$ be as above, and let α_j (for $1 \leq j \leq N$) denote the zeros of P, so that $P(z) = a_N \prod_{j=1}^{N}(z - \alpha_j)$. The Mahler measure of P is defined as

$$M(P) = \exp\Big(\int_0^1 \log|P(e(\theta))|d\theta\Big) = |a_N| \prod_{j=1}^{N} \max\Big(1, |\alpha_j|\Big).$$

Given a complex number z, we define

$$\rho(z) = \begin{cases} z & \text{if } |z| \leq 1 \\ z/|z|^2 & \text{if } |z| > 1. \end{cases}.$$

In other words, consider inverting the complex plane about the unit circle; given a complex number z, the quantity $\rho(z)$ denotes either z or its image under inversion, whichever lies within the unit circle.

Theorem 1. *Let $P \in \mathbb{Z}[x]$ be a polynomial of degree $N \geq 2$ with no repeated roots. Then*

$$\sum_{m=1}^{\infty} \frac{e^{-2m/N}}{m} \Big|\sum_{j=1}^{N} \rho(\alpha_j)^m\Big|^2 \leq (2N-2)\log M(P) + N\log N.$$

Here are two consequences of this theorem.

Corollary 1. *Suppose $P \in \mathbb{Z}[x]$ is of degree $N \geq 2$ with no repeated roots, and with r_1 real roots and $2r_2$ complex roots. Then*

$$NM(P) \geq \exp\Big(\frac{\pi^2}{256}\frac{r_1^2}{N}\Big).$$

Corollary 2. *Suppose $P \in \mathbb{Z}[x]$ is of degree $N \geq 2$ with no repeated roots, and suppose θ is the length of the largest interval $I \in \mathbb{R}/\mathbb{Z}$ which does not contain the argument (divided by 2π) of any zero of P. Then*

$$NM(P) \geq \exp\Big(\frac{2}{15}\theta^2 N\Big).$$

References

[1] Y. Bilu, *Limit distribution of small points on algebraic tori*, Duke Math. J. **89** (1997), 465–476.

[2] P. Erdős and P. Turán, *On the distribution of roots of polynomials*, Ann. of Math. **51** (1950) 105–119.

Problem session

1. (Balazard) We begin by recalling a problem that Michel Balazard asked at a meeting here some years ago: Does there exist a Dirichlet series $D(s)$ that converges in some half-plane $\sigma > \alpha$ and has exactly one zero in this half-plane? The number α is not necessarily the abscissa of convergence of the Dirichlet series. If RH is true, then $1/\zeta(s)$ is such an example. The object is to create an unconditional example.

2. (Montgomery) Let $0 < \gamma_1 \le \gamma_2 \le \dots$ denote the ordinates of the zeros of the zeta function. Let

$$E = \limsup_{j\to\infty} \frac{\gamma_{j+1} - \gamma_j}{2\pi/(\log \gamma_j)} \,.$$

Clearly $E \ge 1$. R. R. Hall has used the asymptotic values of $\int_0^T |\zeta(1/2+it)|^2\,dt$ and $\int_0^T |\zeta(1/2+it)|^4\,dt$ to derive a larger lower bound for E. If one assumes the truth of the conjectures concerning the higher moments of the zeta function on the $1/2$ line, what can be derived? Possibly that $E = \infty$?

3. (Rudnick) With the zeros of the zeta function in mind, and the questions we ask about them, consider similarly the eigenvalues of Maass forms,

$$f \in L^2\Big(SL_2(\mathbb{Z})\backslash\mathbb{H}\Big), \qquad \Delta f_j = \lambda_j f_j \,.$$

Here $0 < \lambda_1 \le \lambda_2 \le \dots$. The number of λ_j not exceeding x is asymptotic to cx, so the average gap $\lambda_{j+1} - \lambda_j$ is $1/c$. We have two problems: Show that the liminf of the gaps is 0, and that the limsup of the gaps is ∞.

4. (Fouvry) Suppose that $p > 3$ and that $t \not\equiv 0 \pmod p$. Let $E_p(t)$ denote the curve (mod p) given by

$$x + \frac{1}{x} + y + \frac{1}{y} = t \,.$$

Then $\#E_p(t) = \#E_p(16/t)$. Is there a bijective proof of this, in which points of $E_p(t)$ are mapped to $E_p(16/t)$, through some magic formula? A proof of this result is found in Kowalski's blog. Granville comments that there may be papers of Lalin and Rodriguez Villegas that are relevant.

5. (Heath-Brown) Let

$$S = \{n \in \mathbb{N} : p|n \implies p \equiv 3 \pmod 4\} \,.$$

Is it true that every sufficiently large even number is the sum of two members of S? That is, $2N = S + S$ for $N > N_0$.

6. (Granville) My good friend Javier Cilleruelo passed away recently, and left behind some mathematical questions that I associate with him. Suppose that m is highly composite, and consider those x such that $x^2 \equiv a \pmod m$. Order these

numbers as $0 < x_1 < x_2 < \cdots < x_K < m$, where $K = \tau(m)$. Fix $\varepsilon > 0$, show that there exists a B_ε such that

$$\#\{x_i \in [y, y + m^{1-\varepsilon}]\} \le B_\varepsilon$$

7. (Granville) Consider the lattice points in the curve $x^2 + y^2 = n$ where $n = p_1 p_2 \cdots p_k$, with distinct primes $p_j \equiv 1 \pmod 4$. There are 2^{k+2} such points. Can there exist two such lattice points very close together? Yes. How about 3 points? They cannot all be within $cR^{1/3}$. For four points we have the same lower bound. For 5 points one can construct a proof that such points are $> cR^{2/5}$ apart. For 6 points, the same, and for 7 points the separation is $> cR^{3/7}$. Can one achieve points that are this close together?

8. (Friedlander) We recall the problem of gaps between sums of two squares, which is $O(x^{1/4})$. By the same method, we can construct numbers a and b so that $a^2 - b^2$ is within $O(n^{1/4})$ of n. Hence there exists a number m with $|m - n| \ll n^{1/4}$, such that $P(m) \ll n^{1/2}$. Can one improve on this? A paper of Friedlander and Lagarias (J. Number Theory 25 (1987), 249–273) is relevant here. The result mentioned above was independently discovered by Balog.

9. (Vaughan–Gafni) Consider the curve $\boldsymbol{x} = (x, x^2, x^3)$. Suppose that $\psi(q)$ is monotonically decreasing to 0. If $\sum_{q=1}^{\infty} \psi(q)^3 < \infty$, does it follow that the set of $\boldsymbol{x}$ for which the inequality $|q\boldsymbol{x} - \boldsymbol{a}| < \psi(q)$ has infinitely many solutions is a set of measure 0. We ask also for a proof that conversely, if the sum diverges, then the inequality has infinitely many solutions for almost all $\boldsymbol{x}$.

10. (Browning) Let $r(n)$ denote the number of ways of writing n as a sum of two squares. Show that there is a positive constant δ such that

$$\sum_{m,\, n \le x} r(m^5 + n^5) \gg x^{1+\delta}\,.$$

The lower bound $\gg x$ is known.

11. (Wooley) Let $p_1 < p_2 < \cdots$ be the sequence of all prime numbers, and let $q_1 < q_2 < \cdots$ be the sequence of all primes that are $\equiv 3 \pmod 4$. Put $P = p_1 p_2 \cdots p_k$, $Q = q_1 q_2 \cdots q_k$. Euclid showed that the least prime factor of $P + 1$ is p_{k+r} for some $r > 0$, and that $4Q - 1$ and $4Q + 3$ have prime factors of the form q_{k+r} with $r > 0$. The proposer has recently shown that the least prime divisor of

$$P^{P^P} - 1$$

is p_{k+1}. Can one define a similar expression, a function of Q, with the property that its least prime divisor is q_{k+1}?

12. (Wooley) Let $C(x_1, x_2, \ldots, x_s) \in \mathbb{Z}[x_1, x_2, \ldots, x_s]$ be a homogeneous cubic polynomial. It is conjectured that if $s \ge 10$, then the number of solutions of $C(x_1, x_2, \ldots, x_s) = 0$ with integral variables in the box $|x_i| \le B$ is $\gg B^{s-9}$. We

know that if N is a cubic norm form, then there is a prime number p such that the only solution $\boldsymbol{x} \in \mathbb{Z}^9$ of the equation

$$N(x_1, x_2, x_3) + pN(x_4, x_5, x_6) + p^2 N(x_7, x_8, x_9) = 0$$

is $\boldsymbol{x} = \mathbf{0}$. Putting $x_i = L_i(y_1, y_2, \dots, y_s)$ where the L_i are certain linear forms, we deduce that the number of solutions of

$$N(L_1, L_2, L_3) + pN(L_4, L_5, L_6) + p^2 N(L_7, L_8, L_9) = 0$$

in $|y_i| \le B$ is $\ll B^{s-9}$.

Consider quadratic polynomials $Q_1, Q_2, \dots, Q_h \in \mathbb{Z}[y_1, y_2, \dots, y_t]$, and let $x_1, x_2, \dots, x_h$ be fixed integers with $|x_i| \le B^\theta$. Is it true that for a positive proportion of these $\boldsymbol{x}$ one has

$$\#\{x_1 Q_1(\boldsymbol{y}) + x_2 Q_2(\boldsymbol{y}) + \cdots + x_h Q_h(\boldsymbol{y}) = 0,\ |y_i| \le B\} \gg B^{t-2-\theta}$$

for some θ with

$$\frac{h-7}{h-1} \le \theta < 1\,?$$

This is related to the h-invariant of a cubic form — the least integer h such that

$$C = L_1 Q_1 + \cdots + L_h Q_h,$$

for linear forms L_i and quadratic forms Q_i. When $h \ge 15$, the circle method applies to show that

$$\#\{C(\boldsymbol{x}) = 0, |\boldsymbol{x}| \le B\} \gg B^{s-3}\,.$$

So one is left to deal with h with $10 \le h \le 15$, to which cases the problem on quadratic polynomials is relevant.

13. (Granville) A number of books mention that the Diophantine equation $3x^3 + 4y^3 + 5z^3 = 0$ has no solution, despite being everywhere locally solvable. However, usually a proof of this is not provided, and when it is, it is not a very attractive proof. Mordell, in his book on Diophantine equations, uses the fact that if $p = a^2 + 3b^2$, then 2 is a cube modulo p if and only if $3|b$, to show that the equation $x^3 + 3y^3 + 20z^3 = 0$ has no solution, despite being everywhere locally solvable. Better proofs in this area are needed.

14. (Goldmakher) Let $K_q(a) = \mathbb{Q}\big(e(1/q), a^{1/q}\big)$. By the Chebotarev density theorem, the primes that split completely in $K_q(a)$ have density

$$\frac{1}{|K_q(a) : \mathbb{Q}|} = \frac{1}{q\phi(q)}\,.$$

Thus

$$\pi(x; K_q(a)) \sim \frac{\pi(x)}{q\phi(q)}\,.$$

If we assume RH for $\zeta_{K_q(a)}(s)$, then we have a quantitative estimate,

$$\pi(x; K_q(a)) = \frac{\pi(x)}{q\phi(q)} + O\big(\sqrt{x}\log(aqx)\big)\,.$$

Lagarias and Odlyzko showed unconditionally that the above holds with the error term

$$O\Big(x \exp\Big(-c\sqrt{\frac{\log x}{q\phi(q)}}\ \Big)\Big).$$

Problem: Show that

$$\frac{1}{\pi(x)} \sum_{q\le x} \pi(x; K_q(a)) = o\big(\sqrt{\log\log x}\big)\,.$$

Let $\ell_a(p)$ denote the order of a modulo p. The estimate above would allow one to show that $\omega\big(\ell_a(p)\big)$ is normally distributed in the manner of the Erdős–Kac law.

Reporter: Jörg Brüdern

Participants

Prof. Dr. Valentin Blomer
Mathematisches Institut
Georg-August-Universität Göttingen
Bunsenstrasse 3-5
37073 Göttingen
GERMANY

Dr. Thomas Bloom
School of Mathematics
University of Bristol
Howard House
Queens Avenue
Bristol BS8 1SN
UNITED KINGDOM

Dr. Andriy V. Bondarenko
Department of Mathematical Sciences
NTNU
7491 Trondheim
NORWAY

Prof. Dr. Tim D. Browning
Department of Mathematics
University of Bristol
University Walk
Bristol BS8 1TW
UNITED KINGDOM

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

Dr. Sam Chow
Department of Mathematics
University of York
Heslington, York YO10 5DD
UNITED KINGDOM

Prof. Dr. Alina Carmen Cojocaru
Department of Mathematics
University of Illinois at Chicago
SEO 322
851 Morgan Street
Chicago, IL 60607
UNITED STATES

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

Fabian Dehnert
Mathematisches Institut
Georg-August-Universität Göttingen
Bunsenstrasse 3-5
37073 Göttingen
GERMANY

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

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

Alexandra Florea
Department of Mathematics
Stanford University
Building 380
Serra Mall
Stanford CA 94305-2125
UNITED STATES

Prof. Dr. Etienne Fouvry
Laboratoire de Mathématiques
Université Paris Sud (Paris XI)
Batiment 425
91405 Orsay Cedex
FRANCE

Dr. Christopher Frei
Institut für Analysis und Zahlentheorie
Technische Universität Graz
Kopernikusgasse 24/II
8010 Graz
AUSTRIA

Prof. Dr. John B. Friedlander
Department of Mathematics
University of Toronto, Scarborough
Scarborough College
Toronto ON M1C 1A4
CANADA

Dr. Ayla Gafni
Department of Mathematics
University of Rochester
P.O. Box 2770138
Rochester, NY 14627
UNITED STATES

Dr. Leo Goldmakher
Department of Mathematics
Bronfman Science Center
Williams College
Williamstown, MA 01267
UNITED STATES

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

Dr. Brandon Hanson
Department of Mathematics
Penn State University
University Park PA 16802
UNITED STATES

Dr. Adam J. Harper
Mathematics Institute
University of Warwick
Zeeman Building
Coventry CV4 7AL
UNITED KINGDOM

Prof. Dr. Roger Heath-Brown
Mathematical Institute
Oxford University
24-29 St. Giles
Oxford OX1 3LB
UNITED KINGDOM

Prof. Dr. Harald 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 & Computer Science
A. Mickiewicz University
ul. Umultowska 87
61-614 Poznań
POLAND

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

Dr. Pierre Le Boudec
École Polytechnique Fédérale de Lausanne
SB IMB
Station 8
1015 Lausanne
SWITZERLAND

Prof. Dr. Robert J. Lemke Oliver
Department of Mathematics
Tufts University
Medford, MA 02155
UNITED STATES

Prof. Dr. Jianya Liu
Department of Mathematics
Shandong University
27 Shanda Nanlu, Jinan
Shandong 250 100
CHINA

Prof. Dr. Helmut Maier
Abteilung Zahlentheorie und Wahrscheinlichkeitstheorie
Universität Ulm
89069 Ulm
GERMANY

Dr. Oscar Marmon
Department of Mathematical Sciences
University of Copenhagen
Universitetsparken 5
2100 København
DENMARK

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

Dr. James A. Maynard
Magdalen College
University of Oxford
Oxford OX1 4AU
UNITED KINGDOM

Prof. Dr. Micah B. Milinovich
Department of Mathematics
University of Mississippi
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. Ramon Moreira Nunes
EPFL
MA-C3-534 (Bâtiment MA)
Station 8
1015 Lausanne
SWITZERLAND

Simon Myerson
Department of Mathematics
University College London
Gower Street
London WC1E 6BT
UNITED KINGDOM

Prof. Dr. Scott T. Parsell
Department of Mathematics
West Chester University
25 University Avenue
West Chester, PA 19383
UNITED STATES

Prof. Alberto Perelli
Dipartimento di Matematica
Universita 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. Janos Pintz
Alfred Renyi Institute of Mathematics
Hungarian Academy of Sciences
P.O.Box 127
1364 Budapest
HUNGARY

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

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

Dr. Olivier Robert
Institut Camille Jordan, CNRS UMR 5208
Universités de Lyon & de Saint-Etienne
23, rue du Dr. Paul Michelon
42000 Saint-Étienne Cedex 02
FRANCE

Dr. Brad Rodgers
Department of Mathematics
University of Michigan
530 Church Street
Ann Arbor, MI 48109-1043
UNITED STATES

Prof. Dr. Zeev Rudnick
Department of Mathematics
School of Mathematical Sciences
Tel Aviv University
Ramat Aviv
Tel Aviv 69978
ISRAEL

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

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

Prof. Dr. Kristian Seip
Department of Mathematical Sciences
NTNU
7491 Trondheim
NORWAY

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

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

Dr. Pankaj H. Vishe
Department of Mathematical Sciences
Durham University
Science Laboratories
South Road
Durham DH1 3LE
UNITED KINGDOM

Prof. Dr. Trevor D. Wooley
Department of Mathematics
University of Bristol
University Walk
Bristol BS8 1TW
UNITED KINGDOM