Mathematisches Forschungsinstitut Oberwolfach

Report No. 51/2013

DOI: 10.4171/OWR/2013/51

Analytic Number Theory

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

20 October – 26 October 2013

Abstract. Analytic number theory has florished 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, 14xx.

Introduction by the Organisers

Analytic number theory is on the roll for quite some time now, with spectacular discoveries year after year. To mention just two examples, our understanding of differences between consecutive primes is now radically different from what we knew a decade ago, thanks to a cascade of important contributions initiated by Goldston-Yıldırım-Pintz. The subject was taken to yet another level by Zhang, only very recently. The work of Wooley, still ongoing, on Vinogradov's mean value theorem also changed the landscape in the areas where it is applied. Thus, 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 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 Wednesday 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 truely 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.

Workshop: Analytic Number Theory

Table of Contents

Abstracts

An attempt to prove an effective Siegel theorem

Jozsef Beck

We outlined a plan how to prove an effective Siegel theorem about the exceptional Dirichlet character. It is presented in full detail in the following two references:

1. J. Beck. An attempt to prove an effective Siegel theorem–Part One, 71 pages, arXiv:1311.1478 [math.NA] (http://arxiv.org/abs/1311.1478),

which gives a nutshell summary in Section 0 (5 pages), and gives a very detailed explanation in Sections 1-5, and

2. Part Two of the paper, which is basically long elementary estimations (280 pages). I am happy to send the pdf-file of Part Two to anybody who requests it by email.

Open questions: (1) Is the (ridiculously long) full version correct? (2) Even if the full version has mistakes, is the basic idea (i.e. Part One) still good?

Integral points on modular curves

Yu Bilu
(joint work with A. Bajolet, Sha Min)

Let X_G be the modular curve of level N corresponding to a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with $\det G = (\mathbb{Z}/N\mathbb{Z})^\times$. Then X_G has a standard geometrically irreducible model over $\mathbb{Q}$. We are interested in the following problem:

Problem 1. *Describe the set of rational points $X_G(\mathbb{Q})$.*

This statement is somewhat vague: what does "describe" mean?

First of all, we restrict to the three cases that we deem most interesting for applications, and which accumulate all the principal difficulties presented by the problem. These are the cases when $N = p$ is a prime number and G is one of the following maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_p)$:

- a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$;
- the normalizer of a split Cartan subgroup;
- the normalizer of a non-split Cartan subgroup.

The corresponding modular curves are denoted $X_0(p)$, $X^+_{\mathrm{sp}}(p)$ and $X^+_{\mathrm{ns}}(p)$, respectively.

Next, recall that if $E/\mathbb{Q}$ is an elliptic curve with complex multiplication and $\mathcal{O} = \mathrm{End}(E)$ then E gives rise to a rational point on one of the curves $X_0(p)$, $X^+_{\mathrm{sp}}(p)$ or $X^+_{\mathrm{ns}}(p)$, depending on whether the prime p is ramified, split or inert in the order $\mathcal{O}$. Rational points obtained this way are called *CM-points*.

We can now state a more precise problem:

Problem 2 (Serre's uniformity problem)**.** *Show that for $p > 37$ there is no rational points on the curves $X_0(p)$, $X_{\mathrm{sp}}^+(p)$ and $X_{\mathrm{ns}}^+(p)$ other than the cusps and the CM-points.*

For $X_0(p)$ the problem was solved in the classical work of Mazur [9]. Recently it was solved [5, 7] for the curves $X_{\mathrm{sp}}^+(p)$ as well.

Theorem 1 (B., Parent, Rebolledo)**.** *For $p \geq 17$ and $p = 11$, the set $X_{\mathrm{sp}}^+(p)(\mathbb{Q})$ consists of the cusps and the CM-points.*

The methods of [9, 5, 7] fail completely for $X_{\mathrm{ns}}^+(p)$. However, some results can be obtained for *integral* points, that is, rational points P with $j(P) \in \mathbb{Z}$, where j is the j-invariant. More generally, let X_G be a modular curve defined over a number field K. For a finite set of places $S \subset M_K$ we define the set of S-integral points $X_G(\mathcal{O}_S)$ as the set of K-rational points P such that $j(P) \in \mathcal{O}_S$. (Here, as usual, $\mathcal{O}_S$ denotes the ring of S-integers.)

In [3, 4] I made the following observation: if X_G is a modular curve of level N with at least 3 cusps, then heights of S-integral points on X_G can be effectively bounded in terms of K, S and N. Bajolet and Sha [2] made this explicit for the curve $X_{\mathrm{ns}}^+(p)$ and $\mathcal{O}_S = \mathbb{Z}$

Theorem 2 (Bajolet, Sha)**.** *Let $p \geq 7$ be a prime number and $d \geq 3$ a divisor of $(p-1)/2$. Then or $P \in X_{\mathrm{ns}}^+(p)(\mathbb{Z})$ we have*

$$\log|j(P)| \leq 10^{10}p^{7d}. \tag{1}$$

Sha [11] extended this to an arbitrary X_G, K and S, making my observation mentioned above totally explicit.

Bound (1) is too huge to allow one to determine all integral points on $X_{\mathrm{ns}}^+(p)$. Until recently, this was done only for $p = 7$ by Kenku [8] and by $p = 11$ by Schoof and Tzanakis [10]. The methods of these references do not extend to $p \geq 13$.

With Bajolet we developed [1] a general method for computing integral points on $X_{\mathrm{ns}}(p)$. Using our method, we proved that for $11 \leq p \leq 67$ the set $X_{\mathrm{ns}}(p)(\mathbb{Z})$ consists only of CM-points.

References

[1] A. Bajolet, Yu. Bilu, Computing integral points on $X_{\mathrm{ns}}^+(p)$, preprint (2012); `arXiv:1212.0665`.

[2] A. Bajolet, M. Sha, Bounding the j-invariant of integral points on $X_{\mathrm{ns}}^+(p)$, Proc. Amer. Math. Soc., to appear; `arXiv:1203.1187`.

[3] Yu. Bilu, Effective analysis of integral points on algebraic curves, *Israel J. Math.* **90** (1995), 235–252.

[4] Yu. Bilu, Baker's method and modular curves, in *A Panorama of Number Theory or The View from Baker's Garden* (edited by G. Wüstholz), pages 73–88; Cambridge University Press, 2002.

[5] Yu. Bilu, P. Parent, Serre's uniformity problem in the split Cartan case, *Ann. Math. (2)*, **173** (2011), 569–584; `arXiv:0807.4954`.

[6] Yu. Bilu, P. Parent, Runge's method and modular curves, *Int. Math. Research Notices* **2011** (2011) 1997–2027; `arXiv:0907.3306`.

[7] Yu. Bilu, P. Parent, M. Rebolledo,Rational points on $X_0^+(p^r)$, *Ann. Inst. Fourier*, to appear. arXiv:0907.3306.

[8] M. A. Kenku, A note on the integral points of a modular curve of level 7, *Mathematatika* 32 (1985), 45–48.

[9] B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.* **44** (1978), 129–162.

[10] R. Schoof, N. Tzanakis, Integral points of a modular curve of level 11, *Acta Arith.* **152** (2012), 39–49.

[11] M. Sha, Bounding the j-invariant of integral points on modular curves, *Intern. Math. Research Notices*, doi: 10.1093/imrn/rnt085; arXiv:1208.1337.

Moments of twisted L-functions

Valentin Blomer
(joint work with D. Milićević)

A landmark result in the theory of the Riemann zeta-function is the asymptotic formula for the fourth moment [Za, Mot]

$$\int_0^T |\zeta(1/2+it)|^4 dt = TP_4(\log T) + O(T^{2/3+\varepsilon}) \tag{1}$$

for a certain polynomial P_4; this is one of the prime applications of the Kuznetsov formula. Good [Go] proved the cuspidal version

$$\int_0^T |L(1/2+it,f)|^2 dt = TP_1(\log T) + O(T^{2/3+\varepsilon}) \tag{2}$$

for a certain polynomial P_1 depending on the holomorphic cusp form f.

A non-archimedean analogue of (1) and (2) would replace the archimedean twist by $|\det|^{it}$ with a twist by a Dirichlet character χ:

$$\text{(A)} \quad \sideset{}{^*}\sum_{\chi\,(q)} |L(1/2,\chi)|^4 \qquad \text{and} \qquad \text{(B)} \quad \sideset{}{^*}\sum_{\chi\,(q)} |L(1/2,f\otimes\chi)|^2$$

where the sum runs over all primitive Dirichlet characters χ modulo q and f is a fixed Hecke cusp form in the second sum. We are interested in asymptotic formulas for these moments *with a power saving error term.* It turns out that these problems are much harder compared to (1) and (2), because fixing the special point $1/2$ (as opposed to an average over t of length 1, say) captures some genuine arithmetic information. It was a major breakthrough when M. Young [Y] recently solved (A) for prime moduli q. The (harder) case (B) has remained unsolved for any infinite sequence of moduli q.

In joint work with D. Milićević [BM] we solve (B) for 99.9% of all moduli, excluding only little more than primes and products of two equal or almost equal primes.

Theorem 1. *Let $0 < \eta < 1/5$, and let q run through positive integers such that*

- *there is no prime $p \geq q^{1-\eta}$ dividing q;*

- *there are no two (possibly equal) primes $p_1, p_2 \geq q^{(1-\eta)/2}$ such that $p_1 p_2 \mid q$.*

Let f be a fixed holomorphic cusp form of (even) weight κ for the group $\mathrm{SL}_2(\mathbb{Z})$ with Hecke eigenvalues $\lambda(n)$. Let

$$P(s) = \prod_{p \mid q} \left(1 - \frac{\lambda(p^2)}{p^s} + \frac{\lambda(p^2)}{p^{2s}} - \frac{1}{p^{3s}}\right) \left(1 - \frac{1}{p^{2s}}\right)^{-1}.$$

Then, as $q \to \infty$ as specified above, we have

$$\sum_{\chi\,(q)}{}^{*} |L(1/2, f \otimes \chi)|^2 = 2\psi(q) \frac{P(1)L(1, \mathrm{sym}^2 f)}{\zeta(2)} \left(\log q + c + \frac{P'(1)}{P(1)}\right) + O_{f,\eta}(q^{1-\delta})$$

for some explicit $\delta = \delta(\eta) > 0$, where the sum is over primitive characters modulo q, $\psi(q)$ is the number of such characters, and

$$c = \gamma - \frac{1}{2}\log(2\pi) + \frac{\Gamma'(\kappa/2)}{\Gamma(\kappa/2)} + \frac{L'(1, \mathrm{sym}^2 f)}{L(1, \mathrm{sym}^2 f)} - \frac{2\zeta'(2)}{\zeta(2)}$$

is a constant depending only on f.

The proof is based on a variety of methods. On the one hand we employ the full power of spectral theory of GL_2-automorphic forms to prove cancellation in a possibly unbalanced (average of a) shifted convolution problem:

$$\sum_{r \asymp N/q} \sum_{\substack{n \asymp N, m \asymp M \\ n-m=rq}} \lambda(m)\lambda(n)$$

where $NM \approx q^2$ and $N \geq M$; in particular N and M may be of very different size.

On the other hand, in the crucial rage $N = q^{3/2+o(1)}$, $M = q^{1/2+o(1)}$ we need power saving cancellation in sums of the type

$$\sum_{m \asymp q^{1/2}} S(m, n_1, q) S(m, n_2, q) \tag{3}$$

for given integers n_1, n_2 (such that $n_1 - n_2$ is sufficiently coprime to q). Here the short range of the m-summation prevents the use of standard Fourier analytic techniques. It is only at this point where the special shape of q enters. We show how a general form of Weyl differencing followed by detecting square-root cancellation in multiple exponential sums (based on independence of Kloosterman sheafs and p-adic analytic techniques) eventually yields a power saving in (3) for the relevant moduli in Theorem 1.

References

[BM] V. Blomer, D. Milićević, *The second moment of twisted modular L-functions*, preprint

[Go] A. Good, *The mean square of Dirichlet series associated with cusp forms*, Mathematika **29** (1982), 278-295

[Mot] Y. Motohashi, *Spectral theory of the Riemann zeta-function*, Cambridge tracts in mathematics **127**, Cambridge 1997

[Y] M. Young, *The fourth moment of Dirichlet L-functions*, Ann. of Math. (2) **173** (2011), 1-50.

[Za] N. I. Zavorotnyi, *On the fourth moment of the Riemann zeta-function*, in: Automorphic Functions and Number Theory 2, Computation Center of the Far East Branch of the Science Academy of USSR 1989, 69-125 (in Russian)

Linear growth for certain elliptic fibrations

Pierre Le Boudec

This report is primarily concerned with quantitative aspects of rational points on del Pezzo surfaces of degree 1 defined over $\mathbb{Q}$. In their anticanonical embedding, these surfaces are defined by sextic forms in $\mathbb{P}(3,2,1,1)$. More precisely, they are isomorphic to a surface V given by an equation of the shape

$$y^2 = x^3 + F_4(u,v)x + F_6(u,v),$$

where the coordinates in $\mathbb{P}(3,2,1,1)$ are denoted by $(y:x:u:v)$ to highlight the elliptic fibration and where $F_4, F_6 \in \mathbb{Z}[u,v]$ are respectively a quartic and a sextic form such that $4F_4^3 + 27F_6^2$ is not identically 0.

For $\mathbf{x} = (y:x:u:v) \in \mathbb{P}(3,2,1,1)(\mathbb{Q})$, we can choose coordinates $y,x,u,v \in \mathbb{Z}$ such that for every prime p, either $p \nmid u$ or $p \nmid v$ or $p^2 \nmid x$ or $p^3 \nmid y$. Then we can define an exponential height function $H : \mathbb{P}(3,2,1,1)(\mathbb{Q}) \to \mathbb{R}_{>0}$ by setting

$$H(\mathbf{x}) = \max\{|y|^{1/3}, |x|^{1/2}, |u|, |v|\}.$$

For any Zariski open subset U of V, we can introduce the number of rational points of bounded height on U, that is

$$N_{U,H}(B) = \#\{\mathbf{x} \in U(\mathbb{Q}), H(\mathbf{x}) \leq B\}.$$

A weak version of a conjecture due to Manin and his collaborators (see [3]) states that there should exist an open subset U of V such that, for any fixed $\varepsilon > 0$,

$$N_{U,H}(B) \ll B^{1+\varepsilon}. \tag{1}$$

This conjecture was previously not known for any single example of surface. The best result in this direction was the work of Munshi [4] in which he exhibited surfaces satisfying an upper bound similar to (1) but with the weaker exponent $5/4+\varepsilon$.

In the recent work [2], the author has studied the case of the following family of surfaces. Let $e_1, e_2, e_3 \in \mathbb{Z}$ be three distinct integers and set $\mathbf{e} = (e_1, e_2, e_3)$. Let also $Q \in \mathbb{Z}[u,v]$ be a non-degenerate quadratic form and let $V_{\mathbf{e},Q} \subset \mathbb{P}(3,2,1,1)$ be the surface defined by the equation

$$y^2 = (x - e_1Q(u,v))(x - e_2Q(u,v))(x - e_3Q(u,v)).$$

Finally, let $U_{\mathbf{e},Q}$ be the open subset defined by removing from $V_{\mathbf{e},Q}$ the two subsets given by $y = 0$ and $Q(u,v) = 0$.

We have the following theorem.

Theorem 1. *Let $\varepsilon > 0$ be fixed. We have the upper bound*

$$N_{U_{\mathbf{e},Q},H}(B) \ll B^{1+\varepsilon}.$$

It is worth noting that the constant involved in the notation $\ll$ may depend on ε, $\mathbf{e}$ and Q.

To establish this result, we start by making use of the natural elliptic fibration and we use the fact that the fibers have full rational 2-torsion to achieve complete 2-descents on the fibers.

At this step, it turns out that in order to prove Theorem 1, it is sufficient to prove that the smooth bihomogeneous threefold $V_3 \subset \mathbb{P}^2 \times \mathbb{P}^2$ defined over $\mathbb{Q}$ by the equation

$$x_0 y_0^2 + x_1 y_1^2 + x_2 y_2^2 = 0,$$

has linear growth, by which we mean that the number of rational points of bounded anticanonical height on this threefold grows linearly. This is a very interesting problem in itself.

The author has investigated this problem in [1] and has been able to prove a much sharper result. Indeed, he has established upper and lower bounds of the exact order of magnitude for the number of rational points of bounded anticanonical height on V_3. The proof of this result makes use of both geometry of numbers and analytic number theory tools.

References

[1] P. le Boudec, Density of rational points on a certain smooth bihomogeneous threefold. arxiv 1308:0033.

[2] P. Le Boudec. Integral points on quadratic twists and linear growth for certain elliptic fibrations. arxiv 1308:0060.

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

[4] R. Munshi, Density of rational points on elliptic fibrations. II. Acta Arith. 134 (2008), no. 2, 133–140.

A multidimensional Birch's Theorem

Julia Brandes

Among the problems of the most lasting importance in number theory is Waring's problem, which concerns the question of integral solutions to the equation

$$x_1^k + \cdots + x_s^k = n.$$

While this has been studied extensively by itself (see e.g. [12] for the history), some modifications have also been considered, among which perhaps the most straightforward one replaces the sum of powers by a general homogeneous polynomial F of degree d. In this case, a classical theorem of Birch [2] establishes an asymptotic formula subject to local solubility, provided the number s of variables suffices

$$s - \dim \operatorname{Sing}(F) > 2^d(d-1).$$

Another, less well-known generalisation of Waring's problem, which goes back to Arkhipov and Karatsuba [1] and has later been studied in great depth by Parsell and others (see e.g. [8, 9, 10]), arises if the variables x_i are replaced by linear forms $L_i \in \mathbb{Z}[t_1, \dots, t_m]$ and the integer n by a homogeneous polynomial $\psi \in \mathbb{Z}[t_1, \dots, t_m]$ of degree k. Notice that for $m = 1$ this reduces to the traditional version of Waring's problem.

Our goal is now to combine these two questions and derive a multidimensional version of Birch's theorem describing the number of solutions to equations of the shape

$$F(\mathbf{x}_1 t_1 + \cdots + \mathbf{x}_m t_m) = \psi(t_1, \dots, t_m). \tag{1}$$

This generalised problem has so far been studied only in the quadratic case, where matrix algebra and dynamical systems provide a different set of methods, and the only attempt to tackle this question by the circle method is a very recent paper by Dietmann and Harvey [7]. We show how, by expanding the left hand side of (1) and equating coefficients of $t_1, \dots, t_m$, every linear form solving the equation translates bijectively to a point solution $\mathbf{x}_1, \dots, \mathbf{x}_m \in [-P, P]^{ms}$ of a system of r equations, where $r \sim m^d$ is the number of monomials in ψ. This allows us to apply the methods for systems of forms developed by Birch [2] and Schmidt [11], and we obtain a Hasse Principle with the expected number of solutions, provided

$$s - \dim \operatorname{Sing}(F) > 3 \cdot 2^{d-1}(d-1)(r+1).$$

This is essentially Theorem 1.1 in [3]. The number of variables required here is smaller by a factor $r \sim m^d$ than comparable results implicit in work by Dietmann [5, 6] and Dietmann and Harvey [7]. This is achieved by exploiting certain symmetries of the system associated to (1).

In the special case when F is definite, the number of representations is finite and one has natural size restrictions for the variables. These will, however, not typically be all of the same size, so it is desirable to have a more general version of the multidimensional Birch theorem that allows for more flexibility in the constraints of the variables. Such a result may also be of interest for some applications in algebraic geometry. It turns out that, provided the constraints are not too distinct, the same methods continue to be applicable (see Chapter 3 in [4] for details), and again one obtains a Hasse Principle with asymptotic formula under the condition

$$s - \dim \operatorname{Sing}(F) > 2^{d-1} \max \left\{ 3(d-1)(r+1), rd \left(\frac{\log P_{\max}}{\log P_{\min}} \right) \right\}.$$

A similar result for the case $d = 2$ is implicit in Dietmann and Harvey's work on representing quadratic forms by quadratic forms [7], and again we save a factor r over their result.

References

[1] G. I. Arkhipov and A. A. Karatsuba, *A multidimensional analogue of Waring's problem.* Soviet Math. Dokl. **36** (1988), 75–77.

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

[3] J. Brandes, *Forms representing forms and linear spaces on hypersurfaces*, Proc. London Math. Soc. (in press). arXiv:1202.5026.

[4] J. Brandes, *Local-global principles for linear spaces on hypersurfaces*, PhD Thesis submitted to the University of Bristol, 2013.

[5] R. Dietmann, *Systems of cubic forms*, J. London Math. Soc. (2) **77** (2008), no. 3, 666–686.

[6] R. Dietmann, *Linear spaces on rational hypersurfaces of odd degree*, Bull. London Math. Soc. **42** (2010), 891–895.

[7] R. Dietmann and M. Harvey, *On the representation of quadratic forms by quadratic forms*, submitted, arXiv:1301.6772.

[8] S. T. Parsell, *A generalization of Vinogradov's mean value theorem*, Proc. London Math. Soc. (3) **91** (2005), no. 1, 1–32.

[9] S. T. Parsell, *Hua-type iteration for multidimensional Weyl sums*, Mathematika 58 (2012), 209–224.

[10] S. T. Parsell, S. M. Prendiville and T. D. Wooley, *Near-optimal mean value estimates for multidimensional Weyl sums*, Geom. Funct. Anal. (in press). arXiv: 1205.6331.

[11] W. M. Schmidt, *The density of integer points on homogeneous varieties*, Acta Math. **154** (1985), no.4, 234–296.

[12] R. C. Vaughan and T. D. Wooley, *Waring's problem: a survey*, Number theory for the millennium, III (Urbana, IL, 2000), 301–340, A K Peters, Natick, MA, 2002.

Power-free polynomials on affine quadrics

Tim Browning
(joint work with Alex Gorodnik, University of Bristol)

Given a polynomial with integer coefficients, the problem of determining whether or not it takes infinitely many square-free values has long been a central concern in analytic number theory. More generally one can ask for r-free values, for any $r \geq 2$, where an integer is said to be *r-free* if it is not divisible by p^r for any prime p. In this paper we initiate an investigation of r-free values for polynomials whose arguments run over thin sets.

Let $Y \subset \mathbb{A}^n$ be an affine variety defined by a system of polynomial equations with integer coefficients and let $f \in \mathbb{Z}[X_1, \dots, X_n]$ be a polynomial. Nevo and Sarnak [5] define the *saturation number* $r(Y, f)$ to be the least positive integer r such that the set of $\mathbf{x} \in V(\mathbb{Z})$, for which $f(\mathbf{x})$ has at most r prime factors, is Zariski-dense in Y. They show that $r(Y, f)$ is finite whenever Y is a principal homogeneous space and f is "weakly primitive". In a similar spirit we can define a number $r^{\square}(Y, f)$ to be the least integer $r \geq 2$ such that the set of $\mathbf{x} \in V(\mathbb{Z})$, for which $f(\mathbf{x})$ is r-free, is Zariski-dense in Y. It is then natural to try and determine conditions on Y and f under which one can show that $r^{\square}(Y, f)$ is finite. For example, Erdős [3] showed that $r^{\square}(\mathbb{A}^1, f(x)) \leq d - 1$, provided that f has degree d and contains no "fixed dth power divisors".

Our main result establishes that $r^{\square}(Y,f)$ is finite when $Y\subset\mathbb{A}^n$ is a suitable affine quadric and f is a homogeneous polynomial satisfying certain genericity conditions.

For $n\geq 3$, let $Q\in\mathbb{Z}[X_1,\dots,X_n]$ be a non-singular indefinite quadratic form and let m be a non-zero integer. We assume that $-m\det(Q)$ is not the square of an integer when $n=3$. Let $Y\subset\mathbb{A}^n$ denote the affine quadric

$$Q=m.$$

We cannot expect $r^{\square}(Y,f)$ to exist without some conditions on Y and f. The following result provides some sufficient conditions.

Theorem 1. *Let $n\geq 3$ and assume that $Y(\mathbb{Z})\neq\emptyset$. Assume that f is a non-singular homogeneous polynomial of degree $d\geq 2$ such that the projective variety $f=Q=0$ is also non-singular and such that there is no prime p such that $p^2\mid f(\mathbf{x})$ for every $\mathbf{x}\in Y(\mathbb{Z})$. Then $r^{\square}(Y,f)<\infty$.*

In fact one can take $r^{\square}(Y,f)\leq 2dn$ when $n\geq 4$. When f is linear one can do better, as follows.

Theorem 2. *Let $n\geq 3$ and assume that $Y(\mathbb{Z})\neq\emptyset$. Assume that f is a linear polynomial such that there is no prime p such that $p^2\mid f(\mathbf{x})$ for every $\mathbf{x}\in Y(\mathbb{Z})$. Then $r^{\square}(Y,f)=2$.*

When $n\geq 4$, work of Baker [1] could easily be modified to establish Theorem 2. Baker's approach uses the Hardy–Littlewood circle method, whereas our work requires tools from dynamical systems relating to uniform lattice point counting (see Gorodnik and Nevo [4])

One ingredient in the proof involves counting integral points in a box on affine quadrics. Suppose we are given a non-zero quadratic polynomial $q\in\mathbb{Z}[T_1,\dots,T_\nu]$, with quadratic part q_0, for $\nu\geq 2$. Consider the counting function

$$M(q;B)=\#\{\mathbf{t}\in\mathbb{Z}^\nu : q(\mathbf{t})=0,\ |\mathbf{t}|\leq B\},$$

for any $B\geq 1$. We will require an upper bound for $M(q;B)$ which is uniform in the coefficients of q and which is essentially as sharp and as general as possible. A trivial estimate is $M(q;B)=O_\nu(B^{\nu-1})$, which is as good as can be hoped for when q is reducible over $\mathbb{Q}$. Assuming that q is irreducible over $\mathbb{Q}$, a result of Pila [6] reveals that $M(q;B)=O_{\varepsilon,\nu}(B^{\nu-3/2+\varepsilon})$, for any $\varepsilon>0$. Again this is essentially best possible when $\operatorname{rank}(q_0)=1$, as consideration of the polynomial $T_1-T_2^2$ shows. For the remaining cases we establish the following improvement, which is based on arguments from [2].

Theorem 3. *Assume that q is irreducible over $\mathbb{Q}$ and that* $\operatorname{rank}(q_0)\geq 2$. *Then we have $M(q;B)=O_{\varepsilon,\nu}(B^{\nu-2+\varepsilon})$, for any $\varepsilon>0$.*

The most important feature of Theorem 3 is its uniformity in the coefficients of the quadratic polynomial q. It reflects the rough order of magnitude of $M(q;B)$ when $q=q_0$. The result is proved by induction on ν, the case $\nu=2$ essentially going back to work of Estermann.

References

[1] R.C. Baker, *The values of a quadratic form at square-free points*, Acta Arith. **124** (2006), 101–137.

[2] T.D. Browning, D.R. Heath-Brown and P. Salberger, *Counting rational points on algebraic varieties*, Duke Math. J. **132** (2006), 545–578.

[3] P. Erdős, *Arithmetical properties of polynomials*, J. London Math. Soc. **28** (1953), 416–425.

[4] A. Gorodnik and A. Nevo, *Counting lattice points*, J. Reine Angew. Math. **663** (2012), 127–176.

[5] A. Nevo and P. Sarnak, *Prime and almost prime integral points on principal homogeneous spaces*, Acta Math. **205** (2010), 361–402.

[6] J. Pila, *Density of integral and rational points on varieties*, Astérisque **228** (1995), 183–187.

The average asymptotic behaviour of the Frobenius fields of an elliptic curve

Alina Carmen Cojocaru

(joint work with Henryk Iwaniec, and Nathan Jones)

Let $E/\mathbb{Q}$ be an elliptic curve, of discriminant $\Delta(E)$. For every prime $p \nmid \Delta(E)$, we have $\#\overline{E}(\mathbb{F}_p) = p + 1 - a_p$, where $a_p = a_p(E) \in \mathbb{Z}$ satisfies $|a_p| < 2\sqrt{p}$. Equivalently, a_p has the property that the polynomial $X^2 - a_pX + p = (X - \pi_p)(X - \overline{\pi}_p)$ has two complex conjugate non-real roots $\pi_p = \pi_p(E)$, $\overline{\pi}_p = \overline{\pi}_p(E)$, which satisfy $\pi_p + \overline{\pi}_p = a_p$ and $\pi_p\overline{\pi}_p = p$. Moreover, any of these roots, say π_p, identifies with the pth power Frobenius endomorphism of $\overline{E}$. As such, we shall call $\mathbb{Q}(\pi_p)$ the *Frobenius field of E at p*.

If E is with CM, that is, if $\operatorname{End}_{\overline{\mathbb{Q}}}(E)$ is an order in an imaginary quadratic field $\mathbb{K}$, then $\mathbb{Q}(\pi_p) \simeq \mathbb{K}$ for any prime p of good ordinary reduction for E. To see this, recall that

$$\mathbb{Q} \subseteq \operatorname{End}_{\overline{\mathbb{Q}}}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \subseteq \operatorname{End}_{\overline{\mathbb{F}}_p}(\overline{E}) \otimes_{\mathbb{Z}} \mathbb{Q}$$

and

$$\mathbb{Z}[\pi_p] \subseteq \operatorname{End}_{\mathbb{F}_p}(\overline{E}) \subseteq \mathbb{Q}(\pi_p) \subseteq \operatorname{End}_{\overline{\mathbb{F}}_p}(\overline{E}) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

By definition, p is ordinary if $\operatorname{End}_{\overline{\mathbb{F}}_p}(\overline{E})$ is an imaginary quadratic order. By the CM assumption, $\operatorname{End}_{\overline{\mathbb{Q}}}(E) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{K}$. Hence, as p varies over ordinary primes, *there is only one Frobenius field* $\mathbb{Q}(\pi_p)$. Even more can be said in this setting. By results of M. Deuring, p is ordinary if and only if it ramifies or splits completely in the CM field $\mathbb{K}$. Combined with the Chebotarev density theorem, this implies that, for any arbitrary imaginary quadratic field K, the function

$$\Pi_E(K; x) := \#\left\{p \le x : \ p \text{ of ordinary good reduction}, \mathbb{Q}(\pi_p) \simeq K\right\}$$

equals 0 if $K \not\simeq \mathbb{K}$, and satisfies the asymptotic

$$\Pi_E(K; x) \sim \frac{1}{2} \cdot \frac{x}{\log x} \tag{1}$$

if $K \simeq \mathbb{K}$.

If E is without CM, that is, if $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$, *there are infinitely many non-isomorphic Frobenius fields* $\mathbb{Q}(\pi_p)$ as p varies over primes p of ordinary reduction for E. The proof was given for the first time by A.C. Cojocaru, É. Fouvry and M.R. Murty in 2005, using sieve methods. We also have:

Conjecture (S. Lang and H. Trotter, 1976)
Let K be an imaginary quadratic field. Let $E/\mathbb{Q}$ be an elliptic curve such that $\mathrm{End}_{\overline{\mathbb{Q}}}(E) \simeq \mathbb{Z}$. *Then there exists a constant $c(E,K) > 0$ such that, as $x \to \infty$,*

$$\Pi_E(K;x) \sim c(E,K)\frac{\sqrt{x}}{\log x}. \tag{2}$$

In 1981, Serre wrote that one could show, under the assumption of a Generalized Riemann Hypothesis (GRH for short) and using Selberg's sieve, that $\Pi_E(K;x) \ll x^\theta$ for some unspecified $\theta < 1$. Later on, Serre added the remark that one could show this without the Selberg's sieve, but instead by applying the effective Chebotarev density theorem of J. Lagarias and A. Odlyzko directly to a mixed Galois representation associated to both E and K. Such a proof was given much later by Cojocaru, Fouvry and Murty in 2005, via the square sieve and the effective Chebotarev density theorem; under GRH, they showed that $\Pi_E(K;x) \ll x^{17/18}\log x$, and, unconditionally, that $\Pi_E(K;x) \ll \frac{x(\log\log x)^{13/12}}{(\log x)^{25/24}}$. These results were followed up with detailed explanations by Serre, who outlined the construction of his aforementioned mixed Galois representation and the proof of the bound $\Pi_E(K;x) \ll x^{7/8}$, under GRH. In 2008, Cojocaru and David refined Serre's method and proved, under GRH, that

$$\Pi_E(K;x) \ll \frac{x^{4/5}}{(\log x)^{1/5}}.$$

At the time of this writing, this upper bound is the best and no lower bound is known.

We *prove an average version of the Lang-Trotter Conjecture.* For simplicity, set

$$\psi_{E,K}(x) := \sum_{\substack{p \le x \\ p \nmid \Delta(E) \\ \mathbb{Q}(\pi_p(E)) \simeq K}} \sqrt{p}\log p. \tag{3}$$

and focus on the asymptotic formula

$$\psi_{E,K}(x) \sim 2c(E,K)x, \tag{4}$$

equivalent to (2) by partial summation. Note also that in (3) we may assume that $p \ge 5$ and p is ordinary.

Setting and notation:

• Let $-D < 0$ be a fixed fundamental discriminant. Consider: $K := \mathbb{Q}(\sqrt{-D})$ the imaginary quadratic field of discriminant $-D$; H_K the Hilbert class field of K; $H(-D)$ the Kronecker class number of $-D$; and χ_K the Kronecker symbol of K. Note that a prime p splits completely in H_K if and only if there exist $r = r(p, D) \in \mathbb{Z}$ and $c = c(p, D) \in \mathbb{N}\backslash\{0\}$ such that $4p = r^2 + Dc^2$. For such p, we define

$$c_p := c \sum_{d|c} \frac{1}{d} \prod_{\substack{\ell | d \\ \ell \text{ prime}}} (1 - \chi_K(\ell)). \tag{5}$$

We denote by $\sum\limits_{\substack{p \leq x \\ p \text{ splits compl. in } H_K}}$ the summation over primes $p \leq x$ which split completely in H_K and define

$$\psi_K(x) := \sum_{\substack{p \leq x \\ p \text{ splits compl. in } H_K}} \frac{c_p \log p}{\sqrt{p}}. \tag{6}$$

• Let $A, B \in \mathbb{N}\backslash\{0\}$ and let $\mathcal{E} = \mathcal{E}(A, B)$ be the family of elliptic curves $E_{ab}/\mathbb{Q}$ given by $E_{ab} : y^2 = x^3 + ax + b$, with coefficients $a, b \in \mathbb{Z}$, $1 \leq a \leq A$, $1 \leq b \leq B$.

• To ensure no bias towards intrinsic features of the elements of $\mathcal{E}$, we let $\mathcal{A} = (\alpha_a)_{1 \leq a \leq A}$, $\mathcal{B} = (\beta_b)_{1 \leq b \leq B}$ be arbitrary sequences in $\mathbb{C}$. We associate to each $E_{ab} \in \mathcal{E}$ the weight $\alpha_a \beta_b$. We set

$$|\mathcal{A}| := \sum_{1 \leq a \leq A} \alpha_a, \qquad ||\mathcal{A}|| := \left(\sum_{1 \leq a \leq A} |\alpha_a|^2 \tau(a) \right)^{\frac{1}{2}},$$

$$|\mathcal{B}| := \sum_{1 \leq b \leq B} \beta_b, \qquad ||\mathcal{B}|| := \left(\sum_{1 \leq b \leq B} |\beta_b|^2 \tau(b) \right)^{\frac{1}{2}},$$

where $\tau(\cdot)$ denotes the divisor function.

Main Theorem

(a) $$\sum_{1 \leq a \leq A} \sum_{\substack{1 \leq b \leq B \\ \Delta(E_{ab}) \neq 0}} \alpha_a \beta_b \psi_{E_{ab}}(x) = |\mathcal{A}||\mathcal{B}| \cdot H(-D) \cdot \psi_K(x) + O\left(||\mathcal{A}||\, ||\mathcal{B}|| \left(x^{\frac{7}{4}} + (A+B)^{\frac{1}{2}} x^{\frac{5}{4}} + (AB)^{\frac{1}{2}} x^{\frac{7}{8}} \right) (\log x)^3 \right).$$

(b) $$\psi_K(x) \sim \tfrac{8\zeta(2)}{DL(1,\chi_K)} \cdot \prod_{\substack{\ell \nmid D \\ \ell \text{ prime}}} \left(1 - \frac{\chi_K(\ell)}{\ell^2} - \frac{1 - \chi_K(\ell)}{\ell^2(\ell+1)} \right) \cdot x.$$

(c) *Let*

$$c(K) := \frac{2\pi}{3\sqrt{D}} \prod_{\substack{\ell \nmid D \\ \ell \text{ prime}}} \left(1 - \frac{\chi_K(\ell)}{\ell^2} - \frac{1 - \chi_K(\ell)}{\ell^2(\ell+1)} \right).$$

Then there exist constants $\gamma_1 > 0$ and $\gamma_2 > 0$ such that, for any real number $d \geq 1$, we have

$$\frac{1}{AB} \sum_{1 \leq a \leq A} \sum_{\substack{1 \leq b \leq B \\ \Delta(E_{ab}) \neq 0}} |c(E_{ab}, K) - c(K)|^d$$

$$\ll_{K,d} \quad \log(\max\{A,B\})^{d\gamma_2} \left(\frac{(\log \min\{A,B\})^{\gamma_1}}{\sqrt{\min\{A,B\}|}} + \frac{\log B (\log A)^7}{B} \right).$$

Zeros of Dirichlet L-functions

Brian Conrey

(joint work with H. Iwaniec, K. Soundararajan)

Let $Q > 0$ be a large number and let $\mathcal{B}(Q)$ be the rectangle in the s-plane with vertices $0, 1, 1 + iQ, iQ$. Let $\mathcal{F}(Q)$ denote the family of L-functions $L(s, \chi)$ such that χ is a primitive character modulo q where $Q < q \leq 2Q$. Let $\mathcal{Z}(Q)$ denote the set of all zeros of any $L(s, \chi)$ which are in $\mathcal{B}(Q)$; the zeros are counted with multiplicity.

Theorem 1. *At least 60% of the zeros in $\mathcal{B}(Q)$ have real parts equal to 1/2.*

We remark that for any **fixed** $L(s, \chi)$ it can be proven that at least 40% of its zeros have real part equal to 1/2. But by averaging over χ and q we can improve the average percentage.

The proof uses the asymptotic large sieve which is a technique developed by the three authors which allow in certain situations for the asymptotic evaluation of averages

$$\sum_q W(q/Q) \sum_{\chi \bmod q}^{*} \left| \sum_{n=1}^{N} a_n \chi(n) \right|^2,$$

where $0 \leq W(x) \leq 1$ is supported on $[1, 2]$. The large sieve inequality asserts that the above is $\ll (Q^2 + N) \sum_{n=1}^{N} |a_n|^2$ for arbitrary sequences $\{a_n\}$. Actually, we use a version of the large sieve in which the weights $|L(1/2, \chi)|^2$ appear, that is we estimate

$$\sum_q W(q/Q) \sum_{\chi \bmod q}^{*} |L(1/2, \chi)|^2 \left| \sum_{n=1}^{N} a_n \chi(n) \right|^2.$$

We prove that the above is

$$= \sum_{q \leq Q} \phi^*(q) \sum_{\substack{m,n \leq N \\ (mn,q)=1}} \frac{b_m \overline{b_n}(m,n)}{mn} \left(\log \frac{q(m,n)^2}{8\pi mn} + \gamma + o(1) \right).$$

provided $N \ll Q^{1-\epsilon}$, $b_n \ll n^{\epsilon}$. Here $\phi^*(q)$ is the number of primitive characters modulo q. This is the analogue for Dirichlet characters of a conjecture of Balasubramanian, Conrey, and Heath-Brown.

The 60% improves upon a previously announced slightly weaker result of 58% which was achieved by an easier argument. The flexibility of this method allows us to use new mollifier weights introduced by Shaoji Feng, thus allowing for the extra 2%.

To describe Feng's mollifier, recall that in the Levinson method, the function we are trying to mollify is basically

$$\zeta(s) + \frac{\zeta'(s)}{\log T} = \zeta + \frac{\zeta'}{L} = \zeta\left(1 + \frac{1}{L}\frac{\zeta'}{\zeta}\right).$$

Motivated by

$$\frac{1}{\zeta + \frac{\zeta'}{\log T}} = \frac{1}{\zeta}\left(1 - \frac{1}{L}\frac{\zeta'}{\zeta} + \frac{1}{L^2}\left(\frac{\zeta'}{\zeta}\right)^2 - \frac{1}{L^3}\left(\frac{\zeta'}{\zeta}\right)^3 + \dots\right)$$

which has Dirichlet series coefficients

$$\mu + \frac{\mu * \Lambda}{L} + \frac{\mu * \Lambda * \Lambda}{L^2} + \frac{\mu * \Lambda * \Lambda * \Lambda}{L^3} + \dots$$

Feng introduced a mollifier of the form

$$\sum_{h \le y} \frac{b_h}{b^s}$$

where

$$\begin{aligned} b_h &= \mu(h) P_1\left(\frac{\log y/h}{\log y}\right) + \lambda_2(h) P_2\left(\frac{\log y/h}{\log y}\right) L^{-2} \\ &\quad + \lambda_3(h) P_3\left(\frac{\log y/h}{\log y}\right) L^{-3} + \dots \\ &\quad + \lambda_{\mathcal{I}}(h) P_{\mathcal{I}}\left(\frac{\log y/h}{\log y}\right) L^{-R} \end{aligned}$$

where

$$\lambda_R(d) = (\mu * \Lambda^{*R})(d).$$

The choices $\mathcal{I} = 3$, $y = Q^{1-\epsilon}$,

$$\begin{aligned} P_1(x) &= x + 0.1560x(1-x) - 1.4045x(1-x)^2 - 0.0662x(1-x)^3 \\ P_2(x) &= 2.0409x + 0.2661x^2 \\ P_3(x) &= -0.0734x \end{aligned}$$

are what are used in the proof that a proportion of at least 0.6085 of zeros of Dirichlet L-functions are on the critical line.

Quantitative versions of Hilbert's Irreducibility Theorem, and Probabilistic Galois Theory

Rainer Dietmann

One of the classical results in Diophantine geometry is *Hilbert's Irreducibility Theorem (HIT):* ([6], [7] §9): If $f(X_1, \ldots, X_r, t_1, \ldots, t_n) \in \mathbb{Q}[\mathbf{X}, \mathbf{T}]$ is irreducible, then there are infinitely many specialisations for $\mathbf{t} \in \mathbb{Q}^n$ such that the specialised polynomial $f(X_1, \ldots, X_r)$ still is irreducible over $\mathbb{Q}$. For $r = 1$, which will be our main focus, more can be said, as we can consider $f(X, \mathbf{t})$ as a separable polynomial in X over the function field $\mathbb{Q}(\mathbf{T})$: let G be the Galois group of the splitting field of f in $\overline{\mathbb{Q}(\mathbf{T})}$. Then a more general form of HIT states that there are infinitely many specialisations $\mathbf{t} \in \mathbb{Q}^n$ such that the specialised rational polynomial $f(X)$ still has Galois group G over $\mathbb{Q}$, which for $r = 1$ generalises the formulation of HIT from above.

A well known example for this forms the setting of *Probabilistic Galois Theory* ([9], [5]): the polynomial

$$X^n + t_1 X^{n-1} + \ldots + t_n$$

has Galois group S_n over $\mathbb{Q}(\mathbf{T})$, whence by applying HIT and specialising $t_1, \ldots, t_n$ we conclude that there are infinitely many rational monic degree n polynomials having Galois group S_n over $\mathbb{Q}$.

In our work we are interested in quantifying such statements. To this end we first observe that if one specialises $\mathbf{t} \in \mathbb{Q}^n$, and $f(X)$ is still separable, then its Galois group will be a subgroup K of its original subgroup G over $\mathbb{Q}(\mathbf{T})$. Let us now without loss of generality assume that f has integer coefficients, and let

$$N_f(H; K) = \#\{\mathbf{t} \in \mathbb{Z}^n : |\mathbf{t}| \leq H \text{ and } \mathrm{Gal}(f/\mathbb{Q}) \subset K\}.$$

Our goal is a good upper bound for $N_f(H; K)$. Cohen [2], using the large sieve, proved that if K is a proper subgroup of G, then

$$N_f(H; K) \ll_{f,\varepsilon} H^{n-1/2+\varepsilon}. \tag{1}$$

This shows that for $r = 1$ in HIT one can replace 'infinitely many' by 'almost all'. Zywina [10], using the larger sieve, could should that if K is a normal subgroup of G (or more generally, a subset of G stable under conjugation), then

$$N_f(H; K) \ll_{f,\varepsilon} H^{n-1+|K|/|G|+\varepsilon}, \tag{2}$$

which is a bound sensitive to the size of $|K|$. Generalising our previous work [3] on the special case $f = X^n + t_1 X^{n-1} + \ldots + t_n$, we can show that (2) holds true for all subgroups K of G, not just normal ones. This does not improve on Cohen's result (1) for subgroups of index 2, but in the important special case $f = X^n + t_1 X^{n-1} + \ldots + t_n$ and $K = A_n$, we can show (see [4]) that

$$N_{X^n + t_1 X^{n-1} + \ldots + t_n}(H; A_n) \ll_{n,\varepsilon} H^{n-2+\sqrt{2}+\varepsilon}. \tag{3}$$

Using (2) and (3) we obtain that all of the monic integer polynomials $X^n + t_1 X^{n-1} + \ldots + t_n$ with coefficients t_i of absolute value at most H have Galois group S_n, with at most

$$O_{n,\varepsilon}(H^{n-2+\sqrt{2}+\varepsilon})$$

exceptions. This improves the previous 1973 world record $O_n(H^{n-1/2}\log H)$ by Gallagher [5].
Our new approach, rather than using reductions modulo primes and applying sieve methods, reduces the problem on getting an upper bound for $N_f(H;K)$ to the problem of bounding the number of integer points on certain auxiliary varieties, so called *Galois resolvents.* To this end recent results about bounding the number of integer points on curves and surfaces ([1], [8]) can be brought into play.

References

[1] Browning, T.D. & Heath-Brown, D.R. Plane curves in boxes and equal sums of two powers, *Math. Z.* **251** (2005), 233–247.

[2] Cohen, S.D. The distribution of Galois groups and Hilbert's irreducibility theorem, *Proc. London Math. Soc.* **43** (1981), 227–250.

[3] Dietmann, R. On the distribution of Galois groups, *Mathematika* **58** (2012), 35–44.

[4] Dietmann, R. Probabilistic Galois theory, *Bull. Lond. Math. Soc.* **45** (2013), no. 3, 453–462.

[5] Gallagher, P.X. The large sieve and probabilistic Galois theory, *Proceedings of Symposia in Pure Mathematics* XXIII (1973, A.M.S.), 91–101.

[6] Hilbert, D. Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten, *J. Reine Angew. Math.* **110** (1892), 104–129.

[7] Lang, S. Fundamentals of Diophantine Geometry, Springer Verlag, 1983.

[8] Salberger, P. Counting rational points on projective varieties, submitted (2010).

[9] van der Waerden, B.L. Die Seltenheit der reduziblen Gleichungen und die Gleichungen mit Affekt, *Monatsh. Math.* **43** (1936), 137–147.

[10] Zywina, D. Hilbert's irreducibility theorem and the larger sieve, *arXiv:1011.6465.*

A probabilistic study of the Explicit Formula

Daniel Fiorilli

Riemann's Explicit Formula gives an exact expression for $\psi(x)$, the weighted prime-counting function, in terms of the zeros of $\zeta(s)$. Under the Riemann Hypothesis, the remainder term $x^{-\frac{1}{2}}(\psi(x)-x)$ is a Besicovitch B^2 almost-periodic function, and thus has a limiting distribution [W]. The study of this error term and its generalizations involves a nice blend of probability and of analytic and algebraic number theory, and applies to many number theoretical questions.

Rubinstein and Sarnak [RS] studied the set of x for which $\pi(x;q,a)>\pi(x;q,b)$, where a and b are coprime to q. They determined under GRH and LI[1] that the logarithmic proportion of x for which $\mathrm{Li}(x)>\pi(x)$ is approximately 0.99999973, a very surprising number. Among many other things, they investigated the inequality $\pi(x;q,a)>\pi(x;q,b)$ for large values of q, in order to find extreme behavior similar to that of the race between $\pi(x)$ and $\mathrm{Li}(x)$. Their conclusion was that $\delta(q;a,b)$ tends to $\frac{1}{2}$ as q tends to infinity, and it turns out that 0.99999973... is

[1] This states that the multiset of nonnegative imaginary parts of the nontrivial zeros of all primitive Dirichlet L-functions is linearly independent over $\mathbb{Q}$.

the highest possible density in this problem. This is related to the fact that $\zeta(s)$ is extreme in the family of Dirichlet L-functions, in that its first zero is the highest. In recent work [F2], the author uncovered the existence of arbitrarily biased prime number races. More precisely, for any $\epsilon > 0$, there exists a modulus q and subsets A and B of the invertible residues modulo q such that the logarithmic density of the set of x for which $\frac{1}{|A|}\sum_{a\in A}\pi(x;q,a) > \frac{1}{|B|}\sum_{b\in B}\pi(x;q,b)$ exceeds $1-\epsilon$. This result is conditional on GRH and an assumption on the multiplicity of the zeros of $L(s,\chi)$, but does not depend on the LI assumption.

The author also used similar tools to tackle a phenomenon raised by Mazur [M] and studied by Sarnak [S], on the summatory function of $a_p(E)$, the trace of the Frobenius of a fixed elliptic curve E. It turns out that a similar bias as that observed by Chebyshev appears in this function. Interestingly, this bias depends directly on the analytic rank of E. Building on the work of Sarnak, the author raised the question of whether it was possible to find highly biased prime number races in this context. The author [F1] was able to prove a conditional equivalence between this statement and the well-believed conjecture that the analytic rank of elliptic curves is unbounded, in a precise quantitative way. Interestingly, the two existing conjectures on the growth of the analytic rank both imply the existence of highly biased elliptic curve prime number races.

The variance of primes in arithmetic progressions. This concerns $V(x;q)$, the variance of primes in the residue classes modulo q:

$$V(x;q) := \sum_{\substack{a \bmod q\\(a,q)=1}} \left|\psi(x;q,a) - \frac{\psi(x;\chi_0)}{\phi(q)}\right|^2.$$

One of the major applications of the large sieve is the Barban-Davenport-Halberstam Theorem which gives an upper bound on the average of $V(x;q)$ over $q \le Q$, in the range $Q > x/(\log x)^A$. Hooley conjectured that $V(x;q) \sim x\log q$ in an unspecified range of q, and the goal of this project is to make a conjecture for the exact range in which this asymptotic should hold. Friedlander and Goldston [FG] conjectured that the range $x^{\frac{1}{2}+\epsilon} < q \le x$ is admissible and might be best possible, however Keating and Rudnick [KR] studied a function field analogue which suggests that this range can be extended to $x^\epsilon < q \le x$. Using the theory of large deviations and conditional estimates on the higher moments of the distribution of $V(x;q)/x$, we prove a probabilistic result which suggests that Hooley's Conjecture holds in the extended range $(\log\log x)^{1+\epsilon} < q \le x$, and that the exponent $1+\epsilon$ is best possible.

The nonvanishing of L-functions at the central point. This work in progress studies the implications of variants of Montgomery's Conjecture on the vanishing of L-functions at the central point. In the context of Dirichlet L-functions, we show that among the characters $\chi \bmod q$ with $q \le Q$, the proportion of those characters for which $L(\frac{1}{2},\chi) = 0$ is $O(Q^{-\frac{1}{2}+\epsilon})$. This in conditional on GRH and on a refined Montgomery Conjecture, which does not involve real zeros of $L(s,\chi)$. In the context of elliptic curves, we show that an adaptation of Montgomery's Conjecture implies that the average rank of certain families of elliptic curve L-functions is exactly $\frac{1}{2}$, in a precise quantitative manner.

References

[F1] Daniel Fiorilli, *Elliptic curves of unbounded rank and Chebyshev's Bias.* To appear, IMRN.

[F2] Daniel Fiorilli, *Highly biased prime number races.* arXiv:1210.6946 [math.NT]

[FG] J. B. Friedlander, D. A. Goldston, *Variance of distribution of primes in residue classes.* Quart. J. Math. Oxford Ser. (2) **47** (1996), no. 187, 313–336.

[KR] J. P. Keating and Z. Rudnick, *The Variance of the Number of Prime Polynomials in Short Intervals and in Residue Classes.* To appear, IMRN.

[M] Barry Mazur, *Finding meaning in error terms.* Bull. Amer. Math. Soc. **45** (2008), no. 2, 185-228.

[RS] M. Rubinstein and P. Sarnak, *Chebyshev's bias.* Experiment. Math. **3** (1994), no. 3, 173–197.

[S] Peter Sarnak, *Letter to Barry Mazur on "Chebyshev's bias" for $\tau(p)$.* http://web.math.princeton.edu/sarnak/MazurLtrMay08.PDF.

[W] Aurel Wintner, *On the distribution function of the remainder term of the prime number theorem.* Amer. J. Math. **63**, (1941). 233–248.

Strongly diagonal behavior in Vinogradov's mean value theorem

Kevin Ford
(joint work with Trevor Wooley)

When k and s are natural numbers, denote by $J_{s,k}(X)$ the number of integral solutions of the system of Diophantine equations

$$\sum_{i=1}^{s}(x_i^j - y_i^j) = 0 \quad (1 \le j \le k), \tag{1}$$

with $1 \le x_i, y_i \le X$ $(1 \le i \le s)$. Equivalently, $J_{s,k}(X)$ may be expressed analytically as

$$J_{s,k}(X) = \int_{[0,1)^k} \Big| \sum_{n \le X} e^{2\pi i(\alpha_1 n + \alpha_2 n^2 + \cdots + \alpha_k n^k)} \Big|^{2s} \, d\alpha_1 \cdots d\alpha_k. \tag{2}$$

In this latter form it is know as *Vinogradov's mean value* or *Vinogradov's integral*, after I. M. Vinogradov, who began the study of $J_{s,k}(X)$ in the 1930s. Bounds on $J_{s,k}(X)$ find application throughout analytic number theory, such as Waring's problem, Diophantine approximation, character sums, equations over finite fields and the theory of the Riemann zeta function.

The lower bound

$$J_{s,k}(X) \gg X^s + X^{2s-\frac{1}{2}k(k+1)},$$

arises by considering the diagonal solutions of the system (1) with $x_i = y_i$ $(1 \le i \le s)$, together with a lower bound over that portion of the integral (2) from $|\alpha_i| \le (10kX^i)^{-1}$ $(1 \le i \le k)$. The *main conjecture* in Vinogradov's mean value theorem asserts that these lower bounds are reasonably sharp, i.e. for each $\varepsilon > 0$, one has

$$J_{s,k}(X) \ll X^{\varepsilon}(X^s + X^{2s-\frac{1}{2}k(k+1)}) = X^{\varepsilon}\begin{cases} X^s & (s \le \frac{k(k+1)}{2}) \\ X^{2s-\frac{1}{2}k(k+1)}) & (s \ge \frac{k(k+1)}{2}). \end{cases}$$

Since the 1940s, the main conjecture was known to hold for $s \gg k^2 \log k$ [5]. A recent breakthrough of Wooley ([6, 7]) has resulted in the main conjecture being proven in the much larger range $s \ge k^2 - 1$. The vehicle for this advance is the so-called “efficient congruencing” method. Our main goal is to establish the main conjecture in the complementary variable regime, showing that diagonal behavior dominates for half of the range conjectured.

Theorem 1. *Suppose that $k \ge 4$ and $1 \le s \le \frac{1}{4}(k+1)^2$. Then for each $\varepsilon > 0$, one has*

$$J_{s,k}(X) \ll X^{s+\varepsilon}. \tag{3}$$

In the range $1 \le s \le k$, the upper bound $J_{s,k}(X) \ll X^s$ follows directly from the Viéte-Girard-Newton formulae concerning the roots of polynomials. Hitherto, the only other case in which the bound (3) had been established was that in which $s = k + 1$ (see [3, Lemma 5.4]). Our proof extends the efficient congruencing method established in [6] and [7], incorporating ideas from the works of Arkhipov and Karatsuba [1] and Tyrina [4].

Our methods also improve the bounds on $J_{s,k}(X)$ for $\frac{1}{4}(k+1)^2 < s < k^2$; in particular, we show that

$$J_{s,k}(X) \ll X^{s+(3/2-\sqrt{2})k^2+O(k)}, \qquad s = \frac{k(k+1)}{2},$$

for the central critical value of s, improving the bound $J_{s,k}(X) \ll X^{s+(1/8)k^2+O(k)}$ established in [7].

References

[1] G. I. Arkhipov and A. A. Karatsuba, *A new estimate of an integral of I. M. Vinogradov*, Izv. Akad. Nauk SSSR Ser. Mat. **42** (1978), 751–762 (Russian), Math. USSR-Izv. **13** (1979), 52–62 (English).

[2] K. Ford and T. D. Wooley, On Vinogradov's mean value theorem: strongly diagonal behaviour via efficient congruencing, preprint.

[3] L.-K. Hua, *Additive theory of prime numbers*, American Math. Soc., Provide nce, RI, 1965.

[4] O. V. Tyrina, *A new estimate for a trigonometric integral of I. M. Vinogradov*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), 363–378 (Russian), Math. USSR-Izv. **30** (1988), 337–351 (English).

[5] I. M. Vinogradov, *The method of trigonometrical sums in the theory of numbers*, Trav. Inst. Math. Stekloff **23** (1947), 109pp (Russian); English translation by A. A. Davenport and K. F. Roth, Interscience, London (1954).

[6] T. D. Wooley, *Vinogradov's mean value theorem via efficient congruencing*, Annals of Math. **175** (2012), 1575–1627.

[7] T. D. Wooley, *Vinogradov's mean value theorem via efficient congruencing, II*, Duke Math. J. **162** (2013), 673–730.

Gaussian law and distribution of the divisor function in arithmetic progressions

Étienne Fouvry

(joint work with Satadal Ganguly, Emmanuel Kowalski and Philippe Michel)

Let f be a Hecke holomorphic cusp form, with even weight k for the full modular group. Let $\rho_f(n)$ be its normalized Fourier coefficient, hence we have the expansion formula

$$f(z) = \sum_{n\geq 1} \rho_f(n) n^{\frac{k-1}{2}} e(nz)\ (\Re z > 0).$$

By Deligne's Theorem, we know that the real number $\rho_f(n)$ is, in absolute value, less than $d(n)$, the usual divisor function. To study the behavior of the function $n \mapsto \rho_f(n)$ in an arithmetic progression, we are naturally led to consider the function

$$E_f(X;p,a) := \frac{\displaystyle\sum_{n\equiv a \bmod p} \rho_f(n) w(n/X)}{(X/p)^{\frac{1}{2}}},$$

where X is some real number tending to infinity, p is a prime number, a is an integer coprime with p, and w is a fixed smooth function, with compact support included in $[1,2]$. Heuristical considerations lead to the conclusion that the function $a \mapsto E_f(X;p,a)$ should roughly behave as a constant.

We also consider the same question for the divisor function, but here we have to substract a main term, since the function $d(n)$ does not oscillate. So let

$$E_d(X;p,a) := \frac{\displaystyle\sum_{n\equiv a \bmod p} d(n) w(n/X) - \frac{1}{p-1} \sum_{(n,p)=1} d(n) w(n/X)}{(X/p)^{\frac{1}{2}}}.$$

To state our central result, we introduce the following notations

$$\|w\| = \int_0^\infty |w(t)|^2\, dt \text{ and } \|f\| = \frac{3}{\pi^2} \int\int_{\mathrm{SL}(2,\mathbb{Z})\backslash\mathbb{H}} |f(z)|^2 \frac{dx\, dy}{y^2}.$$

We now state

Theorem 1. ([1]). *Let $\Phi : \mathbb{R}^+ \to \mathbb{R}^+$, a function tending to infinity at infinity, such that $\Phi(x) = O_\varepsilon(x^\varepsilon)$, for every $\varepsilon > 0$. Let $X := p^2/\Phi(p)$. Then, as p tends to infinity, the distribution of the functions*

$$a \in \mathbb{F}_p^* \mapsto \frac{E_f(X;p,a)}{\|w\|\|f\|\sqrt{4\pi/\Gamma(k)}} \text{ and } a \in \mathbb{F}_p^* \mapsto \frac{E_d(X;p,a)}{\|w\|\sqrt{\pi^{-2}\log^3\Phi(p)}},$$

tends to the normal law $\mathcal{N}(0,1)$.

The proof is based on the computation of the following κ–moment, where κ is an integer ≥ 1

$$\mathcal{M}_g(X;p,\kappa) := \sum_{a=1}^{p-1} E_g^{\kappa}(X;p,a),$$

where $g = f$ or d. In both situations, we appeal to additive characters (to detect the congruence condition) and to the Voronoi summation formula. The cornerstone of the proof of the asymptotic expansion of $\mathcal{M}_g(X;p,\kappa)$ is the following proposition concerning the normalized Kloosterman sum

$$\mathrm{Kl}_2(a;p) := \frac{1}{\sqrt{p}} \sum_{h=1}^{p-1} e\Big(\frac{ah+\overline{h}}{p}\Big).$$

Proposition 1. *Let p a prime number, let $\ell \geq 1$ be an integer, n_i $(1 \leq i \leq \ell)$ be integers, such that $1 \leq n_i < n_2 < \cdots < n_\ell < p$, and let $k_i (1 \leq i \leq \ell)$ be ℓ positive integers. We then have the equality*

$$\sum_{1 \leq a < p} \big(\mathrm{Kl}_2(an_1;p)\big)^{k_1} \cdots \big(\mathrm{Kl}_2(an_\ell;p)\big)^{k_\ell} = A(k_1,\ldots,k_\ell)\, p + O(p^{\frac{1}{2}}),$$

where the O–constant only depends on $(k_1,\ldots,k_\ell)$, and where

$$A(k_1,\ldots,k_\ell) := \Big(\frac{2}{\pi}\int_0^{\pi} (2\cos\theta)^{k_1} \sin^2\theta \, d\theta\Big) \cdots \Big(\frac{2}{\pi}\int_0^{\pi} (2\cos\theta)^{k_\ell} \sin^2\theta \, d\theta\Big).$$

In particular, we have $A(2,\ldots,2) = 1$.

The proof of this proposition consists in proving that some Kloosterman sheaves are independent. It is highly inspired by the work of Katz [2] concerning the vertical Sato–Tate law of the angles of $\mathrm{Kl}_2(a;p)$.

Proposition 1 can be generalised in several directions. For instance, we can answer to the following question: let

$$\gamma := \begin{pmatrix} \gamma_1 & \gamma_2 \\ \gamma_3 & \gamma_4 \end{pmatrix},$$

be a matrix with integer coefficients and non–zero determinant. For p sufficiently large, γ acts on $\mathbb{P}^1(\mathbb{F}_p)$ by the linear transformation $a \mapsto (\gamma_1 a + \gamma_2)/(\gamma_3 a + \gamma_4)$. When are the random variables

$$a \mapsto E_g(X;p,a) \text{ and } a \mapsto E_g(X;p,\gamma\cdot a),$$

independent? For $g = f$ or d, we find necessary and sufficient conditions for the required independency in terms of γ, w and g.

Finally, the authors conjecture that Theorem 1 should be true if Φ satisfies the weaker condition: $\Phi(x) = O_\varepsilon(x^{1-\varepsilon})$ for some $\varepsilon > 0$.

References

[1] E. Fouvry, S. Ganguly, E. Kowalski and Ph.Michel, *Gaussian distribution for the divisor function and Hecke eigenvalues in arithmetic progressions*, Comm. Math. Helv. (to appear).

[2] N.M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Annals of Mathematics Studies, 116. Princeton University Press, Princeton, NJ, 1988.

Finite Euler product approximations of the Riemann zeta-function

Steven M. Gonek

Let $F(s) = \zeta(s)+\chi(s)\zeta(\bar{s})$, where $\zeta(s)$ is the Riemann zeta-function and $\chi(s)$ is the factor from the functional equation $\zeta(s) = \chi(s)\zeta(1-s)$. Although $F(s)$ is not analytic, "knowing" it is essentially the same as "knowing" $\zeta(s)$. For instance, $F(s)$ has the same zeros as $\zeta(s)$ in the strip $1/2 \leq \Re s \leq 1$, except for finitely many exceptions. We construct a family of approximations $\{F_X(s)\}, X = 2, 3, \ldots,$ of $F(s)$ using finite Euler products, the pole of the zeta-function at $s = 1$, and any zeros the zeta-function might have in the right half of the critical strip. This construction is based on a hybrid Euler-Hadamard product formula for the zeta-function and the functional equation. We are then able to show that $F_X(s)$ converges to $F(s)$ as $X \to \infty$ provided that s is not a zero of the zeta-function. We also show how large X must be, in terms of s and the distance from s to the nearest zero, to guarantee a close approximation. By construction F and F_X have essentially the same zeros to the right of the critical line, F_X has at least as many zeros as F on the critical line, and these zeros converge to the zeros of F as $X \to \infty$. The analysis is unconditional and suggests that the zeta-function's zeros on and off the critical line "arise" in two ways. It is likely that F_X has about the same number of zeros as F on the critical line rather than more, but this seems quite difficult to prove when X is large.

References

[1] S. M. Gonek, *A note on finite Euler product approximations of the Riemann zeta-function*, to appear in Proc. Amer. Math. Soc..

[2] S. M. Gonek, *Finite Euler products and the Riemann Hypothesis*, Trans. Amer. Math. Soc. **364** (2012), 2157–2191.

[3] S. M. Gonek, C. P. Hughes and J. P. Keating, *A hybrid Euler-Hadamard product for the Riemann zeta function*, Duke Math. J. **136**, no. 3 , (2007), 507–549.

[4] S. M. Gonek and H. L. Montgomery, *Zeros of a Family of Approximations of the Riemann Zeta-Function*, Int Math Res Notices (2012). doi: 10.1093/imrn/rns187. First published online: August 14, 2012.

[5] E. C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, 2nd ed. (revised by D. R. Heath-Brown), The Claredon Press, Oxford University Press, New York, 1986.

Sharp bounds for moments of zeta

Adam Harper

The moments of the Riemann zeta function (on the critical line) are the integrals

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

where we usually think of $k \geq 0$ as fixed whilst $T \to \infty$. Random matrix theory supplies precise conjectures about the asymptotic behaviour of the moments, but the only known rigorous asymptotics are the classical results that

$$\int_T^{2T} |\zeta(1/2+it)|^2 dt \sim T \log T \quad \text{and} \quad \int_T^{2T} |\zeta(1/2+it)|^4 dt \sim \frac{1}{2\pi^2} T \log^4 T,$$

due to Hardy and Littlewood and to Ingham, respectively. If one could obtain good upper bounds for the moments with k large, one could deduce pointwise upper bounds for $|\zeta(1/2+it)|$, and potentially prove the Lindelöf Hypothesis. But until quite recently, even assuming the truth of the Riemann Hypothesis did not supply very good upper bounds[1] for the moments when $k > 2$.

In my talk I discussed the following result, taken from my preprint [1].

Theorem 1. *Assume the Riemann Hypothesis is true, and let $k \geq 0$ be fixed. Then for all large T we have*

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

where the implicit constant depends on k only.

This is sharp, except for the value of the implicit constant. Previously a sharp bound was only known (even conditionally on the Riemann Hypothesis) when $k < 2 + 2/11$, due to work of Ramachandra and of Heath-Brown [2] for $k \leq 2$, and work of Radziwiłł [3] for $2 < k < 2 + 2/11$. It was also known, assuming the Riemann Hypothesis, that $\int_T^{2T} |\zeta(1/2+it)|^{2k} dt \ll_{k,\epsilon} T \log^{k^2+\epsilon} T$ for any fixed $k \geq 0$ and $\epsilon > 0$, thanks to important recent work of Soundararajan [4].

The proof of Theorem 1 is a reworking of the proof of Soundararajan's bound $\ll_{k,\epsilon} T \log^{k^2+\epsilon} T$, and in my talk I began by discussing that argument. Whereas classical work on moments proceeds by approximating $\zeta(1/2+it)$ by partial sums $\sum_{n \leq x} \frac{1}{n^{1/2+it}}$ of its Dirichlet series, Soundararajan's argument proceeds by upper bounding $|\zeta(1/2+it)|$ by truncations of its Euler product. Thus Soundararajan showed, roughly speaking, that if the Riemann Hypothesis is true then

$$\log |\zeta(1/2+it)| = \Re \log \zeta(1/2+it) \lesssim \Re \sum_{p \leq x} \frac{1}{p^{1/2+it}} + \frac{\log T}{\log x},$$

where $T \leq t \leq 2T$, $2 \leq x \leq T^2$ is a free parameter, and p denotes primes.

[1] Prior to Soundararajan's work [4], by assuming the Riemann Hypothesis one could prove upper bounds of the form $T^{1+o_k(1)}$. These do imply the Lindelöf Hypothesis, but having assumed the Riemann Hypothesis one might hope to obtain much more precise information.

Formulae similar to the preceding one appear in classical work of Selberg and others. But the right hand side of Soundararajan's formula does not involve the zeta function or its zeros, whose behaviour is obscure, but only a sum over primes whose *distribution* may be studied as $T \leq t \leq 2T$ varies. In fact, integration by parts shows $\int_T^{2T} |\zeta(1/2+it)|^{2k} dt$ equals

$$\int_T^{2T} e^{2k \log|\zeta(1/2+it)|} dt = 2k \int_{-\infty}^{\infty} e^{2kV} \text{meas}\{T \leq t \leq 2T : \log|\zeta(1/2+it)| \geq V\} dV.$$

Then Soundararajan's formula implies that, for any choice of $2 \leq x = x(k,T,V) \leq T^2$, and writing $U = V - (\log T)/\log x$,

$$\text{meas}\{T \leq t \leq 2T : \log|\zeta(1/2+it)| \geq V\} \lesssim \text{meas}\{T \leq t \leq 2T : \Re \sum_{p \leq x} \frac{1}{p^{1/2+it}} \geq U\}.$$

Finally, to bound the measure of the latter set one notes that, for any $U \geq 0$ and any $A = A(k,T,V,x) \geq 0$,

$$\text{(1)} \qquad \text{meas}\{T \leq t \leq 2T : \Re \sum_{p \leq x} \frac{1}{p^{1/2+it}} \geq U\} \leq \frac{1}{U^A} \int_T^{2T} \left| \sum_{p \leq x} \frac{1}{p^{1/2+it}} \right|^A dt.$$

In practice, one needs to choose A to be an even integer, and such that $x^{A/2} \leq T$ (say), in order to obtain reasonable bounds for the integral. But nevertheless one has enormous flexibility in choosing x and A, separately for each V, and this is why Soundararajan's argument comes close to providing sharp bounds for moments.

There are two sources of loss in Soundararajan's argument. One of these, which I will not discuss here (see [1] for details), is a small intrinsic loss when bounding the measures of sets using "Markov's inequality", as in (1). A reader familiar with large deviation results in probability theory might be aware of this phenomenon in that context: one obtains bounds of the shape $e^{-z^2/2}$ for tail probabilities, rather than bounds $(1/z)e^{-z^2/2}$ which would generally (e.g. in the Gaussian case) be sharp. Here this phenomenon produces a loss of size about $\sqrt{\log\log T}$.

The other source of loss produces most of the $\log^{\epsilon} T$ factor. The crucial range of V in the argument is $V \approx k \log\log T$, and then one needs to choose A rather large, and certainly such that $A \to \infty$ as $T \to \infty$, in order to obtain reasonable bounds in (1). But since we must have $x^{A/2} \leq T$, this necessitates choosing $x = T^{o(1)}$. Then the term $(\log T)/\log x$ in Soundararajan's upper bound for $\log|\zeta(1/2+it)|$, which for most purposes should be thought of as an error term, tends to infinity with T and produces a loss. In order to obtain sharp bounds for moments, one needs to find a way to work with $x = T^{c(k)}$, where $c(k) > 0$ is small but *fixed*.

To see how to do this, it is useful to think heuristically about the behaviour of $\Re \sum_{p \leq x} \frac{1}{p^{1/2+it}}$. As $T \leq t \leq 2T$ varies, the $(p^{it})_{p \leq x}$ "ought to behave" rather like independent random variables $(U_p)_{p \leq x}$, each distributed uniformly on the unit circle $\{|z| = 1\}$. Thus by the Central Limit Theorem, and a simple computation of the mean and variance of the sum, one expects that

$$\Re \sum_{p \le x} \frac{1}{p^{1/2+it}} \quad \text{will behave like} \quad N(0, \frac{1}{2} \sum_{p \le x} \frac{1}{p}).$$

Now the crucial point is that $\sum_{p \le x} 1/p \sim \log\log x$ grows very slowly with x, and in particular *later terms in the sum contribute very little.* Thus we would expect that, usually, $\Re \sum_{p \le T} \frac{1}{p^{1/2+it}} \asymp \sqrt{\log\log T}$ (which is its "standard deviation"), but that usually $\Re \sum_{T^{1/1000} \le p \le T} \frac{1}{p^{1/2+it}} \asymp \sqrt{\sum_{T^{1/1000} \le p \le T} \frac{1}{p}} \asymp 1$. So, presumably, it is usually true that if $\Re \sum_{p \le T^{c(k)}} \frac{1}{p^{1/2+it}}$ is very large, it is because the "first part" of the sum is very large.

The course of action suggested by the above is that, instead of investigating $\text{meas}\{T \le t \le 2T : \Re \sum_{p \le x} \frac{1}{p^{1/2+it}} \ge U\}$, one should try to bound

$$\begin{aligned} \text{meas}\{T \le t \le 2T : \quad & \Re \sum_{p \le x_1} \frac{1}{p^{1/2+it}} \ge U_1, \\ & \text{and } \Re \sum_{x_1 < p \le x_2} \frac{1}{p^{1/2+it}} \ge U_2, \text{ and } ... \Re \sum_{x_{l-1} < p \le x_l} \frac{1}{p^{1/2+it}} \ge U_l\}, \end{aligned}$$

where $2 \le x_1 < x_2 < ... < x_l = T^{c(k)}$ are suitably chosen break points. Then in place of (1) one considers integrals of the form

$$\frac{1}{U_1^{A_1} ... U_l^{A_l}} \int_T^{2T} \left| \sum_{p \le x_1} \frac{1}{p^{1/2+it}} \right|^{A_1} ... \left| \sum_{x_{l-1} < p \le x_l} \frac{1}{p^{1/2+it}} \right|^{A_l} dt.$$

In particular, there is obviously no requirement for all the A_j to be the same, so one can choose $A_j \to \infty$ for small j (where it needs to be large to detect large values of $\sum_{x_{j-1} < p \le x_j} \frac{1}{p^{1/2+it}}$, but this is permissible because x_j is small), whilst choosing $A_j = O(1)$ for larger j. One actually needs a multi-stage argument that lets one assume that all the sums are "about the right size", but essentially this kind of splitting procedure is what is needed to obtain sharp moment bounds.

Needless to say, it would be of great interest to upgrade Theorem 1 to give an asymptotic formula in any case when $k \ne 0, 1, 2$, but at present there is no apparent way to do so.

References

[1] A. J. Harper. Sharp conditional bounds for moments of the Riemann zeta function. Preprint available online at `http://arxiv.org/abs/1305.4618`

[2] D. R. Heath-Brown. Fractional moments of the Riemann zeta-function. *J. London Math. Soc.*, **24**, no. 2, pp 65-78. 1981

[3] M. Radziwiłł. The 4.36th Moment of the Riemann Zeta-Function. *International Mathematics Research Notices*, **2012**, no. 18, pp 4245-4259. 2012

[4] K. Soundararajan. Moments of the Riemann zeta function. *Ann. Math.*, **170**, pp 981-993. 2009

Zeros of systems of forms

Roger Heath-Brown
(joint work with Tim Browning)

This talk concerns work in progress. We are concerned with integral solutions to general systems of homogeneous equations

$$F_1(x_1,\dots,x_n)=\cdots=F_R(x_1,\dots,x_n)=0 \tag{1}$$

where each form F_i has coefficients in $\mathbb{Z}$. Our strategy is to build on the methods developed by Birch [1] and Schmidt [2], using the circle method.

Birch's method applies only when all the forms have the same degree D, say. His result is described in terms of the dimension (B say) of the "singular locus", and shows that the expected Hardy-Littlewood asymptotic formula holds when

$$n>B+R(R+1)(D-1)2^{D-1}. \tag{2}$$

We shall say that the system (1) is nonsingular if the gradient vectors

$$\nabla F_1(\mathbf{x}),\dots,\nabla F_R(\mathbf{x})$$

are linearly dependent for all non-zero $\mathbf{x}\in\overline{\mathbb{Q}}^n$ satisfying (1). Under this condition one can show that $B\le R-1$, and it appears to be an open question whether or not one always has $B=R-1$. In any event one may conclude that, when $R=1$ and $F_1=0$ defines a smooth hypersurface in $\mathbb{P}^{n-1}$ it suffices to have

$$n>(D-1)2^D. \tag{3}$$

In Schmidt's analysis one is allowed forms of differing degrees. For most of his results the work is based on certain "h-invariants". These give results involving lower bounds for n which are not directly comparable with Birch's because the number B does not appear. However for nonsingular systems of forms of equal degrees the Birch bound is sharper.

Our goal is to apply Birch's approach to systems of differing degrees. Schmidt provides a result in this direction [2, Corollary, page 262], but there are some losses in his method.

We prove two particularly succinct results, which generalize (3).

Theorem 1. *Let $V\subseteq\mathbb{P}^n$ be a smooth, non-degenerate, absolutely irreducible variety defined over $\mathbb{Q}$. Then V satisfies the Hasse principle and weak approximation provided only that*

$$n\ge(\deg(V)-1)2^{\deg(V)}.$$

Moreover there is an asymptotic formula of Hardy–Littlewood type for the counting function for rational points of bounded height on V.

When V is a hypersurface this theorem reduces to (1). However we are able to handle varieties of arbitrary codimension. We would like to emphasize indeed that our lower bound on n makes no reference to the codimension of V, nor to the shape of the defining equations for V. In particular we have not required V to be a complete intersection.

For our second result we suppose that our system consists of r_d forms of degree d, for each positive integer $d \leq D$. We assume that $r_D \geq 1$, but do not require that $r_d \neq 0$ for smaller d. We then write $\mathcal{D} = r_1 + 2r_2 + \ldots + Dr_D$.

Theorem 2. *Suppose we have a nonsingular system of forms for which*

$$n > (\mathcal{D} - 1)2^{\mathcal{D}}.$$

Then the corresponding projective variety satisfies the Hasse principle and weak approximation. Moreover there is an asymptotic formula of Hardy–Littlewood type for the counting function for integral zeros of the system.

In fact the bounds required for n in these two results are very wasteful as soon as $R \geq 2$.

To state our most general result we define

$$\mathcal{D}_j = r_1 + 2r_2 + \ldots + jr_j, \quad (0 \leq j \leq D),$$

$$t_d = \sum_{k=d}^{D} 2^{k-1}(k-1)r_k, \quad (1 \leq d \leq D+1),$$

and

$$n_0(d) = R - 1 + \mathcal{D}_d\left(2^{d-1} + t_{d+1}\right) + t_{d+1} + \sum_{j=d+1}^{D} t_j r_j.$$

We then have the following.

Theorem 3. *Suppose we have a nonsingular system of forms such that* n *is strictly greater than* $n_0(d)$ *for every degree* d *for which* $r_d \geq 1$*, and assume also that* $n > n_0(0)$*. Then the corresponding projective variety satisfies the Hasse principle and weak approximation. Moreover there is an asymptotic formula of Hardy–Littlewood type for the counting function for integral zeros of the system.*

As an application one may consider a system consisting of just two forms, of degrees $D > E \geq 2$. One then finds that one requires

$$n > 1 + (2 + E)(D - 1)2^{D-1} + E2^{E-1}.$$

One may compare this with the corresponding result for systems consisting of two forms of degree D, for which the corresponding condition is that $n > 1+3(D-1)2^D$. Thus the bound for degrees E and D is larger than the bound for degrees D and D, as soon as $E \geq 4$. This is a little disappointing since one expects that the former case should be “easier”.

References

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

[2] W. Schmidt, *The density of integer points on homogeneous varieties*, Acta Math. **154** (1985), 243–296.

The ternary Goldbach problem

Harald Helfgott

The ternary Goldbach conjecture (or *three-prime problem*) states that every odd number n greater than 5 can be written as the sum of three primes. Both the ternary Goldbach conjecture and the (stronger) binary Goldbach conjecture (stating that every even number greater than 2 can be written as the sum of two primes) have their origin in the correspondence between Euler and Goldbach (1742). See [1, Ch. XVIII] for the early history of the problem.

I. M. Vinogradov [7] showed in 1937 that the ternary Goldbach conjecture is true for all n above a large constant C. Unfortunately, while the value of C has been improved several times since then, it has always remained much too large ($C = e^{3100}$, [5]) for a mechanical verification up to C to be even remotely feasible. The situation was paradoxical: the conjecture was known above an explicit C, but, even after seventy years of improvements, this C was so large that it could not be said that the problem could be attacked by any conceivable computational means within our physical universe. (The number of subatomic particles in the known universe is currently estimated at $\sim 10^{80}$.) Thus, the only way forward was a series of drastic improvements in the mathematical, rather than computational, side.

In two recent papers ([2] and [3]), I prove the ternary Goldbach conjecture.

Every odd integer n greater than 5 *can be expressed as the sum of three primes.*

The proof given in [2] and [3] works for all $n \geq C = 10^{29}$. The main theorem has been checked deterministically by computer for all $n < 10^{29}$ (and indeed for all $n \leq 8.875 \cdot 10^{30}$) [4].

(An analytic proof, in general, gives not only the existence of a way to express a number n in a certain form (say, as the sum of three primes), but also an estimate on the (weighted) number of ways to do so. Such an estimate is of the form

$$\text{main term} + \text{error term},$$

where the main term is a precise function $f(n)$ and the error term is shown to be bounded from above by a function $g(n)$; the proof works if $g(n) < f(n)$ asymptotically as $n \to \infty$. Of course, this means that such a proof works only for n greater than some constant C, leaving small n to be verified by direct computation. The task of verifying the main theorem for $n < 10^{29}$ is really a minor computational task. The main computation involved in the proof is by far a verification of GRH up to bounded conductor and bounded height (due to D. Platt [6]).)

The approach is based on the circle method, and, more particularly, on a study of exponential sums $\sum_p e(\alpha p)\eta(p/x)$, where η is a weight of our choice (a "smoothing function", or simply a "smoothing"). Such exponential sums are estimated in [2] and [3] for α lying in the major and minor arcs, respectively.

I am able to set major arcs to be few and narrow because the minor-arc estimates in [3] are very strong; I am forced to take them to be few and narrow because of the kind of L-function bounds we will rely upon.

One of the main lessons of the proof – also present in [3] – is the close relation between the circle method and the large sieve; rather than see large-sieve methods as a black box, it is best, in this context, to see them as a source for ideas. The large sieve for primes – nearly optimized here, following Ramaré – is a case in point.

References

[1] L. E. Dickson, *History of the theory of numbers. Vol. I: Divisibility and primality*, Chelsea Publishing Co., 1966, xii+486.

[2] H. A. Helfgott, “Major arcs for Goldbach's problem”, preprint. Available as `arXiv:1205.5252`.

[3] H. A. Helfgott, “Minor arcs for Goldbach's problem”, preprint. Available as `arXiv:1305.2897`.

[4] H. A. Helfgott and D. Platt, “Numerical Verification of the Ternary Goldbach conjecture up to $8.875e30$”, preprint. Available as `arXiv.org:1305.3062`.

[5] M.-Ch. Liu and T. Wang, “On the Vinogradov bound in the three primes Goldbach conjecture”, *Acta Arith.* **105** (2002), no. 2, pp. 133–175.

[6] D. Platt, “Numerical computations concerning GRH”, preprint. Available as `arXiv:1305.3087`.

[7] I. M. Vinogradov, “Representation of an odd number as a sum of three primes”, *Dokl. Akad. Nauk. SSR* **15** (1937), 291–294.

Twists and resonance of *L*-functions

Jerzy Kaczorowski

(joint work with Alberto Perelli)

For an L-function F from the extended Selberg class $S^\sharp$ and a real valued function f defined on positive integers, the twist is defined as follows

$$F(s,f)=\sum_{n=1}^{\infty}\frac{a_F(n)}{n^s}e(f(n)) \qquad (\sigma>1)$$

where, as usual, $e(\theta)=\exp(2\pi i\theta)$. We refer to [1] for the basic information on the Selberg class theory. We say that there is a resonance between coefficients $a_F(n)$ and the exponent $f(n)$ if $F(s,f)$ has meromorphic continuation to $\mathbb{C}$ and has at least one singularity. For a given $F\in S^\sharp$ of positive degree d_F and $f:\mathbb{N}\to\mathbb{R}$ of the form

$$f(n,\alpha)=n^{\kappa_0}\sum_{\nu=0}^{N}\alpha_\nu n^{-\omega_\nu},$$

where $\alpha=(\alpha_0,\ldots,\alpha_N)\in\mathbb{R}^{N+1}$, $0=\omega_0<\omega_1<\ldots<\omega_N<\kappa_0$, $\kappa_0>1/d_F$ we define the conjugated exponent $f^*(n,\alpha)$ which is of the form

$$f^*(n,\alpha)=n^{\kappa_0^*}\sum_{\substack{\omega\in D_f\\ \omega<\kappa_0}}A_\omega(\alpha)n^{-\omega^*},$$

where $\kappa_0^*=\kappa_0/(\kappa_0 d_F-1)$, $\omega^*=\omega/(\kappa_0 d_F-1)$, and D_f is the additive semigroup generated by the ω-exponents of f. We skip here details of this construction.

Twists $F(s,f)$ and $F(s,f^*)$ are related by a general transformation formula of the following form

$$F(s,f) = \sum_j W_j(s) F(s^* + \eta_j, f^*) + G(s), \tag{1}$$

where W_j's and G are 'nice' functions of s, and η_j's are real shifts. For a 'normalized' F we have

$$s^* = \frac{s + \frac{d_F\kappa_0}{2} - 1}{d_F\kappa_0 - 1}.$$

We consider the group G_F generated by the following transformations of exponents: $T : f \mapsto f^*$ and $S_m : f \mapsto f + n^m$ for every $m = 1, 2, \ldots$ For $X \in G_F$ we define $X(f)$ in an obvious way whenever possible. By (1) it is evident that analytic properties of $F(s, X(f))$ can be read from these of $F(s,f)$ and vice versa. Let

$$\mathcal{A}(F) = \{f = X(f_0) : X \in G_F \text{ and } f_0 \text{ has the leading exponent } \kappa_0 \le 1/d_F\},$$

$$\mathcal{A}_0(F) = \{f \in \mathcal{A}(F) : f_0(n) = \alpha n^{1/d_F},\ a_F(q_F|\alpha|^{d_F} d_F^{-d_F}) \neq 0\},$$

where q_F denotes the conductor of F and we put $a_F(\xi) = 0$ if $\xi \notin \mathbb{N}$.

Theorem. *For an L-function $F \in S^\sharp$ of a positive degree the following statements hold true.*

1. *If $f \in \mathcal{A}(F)$ then the twist $F(s,f)$ is meromorphic on $\mathbb{C}$ and for every fixed real $A < B$ and $\varepsilon > 0$ we have $F(\sigma + it, f) \ll \exp(\varepsilon|t|)$ as $|t| \to \infty$ uniformly for $A < \sigma < B$.*
2. *If $f \in \mathcal{A}(F) \backslash \mathcal{A}_0(F)$ then $F(s,f)$ is entire.*
3. *If $f \in \mathcal{A}_0(F)$ then $F(s,f)$ has simple poles on the half-line $s = \sigma + i\theta_F$, $\sigma \le \frac{1}{2} + \frac{1}{2d_F D(f)}$, where θ_F is a constant depending only on F, and $D(f)$ is a constant explicitly defined in terms of $X \in G_F$ such that $f = X(f_0)$.*

Example. Consider the following elliptic curve defined over $\mathbb{Q}$

$$E : y^2 - y = x^3 - x.$$

The corresponding (normalized) L-function $F(s) = L(s + \frac{1}{2}, E)$ belongs to the Selberg class, has degree 2 and conductor 37. Take $f_0(n) = \frac{2}{\sqrt{37}} n^{1/2}$ and $X = TS_2 \in G_F$. Then

$$X(f_0)(n) = \alpha_0 n^{2/3} + \beta_0 n^{1/6},$$

where

$$\alpha_0 = 3 \cdot 2^{-4/3} 37^{-2/3} \quad \text{and} \quad \beta_0 = 37^{-2/3}.$$

We have $X(f_0) \in \mathcal{A}_0(F)$. Hence the twist

$$\sum_{n=1}^{\infty} \frac{a_E(n)}{n^s} e(\alpha_0 n^{2/3} + \beta_0 n^{1/6})$$

defined initially for $\sigma > 1$ has meromorphic continuation to $\mathbb{C}$ with a simple pole at $s = 7/12$. In particular

$$\sum_n a_E(n) e(\alpha_0 n^{2/3} + \beta_0 n^{1/6}) e^{-n/x} \sim c_0 x^{\frac{7}{12}} \qquad (x \to \infty)$$

for certain $c_0 \neq 0$. We see that the resonance is present in this case. It can disappear when we change β_0. For instance if $|\beta| < \beta_0$ then the new exponent $\alpha_0 n^{2/3} + \beta n^{1/6}$ belongs to $\mathcal{A}(F) \backslash \mathcal{A}_0(F)$ and the corresponding twist is entire. There is no resonance here and we have

$$\sum_n a_E(n) e(\alpha_0 n^{2/3} + \beta n^{1/6}) e^{-n/x} \ll 1 \qquad (x \to \infty).$$

The same happens when we keep α_0 and β_0 but introduce a new term with a lower exponent:

$$f(n) = \alpha_0 n^{2/3} + \beta_0 n^{1/6} + \gamma n^{\lambda},$$

$\gamma \neq 0$, $0 < \lambda < 1/6$.

References

[1] J. Kaczorowski, A. Perelli, - *The Selberg class: a survey* - In *Number Theory in Progress*, Proc. Conf. in Honor of A.Schinzel, ed. by K.Győry *et al.*, 953–992, de Gruyter 1999.

On sums of cubes of primes and almost primes.

Koichi Kawada

In 1938, Hua showed amongst others that every sufficiently large odd integer is the sum of nine cubes of primes, by applying technique on estimating exponential sums over primes that Vinogradov had published in the preceding year. In this direction, one may next wish to prove that every large even integer can be written as the sum of eight cubes of primes.

The parity constraints contained in these statements are often called "necessary" congruence conditions. If an odd integer is the sum of eight cubes of primes, for instance, then at least one of the eight primes must be even, that is, 2. Thus searching for a representation of an odd integer n as the sum of eight cubes of primes is reduced to seeking for a representation of $n - 2^3$ as the sum of *seven* cubes of primes, so the question turns into a problem involving only seven variables. In this sense, it is natural to concentrate on even integers when we consider representations by sums of eight cubes of primes. But needless to say, there are many odd integers that are sums of eight cubes of primes, and indeed this year, 2013, is such an example.

Theorem 1. Although 2013 is odd, it is the sum of eight cubes of primes.

Proof. $2013 = 2^3 + 3^3 + 3^3 + 3^3 + 5^3 + 5^3 + 7^3 + 11^3$.

Seriously, no one hitherto has succeeded in proving that every large even integer is the sum of eight cubes of primes, but several results that somewhat approach this end have been obtained. In particular, Brüdern [1] proved that every large even n can be written as

$$n = p_1^3 + \cdots + p_7^3 + x^3, \tag{1}$$

where p_j's are primes and x is a P_4. (We call an integer x P_r, when x is the product of at most r primes.) Following this work, the author [3] showed that P_4 can be replaced by P_3 in the latter statement, and also in a collaboration with Brüdern [2] that every large even n may be written as $n = p_1^3 + \cdots + p_6^3 + x^3 + y^3$, with primes p_j and P_2-numbers x and y. The result I report in my talk is a refinement of the latter assertions.

Theorem 2. Every large even integer n admits the expression (1) with primes p_j and a P_2-number x.

The proof is relies on a couple of important methods. One is the diminishing range method restricted minor arcs only due to Vaughan [4]. Another is the new method on handling minor arc integrals that recently invented by Zhao [5], who gave a fine lecture on this very method in this workshop. The strategy of the proof of Theorem 2 fails very narrowly, in a certain sense, to establish that every large even integer is the sum of eight cubes of primes.

It is known that this kind of work is closely related to conclusions concerning sums of four cubes, and indeed we may also show that almost all integers n satisfying the necessary congruence condition ($n \pm 1$ are both coprime to 14, and $n \not\equiv \pm 1, \pm 3 \pmod 9$) can be written as $n = p_1^3 + p_2^3 + p_3^3 + x^3$, where p_j's are primes and x is a P_2.

References

[1] J. Brüdern, *A sieve approach to the Waring-Goldbach problem, I: Sums of four cubes*, Ann. Scient. École. Norm. Sup. (4) **28** (1995), 461–476.

[2] J. Brüdern and K. Kawada, *On the Waring-Goldbach problem for cubes*, Glasg. Math. J. **51** (2009), 703–712.

[3] K. Kawada, *Note on the sum of cubes of primes and an almost prime*, Arch. Math. (Basel) **69** (1997), 13–19.

[4] R. C. Vaughan, *On Waring's problem for sixth powers*, J. London Math. Soc. (3) **33** (1986), 227–236.

[5] L. Zhao, *On the Waring-Goldbach problem for fourth and sixth powers*, to appear.

On congruences and equations with products of variables from short intervals and applications

Sergei Konyagin

(joint work with Jean Bourgain, Moubariz Garaev, Igor Shparlinski)

We obtain upper bounds on the number of solutions to congruences of the type

$$(x_1+s)\dots(x_\nu+s)\equiv(y_1+s)\dots(y_\nu+s)\not\equiv 0 \pmod p$$

modulo a prime p with variables from some short intervals. We give some applications of our results and in particular improve several recent estimates of J. Cilleruelo and M. Z. Garaev on exponential congruences and on cardinalities of products of short intervals, some double character sum estimates of J. Friedlander and H. Iwaniec and some results of M.-C. Chang and A. A. Karatsuba on character sums twisted with the divisor function. For almost all p and all s and also for a fixed p and almost all s, we derive stronger bounds. Next, we estimate the number of nontrivial solutions to the equation

$$(x_1+s)\dots(x_\nu+s)=(y_1+s)\dots(y_\nu+s)\not\equiv 0$$

for algebraic s. We also use similar ideas to show that for almost all primes, one can always find an element of a large order in any rather short interval.

Our results are published in [1] and [2].

References

[1] J. Bourgain, M.Z. Garaev, S.V. Konyagin, I.E. Shparlinski, *On congruences with products of variables from short intervals and applications*, Proc. Steklov Inst. Math. **280** (2013), 67–96; arXiv:1203.0017.

[2] J. Bourgain, M.Z. Garaev, S.V. Konyagin, I.E. Shparlinski, *Multiplicative congruences with variables from short intervals*, arXiv:1210.6429.

The distribution of the maximum of character sums

Dimitris Koukoulopoulos

(joint work with Jonathan Bober, Leo Goldmakher and Andrew Granville)

Given a Dirichlet character $\chi \pmod q$, we define

$$M(\chi)=\max_{1\le x\le q}\left|\sum_{n\le x}\chi(n)\right|,$$

the maximum modulus of its partial sums. If χ is non-principal, then Pólya and Vinogradov [Da00, Ch. 23] showed in 1918 that

$$M(\chi)\ll\sqrt{q}\log q.$$

This result was improved by Montgomery and Vaughan [MV77] under the assumption of the Generalized Riemann Hypothesis to

$$M(\chi)\ll\sqrt{q}\log\log q.$$

The latter result is best possible, as Paley [Pa] had already shown in 1932 that there is a sequence of moduli $q_n \to \infty$ such that

$$M\left(\left(\frac{q_n}{\cdot}\right)\right) \gg \sqrt{q_n}\log\log q_n.$$

However, such extremal examples are believed to be rare. To this end, given $\tau \geq 0$, we set

$$P_q(\tau) = \frac{1}{\phi(q)}\#\left\{\chi \,(\mathrm{mod}\, q) : M(\chi) > (e^{\gamma}/\pi)\cdot\tau\sqrt{q}\right\},$$

the probability that $M(\chi) > \frac{e^{\gamma}}{\pi}\tau\sqrt{q}$. (Here the constant e^{γ}/π is inserted to make the statements of our results simpler.) Montgomery and Vaughan [MV79] showed that $P_q(\tau) \ll_A 1/\tau^A$, uniformly for $\tau \geq 1$ and $q \in \mathbb{N}$, where A is an arbitrary fixed number. This result was improved in some aspects recently by Bober and Goldmakher [BG13], who showed that, for fixed $\tau \geq 1$ and $q \to \infty$ over primes,

$$\exp\left\{-\frac{c_0 e^{\tau}}{\tau}(1 + o_{\tau\to\infty}(1))\right\} \leq P_q(\tau) \leq \exp\left\{-e^{B\sqrt{\tau}/(\log\tau)^{1/4}}\right\},$$

where B is some constant and $c_0 = 1.09258\ldots$ is an explicit constant given in terms of Bessel functions. It should be noted that the same constant c_0 appears also in the work of Granville-Soundararajan [GS07] on the distribution of $L(1,\chi)$. This is by no means a coincidence: both the aforementioned result as well as Theorem 1 below pass through results about the distribution of $L(1,\chi)$.

In our work we improve on the above results. More precisely, we show the following theorem:

Theorem 1. *If q is prime and $1 \leq \tau \leq \log\log q - M$, for some $M \geq 1$, then*

$$\exp\left\{-\frac{c_0 e^{\tau}}{\tau}(1 + o_{\tau,M\to\infty}(1))\right\} \leq P_q(\tau) \leq \exp\left\{-e^{\tau + O_{\epsilon}(\tau^{1/2+\epsilon})}\right\}.$$

The proof of the above result incorporates a combination of various techniques. We use some probabilistic methods, such as the estimation of certain high moments of objects related to $M(\chi)$. Moreover, as mentioned above, we use ideas from the study of the distribution of $L(1,\chi)$. Finally, we employ some techniques arising from the theory of *pretentious multiplicative functions*. This theory played a central role in the work of Granville and Soundararajan [GS07], who realized that characters for which $M(\chi)$ is abnormally large have a multiplicative structure which resembles a lot the structure of another character of smaller conductor. Goldmakher [Gol12] subsequently built further on these ideas to obtain sharper results. This idea, of a character pretending to be another character, features prominently in the proof of Theorem 1. In fact, our arguments imply that most of the contribution to $P_q(\tau)$ comes from odd characters $\chi \pmod q$ such that $\chi(p) \approx 1$ for most primes $p \leq e^{\tau}$.

References

[BG13] J. Bober and L. Goldmakher, *The distribution of the maximum of character sums.* Mathematika 59 (2013), no. 2, 427–442.

[Da00] H. Davenport, *Multiplicative number theory.* Third edition. Revised and with a preface by Hugh L. Montgomery. Graduate Texts in Mathematics, 74. Springer-Verlag, New York, 2000.

[Gol12] L. Goldmakher, *Multiplicative mimicry and improvements to the Pólya-Vinogradov inequality.* Algebra Number Theory **6** (2012), no. 1, 123–163.

[GS06] A. Granville and K. Soundararajan, *Extreme values of* $|\zeta(1+it)|$. The Riemann zeta function and related themes: papers in honour of Professor K. Ramachandra, 65–80, Ramanujan Math. Soc. Lect. Notes Ser., 2, Ramanujan Math. Soc., Mysore, 2006.

[GS07] —, *Large character sums: pretentious characters and the Pólya-Vinogradov theorem.* J. Amer. Math. Soc. **20** (2007), no. 2, 357–384.

[MV77] H. L. Montgomery and R. C. Vaughan, *Exponential sums with multiplicative coefficients.* Invent. Math. **43** (1977), no. 1, 69–82.

[MV79] —, *Mean values of character sums.* Canad. J. Math.**31** (1979), no. 3, 476–487.

[Pa] R. E. A. C. Paley, *A Theorem on Characters.* J. London Math. Soc. S1-7 no. 1, 28.

Diophantine equations in the primes

Ákos Magyar
(joint work with Brian Cook)

We studied prime solutions of general systems of diophantine equations. Our main result was to obtain an asymptotic formula for the number of prime solutions for systems whose Schmidt rank is sufficiently large with respect to the the number and degree of the polynomials.

The primary technique used in the proof is the circle method, and our approach is based on a partition of the variables to apply mean value type estimates on the minor arcs. A crucial novel feature of the argument is a ”regularity lemma” exploiting the reductive properties of the Schmidt rank. It essentially means that one can partition the level sets of a system of forms by the level sets of a new systems of forms which have high Schmidt rank in each degree. This new system is regular in the sense that the lattice points are distributed uniformly on its level sets. Passing to the joint level of sets of this regular system forms provides a place to carry out a simple Cauchy-Schwartz argument providing suitable mean value estimates on the minor arcs. The derivation of the asymptotic formula from the contribution of the major arcs is standard and is in agreement with general local-global type heuristics.

Our method have a certain flexibility and might be modified to study further related problems.

1. One may study not just the number but the large scale distribution of prime points (points with prime coordinates) on varieties defined by a system of integral polynomials of large rank. The crucial point is to understand the Fourier transform of the prime points on such varieties. This might be feasible as the minor arcs estimates seem to be uniform in the phase variable.

2. The results may also be strengthened in various ways. An immediate question is to prove our asymptotic formula under the more natural condition of the largeness of the rational Schmidt rank, instead of the complex Schmidt rank. Here one needs to refine the elementary algebraic geometric arguments used to obtain a suitable partition of the system to sub-systems of large ranks.

3. An interesting, and challenging problem is to bring the rank conditions in agreement with those of Schmidt and Birch for the case of integer solutions. For example for a single quadratic form our method needs the rank to be at least 22 as opposed to 5 needed for the existence of integer solutions. It might be that one can approach this problem through an appropriate transference principle, such transfer principle played a crucial role for systems of linear forms.

Generalizations of a cotangent sum associated to the zeros of the Estermann zeta function

Helmut Maier
(joint work with Michael Th. Rassias)

The Estermann zeta function $E\left(s, \frac{h}{k}, \alpha\right)$ is defined by the Dirichlet series

$$E\left(s, \frac{h}{k}, \alpha\right) = \sum_{n\geq 1} \frac{\sigma_\alpha(n)\exp\left(2\pi i h n/k\right)}{n^s}\ ,$$

where $Re\, s > Re\, \alpha + 1$, $k \geq 1$, $(h,k) = 1$ and $\sigma_\alpha(n) = \sum_{d|n} d^\alpha$.
In 1985, R. Balasubramanian, J. B. Conrey and D. R. Heath-Brown [2], used properties of $E\left(0, \frac{h}{k}, 0\right)$ to prove an asymptotic formula for

$$I = \int_0^T \left|\zeta\left(\frac{1}{2}+it\right)\right|^2 \left|A\left(\frac{1}{2}+it\right)\right|^2 dt\ ,$$

where $A(s)$ is a Dirichlet polynomial.
Period functions and families of cotangent sums appear in recent work of S. Bettin and J. B. Conrey (see [3]). They generalize the Dedekind sum and share with it the property of satisfying a reciprocity formula. They have proved a reciprocity formula for the V. I. Vasyunin's sum (see [9]), which appears in the Nyman-Beurling criterion (see [1]) for the Riemann Hypothesis.
In 1995, M. Ishibashi (see [5]) among other results proved that for $k \geq 2$, $1 \leq h \leq k$, $(h,k) = 1$, it holds

$$E\left(0, \frac{h}{k}, 0\right) = \frac{1}{4} + \frac{i}{2} c_0\left(\frac{h}{k}\right)\ ,$$

where

$$c_0\left(\frac{h}{k}\right) = -\sum_{m=1}^{k-1} \frac{m}{k} \cot\left(\frac{\pi m h}{k}\right)\ .$$

In the present talk, an improvement as well as a further generalization of Vasyunin's asymptotic formula regarding the relevant cotangent sums are presented. Furthermore, we discuss asymptotic formulas for the moments of the cotangent sums under consideration. We present the following results:

Theorem 1. *Let $b, n \in \mathbb{N}$, $b \geq 6N$, with $N = \lfloor n/2 \rfloor + 1$.There exist absolute real constants $A_1, A_2 \geq 1$ and absolute real constants E_l, $l \in \mathbb{N}$ with $|E_l| \leq (A_1 l)^{2l}$, such that for each $n \in \mathbb{N}$ we have*

$$c_0\left(\frac{1}{b}\right) = \frac{1}{\pi} b \log b - \frac{b}{\pi}(\log 2\pi - \gamma) - 1 + \sum_{l=1}^{n} E_l b^{-l} + R_n^*(b)$$

where $|R_n^*(b)| \leq (A_2 n)^{4n}\, b^{-(n+1)}$.

Proposition 1. *For r, $b \in \mathbb{N}$ with $(r, b) = 1$, it holds*

$$c_0\left(\frac{r}{b}\right) = \frac{1}{r}\, c_0\left(\frac{1}{b}\right) - \frac{1}{r} Q\left(\frac{r}{b}\right),$$

where

$$Q\left(\frac{r}{b}\right) = \sum_{m=1}^{b-1} \cot\left(\frac{\pi m r}{b}\right) \left\lfloor \frac{rm}{b} \right\rfloor .$$

Theorem 2. *Let $r, b_0 \in \mathbb{N}$ be fixed, with $(b_0, r) = 1$. Let b denote a positive integer with $b \equiv b_0 \pmod r$. Then, there exists a constant $C_1 = C_1(r, b_0)$, with $C_1(1, b_0) = 0$, such that*

$$c_0\left(\frac{r}{b}\right) = \frac{1}{\pi r} b \log b - \frac{b}{\pi r}(\log 2\pi - \gamma) + C_1\, b + O(1), \quad (b \to +\infty).$$

Theorem 3. *Let $k \in \mathbb{N}$ be fixed. Let also A_0, A_1 be fixed constants such that $1/2 < A_0 < A_1 < 1$. Then there exists a constant $H_k > 0$, depending only on k, such that*

$$\sum_{\substack{r:(r,b)=1 \\ A_0 b \leq r \leq A_1 b}} c_0\left(\frac{r}{b}\right)^{2k} = H_k \cdot (A_1 - A_0) b^{2k} \phi(b)(1 + o(1)), \quad (b \to +\infty).$$

Theorem 4. *Let $k \in \mathbb{N}$ be fixed. Let also A_0, A_1 be fixed constants such that $1/2 < A_0 < A_1 < 1$. Then we have*

$$\sum_{\substack{r:(r,b)=1 \\ A_0 b \leq r \leq A_1 b}} c_0\left(\frac{r}{b}\right)^{2k-1} = o\left(b^{2k-1}\phi(b)\right), \quad (b \to +\infty).$$

References

[1] B. Bagchi, *On Nyman, Beurling and Baez-Duarte's Hilbert space reformulation of the Riemann hypothesis*, Proc. Indian Acad. Sci. Math. 116(2)(2006), 137–146.

[2] R. Balasubramanian, J. B. Conrey and D. R. Heath-Brown, *Asymptotic mean square of the product of the Riemann zeta-function and a Dirichlet polynomial*, J. Reine Angew. Math. 357(1985), 161–181.

[3] S. Bettin and B. Conrey, *Period functions and cotangent sums*, Algebra & Number Theory 7(1)(2013), 215–242.

[4] T. Estermann, *On the representation of a number as the sum of two products*, Proc. London Math. Soc. 31(2)(1930), 123–133.

[5] M. Ishibashi, *The value of the Estermann zeta function at $s = 0$*, Acta Arith. 73(4)(1995), 357–361.

[6] H. Iwaniec, *On the mean values for Dirichlet's polynomials and the Riemann zeta function*, J. London Math. Soc. 22(2)(1980), 39–45.

[7] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, A.M.S Colloq. Publ. 53, A.M.S, 2004.

[8] M. Th. Rassias, *On a cotangent sum related to the zeros of the Estermann zeta function.*

[9] V. I. Vasyunin, *On a biorthogonal system associated with the Riemann hypothesis*, (in Russian) Algebra i Analiz 7(3)(1995), 118–135; english translation in St. Petersburg Math. J. 7(3)(1996), 405–419.

The density of twins of k-free numbers

Oscar Marmon
(joint work with Rainer Dietmann)

For $k \geq 2$, let $A_k(Z)$ be the number of positive integers $n \leq Z$ such that both n and $n+1$ are k-free. It has been known since the 1930:s that

$$A_k(Z) = c_k Z + O_{k,\varepsilon}\left(Z^{\frac{2}{k+1}+\varepsilon}\right) \tag{1}$$

for any $\varepsilon > 0$, where

$$c_k = \prod_p \left(1 - \frac{2}{p^k}\right).$$

In the case $k = 2$, Heath-Brown [2] has improved the exponent $2/3 + \varepsilon$ to $7/11 + \varepsilon$, using the so-called square sieve. Brandes [1] adapted this method to arbitrary k, obtaining the exponent $14/(7k+8) + \varepsilon$. In a recent preprint, Reuss [5] gives substantial improvements for small values of k, proving the asymptotic formula (1) with error term $O(Z^{\omega(k)+\varepsilon})$, where in particular $\omega(2) \approx 0.578$ and $\omega(3) \approx 0.391$. However, so far all results have involved exponents that approach the trivial exponent $2/k$ as $k \to \infty$. Our main result remedies this situation.

Theorem. We have

$$A_k(Z) = c_k Z + O_{k,\varepsilon}\left(Z^{\frac{14}{9k}+\varepsilon}\right)$$

for any $\varepsilon > 0$.

The main feature of the proof is a good upper bound for the density of solutions to the Diophantine equation $ax^k - by^k = 1$. More precisely, if $N(X,Y,Z)$ denotes the number of solutions $(a,b,x,y) \in \mathbb{N}^4$ satisfying $X < x \leq 2X$, $Y < y \leq 2Y$ and $Z < by^k \leq 2Z$, then we prove that $N(X,Y,Z) \ll_{k,\varepsilon} Z^{14/(9k)+\varepsilon}$ as soon as $XY \gg Z^{14/(9k)}$. For this, we use ideas from Heath-Brown's paper [4], where he introduced a bihomogeneous version of the approximate determinant method developed in [3].

References

[1] Julia Brandes. Twins of s-free numbers. Diploma Thesis, University of Stuttgart, arXiv:1307.2066, 2009.

[2] D. R. Heath-Brown. The square sieve and consecutive square-free numbers. *Math. Ann.*, 266(3):251–259, 1984.

[3] D. R. Heath-Brown. Sums and differences of three kth powers. *J. Number Theory*, 129(6):1579–1594, 2009.

[4] D. R. Heath-Brown. Square-free values of n^2+1. *Acta Arith.*, 155(1):1–13, 2012.

[5] Thomas Reuss. Pairs of k-free numbers, consecutive square-full numbers. arXiv:1212.3150, 2012.

On signs of Hecke eigenvalues

Kaisa Matomäki

Let f be a holomorphic Hecke cusp form of even weight, write $\lambda_f(n)$ for the corresponding Hecke eigenvalues, and write

$$\mathcal{N}_f^{\pm}(x) := |\{n \leq x \colon \lambda_f(n) \gtrless 0\}|.$$

Lau and Wu [1] have shown that $\mathcal{N}_f^{\pm}(x) \gg x$, but their proof does not yield for instance that $\mathcal{N}_f^{\pm}(2x) - \mathcal{N}_f^{\pm}(x) \gg x$. Halász's theorem on mean values of multiplicative functions together with some properties of the eigenvalues imply that one has even more, namely

Theorem 1. *There exists a positive constant $c = c(f)$ such that, for $\sigma \in \{+,-\}$, one has*

$$\mathcal{N}_f^{\sigma}(x) = (\tfrac{1}{2} + o(1)) \cdot |\{n \leq x \colon \lambda_f(n) \neq 0\}| = (c + o(1))x.$$

My main interest has been in studying sign changes in short intervals; in particular I have shown the following two theorems.

Theorem 2. *Let $\varepsilon > 0$ and $\sigma \in \{+,-\}$. Then*

$$\mathcal{N}_f^{\sigma}(x + x^{\varepsilon}) - \mathcal{N}_f^{\sigma}(x) \gg_{f,\varepsilon} \frac{x^{\varepsilon}}{\log^5 x}$$

for almost all $x \sim X$.

Theorem 3. *The number of sign changes in the sequence $(\lambda_f(n))_{n \leq x}$ is at least $cx/\log^2 x$ for some positive constant c.*

Before these results it was only known that the sequence $(\lambda_f(n))_{n \leq x}$ changes sign at least $cx^{1/2}$ times for some positive constant c, as a consequence of a short interval result of Lau and Wu [1].

In the proofs of Theorems 2 and 3 I show, for appropriate h and amount of $x \sim X$, incompatible upper and lower bounds for

$$\sum_{x \leq n \leq x+h} \lambda_f(n) \quad \text{and} \quad \sum_{x \leq n \leq x+h} |\lambda_f(n)|.$$

An upper bound for the first sum follows from the well-known analogue of additive divisor problem for cusp form coefficients and for the lower bound for the first sum we use some results from sieve theory.

Similar methods can be used to prove some related results for $\lambda_f(n^k)$ with $k \geq 2$ and for Dirichlet series coefficients of symmetric power L-functions.

I am currently interested in improving the lower bound in Theorem 3 further and in studying similar questions for more general multiplicative functions. In particular, after my talk at Oberwolfach, Brian Conrey and Maksym Radziwill pointed out that it might be possible to improve on Theorem 3 by introducing a mollifier, and I am currently investigating this possibility together with Radziwill.

References

[1] Y.-K. Lau and J. Wu. The number of Hecke eigenvalues of same signs. *Math. Z.*, 263(4):959–970, 2009.

Norm forms as products of linear polynomials

Lilian Matthiesen
(joint work with Tim Browning)

Let $K/\mathbb{Q}$ be a field extension of finite degree n and let $\{\omega_1, \dots, \omega_n\}$ denote a $\mathbf{Z}$-basis of $\mathfrak{o}_K$. Then the form

$$\mathbf{N}_K(x_1, \dots, x_n) = N_{K/\mathbb{Q}}(\omega_1 x_1 + \cdots + \omega_n x_n)$$

is called a norm form.

Let $P \in \mathbb{Q}[t]$ be a polynomial. It was conjectured by Colliot-Thélène that smooth and projective models for the affine variety $X \subset \mathbb{A}^{n+1}_{\mathbb{Q}}$ defined by

$$N_K(\mathbf{x}) = P(t)$$

have the property that the Brauer–Manin obstruction is the only obstruction to the Hasse principle and weak approximation. (This conjecture was in fact phrased for a general ground field in place of $\mathbb{Q}$.)

We establish the conjecture for arbitrary finite extensions $K/\mathbb{Q}$ and polynomials P that split into linear factors over $\mathbb{Q}$. Our proof uses the descent theory of Colliot-Thélène and Sansuc in order to turn the problem into one that is more tractable by analytic methods. For the analysis of the descent varieties we invoke methods from additive combinatorics, developed by Green and Tao, and an application of the Green–Tao–Ziegler inverse result for Gowers uniformity norms.

Small gaps between primes

James Maynard

We introduce work in progress on a refinement of the 'GPY method' for studying small gaps between primes. This refinement allows us to prove that

$$\liminf_n (p_{n+1}-p_n) \leq 700. \tag{1}$$

Moreover, under the Elliott-Halberstam conjecture, we can show

$$\liminf_n (p_{n+1}-p_n) \leq 12, \qquad \liminf_n (p_{n+2}-p_n) \leq 700. \tag{2}$$

This is the first such conditional result to show that $\liminf(p_{n+2}-p_n)<\infty$, and this is possible because our variation allows us to avoid some key limitations of the original GPY method.

The basic idea of the GPY sieve method is to compare the sums

$$S_1 = \log 3N \sum_{N\leq n\leq 2N} w_n, \tag{3}$$

$$S_2 = \sum_{N\leq n\leq 2N}\Big(\sum_{i=1}^k \Lambda(n+h_i)\Big) w_n, \tag{4}$$

for some weights $w_n \geq 0$ and for a fixed 'admissible' set $\mathcal{H}=\{h_1,\dots,h_k\}$. (We say $\{h_1,\dots,h_k\}$ is admissible if the polynomial $P(n)=\prod_{i=1}^k(n+h_i)$ has no fixed prime divisor.) If we can choose w_n such that $S_2 > mS_1 > 0$ for all large N, then it follows that $\liminf_n(p_{n+m}-p_n) \leq \sup_{i\neq j}(h_i-h_j)$.

The standard form of the GPY method takes the weights w_n to be approximately of the form

$$w_n \approx \Big(\sum_{d|\prod_{i=1}^k(n+h_i)} \mu(d)f(d)\Big)^2, \tag{5}$$

for a suitable smooth function $f:\mathbb{R}\rightarrow\mathbb{R}$.

The key idea in our method is to take instead

$$w_n \approx \Big(\sum_{d_i|n+h_i\forall i}\Big(\prod_{j=1}^k \mu(d_j)\Big) f(d_1,\dots,d_k)\Big)^2, \tag{6}$$

for a suitable smooth function $f:\mathbb{R}^k\rightarrow\mathbb{R}$. It is the extra flexibility gained by allowing our weights w_n to depend on the divisors of each factor $n+h_i$ individually which gives our improvement over the original GPY method.

To get asymptotic estimates for the sums S_1 and S_2, the GPY method relies on results on the distribution of primes in arithmetic progressions. Given $\theta>0$, we say the primes have 'level of distribution θ' if, for any $A>0$, we have

$$\sum_{q\leq x^\theta} \max_{(a,q)=1}\Big|\pi(x;q,a)-\frac{\pi(x)}{\phi(q)}\Big| \ll_A \frac{x}{(\log x)^A}. \tag{7}$$

The Bombieri-Vinogradov theorem shows that the primes have level of distribution θ for any $\theta < 1/2$, and the Elliot-Halberstam conjecture is the claim that this can be extended to any $\theta < 1$.

The original work of Goldston, Pintz and Yıldırım [1] on small gaps between primes showed that if (7) holds for some $\theta > 1/2$ then $\liminf(p_{n+1} - p_n) < \infty$. This just fails to show the existence of bounded gaps between primes unconditionally. The key breakthrough of Zhang's recent work was in showing a weakened form of (7) holds for some $\theta > 1/2$, which is enough to establish the existence of bounded gaps between primes.

If the primes have level of distribution $\theta > 0$, then we can choose our weights w_n in terms of θ and a suitable smooth function $F : \mathbb{R}^k \to \mathbb{R}$, and we can obtain asymptotic estimates for the sums S_1 and S_2 as $N \to \infty$. We find that this gives

$$\frac{S_2}{S_1} \sim \frac{\theta J_k(F)}{2 I_k(F)}, \tag{8}$$

where J_k and I_k are given by

$$I_k(F) = \int_0^1 \cdots \int_0^1 F(t_1, \dots, t_k)^2 dt_1 \dots dt_k,$$
$$J_k(F) = \sum_{m=1}^{k} \int_0^1 \cdots \int_0^1 \left(\int_0^1 F(t_1, \dots, t_k) dt_m \right)^2 dt_1 \dots dt_{m-1} dt_{m+1} \dots dt_k.$$

The only important restriction of F is that it has its support limited to the set $\mathcal{R}_k = \{(x_1, \dots, x_k) \in [0,1]^k : \sum_{i=1}^k x_i \le 1\}$.

By taking F to be a suitable symmetric polynomial on $\mathcal{R}_k$ (and zero elsewhere), we can calculate $J_k(F)$ and $I_k(F)$ exactly. In particular, we find by computation that we can choose F such that

$$\frac{J_{110}(F)}{I_{110}(F)} > 4.018. \tag{9}$$

By the Bombieri-Vinogradov theorem, we can take $\theta = 0.498$ unconditionally, and so with this choice of F we have $S_2 > S_1 > 0$ with $k = 110$. By choosng $\mathcal{H}$ suitably this gives $\liminf(p_{n+1} - p_n) \le 700$.

Under the Elliott-Halberstam conjecture we can take $\theta = 0.996$, and so we see that $S_2 > 2S_1 > 0$ with $k = 110$. This gives $\liminf(p_{n+2} - p_n) \le 700$.

Finally, we find that when $k = 5$ we can choose F suitably such that

$$\frac{J_5(F)}{I_5(F)} > 2.004. \tag{10}$$

Thus, we see that under the Elliott-Halberstam conjecture we have $S_2 > S_1 > 0$. If we take $\mathcal{H} = \{0, 2, 6, 8, 12\}$ (which is admissible), this gives $\liminf(p_{n+1} - p_n) \le 12$.

References

[1] Daniel A. Goldston, János Pintz, and Cem Y. Yıldırım. Primes in tuples. I. *Ann. of Math. (2)*, 170(2):819–862, 2009.

[2] Y. Zhang. Bounded gaps between primes. *Ann. of Math.(2), to appear.*

Counting rational points on intersection of two quadrics

Ritabrata Munshi

Let $Q_1(x_1, \dots, x_n)$ and $Q_2(x_1, \dots, x_n)$ be two quadratic forms in n variables with integral coefficients. One is interested in the asymptotic behaviour of the counting function

$$N(B) = \#\{\mathbf{m} \in \mathbb{Z}^n : \max_{1 \leq i \leq n} |m_i| \leq B, \; Q_1(\mathbf{m}) = Q_2(\mathbf{m}) = 0\}.$$

From the general result of Birch [1], it follows that an asymptotic of the Hardy-Littlewood type holds for $N(B)$ if the number of variables n is large enough. More precisely,

$$N(B) = \mathfrak{S} J_0 B^{n-4} + O\left(B^{n-4-\delta}\right)$$

for some $\delta > 0$ if $n \geq 13 + \Delta$, where Δ is the dimension of the singular locus, in the sense of Birch, i.e.

$$\Delta = \dim \left\{\mathbf{x} \in \mathbb{C}^n : \mathrm{rank}(M_1\mathbf{x}, M_2\mathbf{x}) \leq 1\right\}.$$

If we assume that the variety $V : \; Q_1 = Q_2 = 0$ is non-singular then $\Delta = 1$ or 2. In the generic case one expects $\Delta = 1$. In the rest of this note we assume that the variety V is smooth and $\Delta = 1$.

One seeks to reduce the required number of variables in Birch's result (at least) to $n \geq 9$. Indeed for $n \geq 9$ one knows that the local solutions exist for any finite prime from the work of Demyanov [8] (also see [2]). On the other hand from the work of Colliot-Thélène, Sansuc and Swinnerton-Dyer [6], [7], we know that the Hasse principle holds for $n \geq 9$. (This has been improved for non-singular intersections in a recent pre-print of Heath-Brown [9], where he shows that the Hasse principle holds for $n \geq 8$.)

Let W be a non-negative smooth function compactly supported in $\mathbb{R}^n$, satisfying $W^{(j)} \ll_j 1$, and such that $\mathbf{0} \notin \mathrm{Supp}(W)$. Then we prove that

$$\sum_{\substack{\mathbf{m}=(m_1,\dots,m_n)\in\mathbb{Z}^n \\ Q_1(\mathbf{m})=Q_2(\mathbf{m})=0}} \cdots \sum W\left(\frac{\mathbf{m}}{B}\right) = \mathfrak{S} J_0(W) B^{n-4} + O\left(B^{n-5+\varepsilon} + B^{3n/4-41/32+\varepsilon}\right),$$

where the singular integral $J_0(W)$ depends on W, and the implied constant depends on Q_i and ε. The error term is smaller than the main term if $n - 4 > 3n/4 - 41/32$, which holds if $n \geq 11$. Note that for $\Delta = 1$, Birch [1] required $n \geq 14$. A result of similar strength can be obtained for the counting function $N(B)$ (without smoothing).

In certain special cases one can prove stronger results. For example, in the case of pairs of diagonal quadratic forms, Cook [5] established the asymptotic for $N(B)$ if $n \geq 9$. Recently in two joint works with T.D. Browning [3], [4], we established an asymptotic for the counting functions when the pair of forms has a different special structure, namely

$$Q_1(\mathbf{x}) = q_1(x_1, \dots, x_{n-2}) - x_{n-1}^2 - x_n^2, \quad \text{and} \quad Q_2(\mathbf{x}) = q_2(x_1, \dots, x_{n-2}),$$

with q_1 and q_2 being quadratic forms (not necessarily diagonal). Such pairs of quadrics appear naturally in many other important counting problems, e.g. the Batyrev-Manin conjecture for Châtelet surfaces (see [3]). In [3] we treat the case where $n \geq 9$, and in [4] we further specialize the forms q_i and prove an asymptotic for $n = 8$.

We conclude this note by giving a brief sketch of the proof. The strategy builds on [3], where we used multiplicative characters to deal with the first equation and additive characters (the circle method) to detect the second equation. A vital 'trick' was to use the modulus of the multiplicative character to reduce the size of the modulus in the circle method. This idea can also be used while applying the circle method to detect both the equations. Say we use modulus $1 \leq q_1 \leq B$ to detect the first equation $Q_1(\mathbf{m}) = 0$, which has 'size' B^2. Then we split the second equation $Q_2(\mathbf{m}) = 0$ into a congruence $Q_2(\mathbf{m}) \equiv 0 \bmod q_1$ and an (integral) equation $Q_2(\mathbf{m})/q_1 = 0$. Now to detect the last equation by the circle method we need modulus of size $B/\sqrt{q_1}$. Hence the total modulus $q_1 q_2$ has size $B^{3/2}$, instead of B^2 which should be the size if one used the circle method independently for both the equations. Since the size of the modulus is much smaller than the square of the length of the variables m_i, we save by applying Poisson summation formula to each variable. This is already sufficient to give us an asymptotic for sufficiently many variables $n \geq 15$. But the method allows us to have a Kloosterman refinement in the first application of the circle method and a double Kloosterman refinement in the second application. This together with the subconvexity for the Dirichlet L-function reduces the number of required variables to $n \geq 11$.

References

[1] B.J. Birch, *Forms in many variables*, Proc. R. Soc. Lond. Ser. A **265** (1962), 245–263.

[2] B.J. Birch; D.J. Lewis and T.G. Murphy, *Simultaneous quadratic forms*, American J. Math. **84** (1962), 110–115.

[3] T.D. Browning and R. Munshi, *Rational points on singular intersections of quadrics*, Compositio Math. **149** (2013), 1457–1494.

[4] T.D. Browning and R. Munshi, *Pairs of diagonal quadratic forms and linear correlations among sums of two squares*, Forum Math., to appear.

[5] R.J. Cook, *Simultaneous quadratic equations*, J. Lond. Math. Soc. (2) **4**, (1971), 319–326.

[6] J.-L. Colliot-Thélène; J.-J. Sansuc and P. Swinnerton-Dyer, *Intersections of two quadrics and Châtelet surfaces*, I, J. Reine Angew. Math. **373** (1987), 37–107.

[7] J.-L. Colliot-Thélène; J.-J. Sansuc and P. Swinnerton-Dyer, *Intersections of two quadrics and Châtelet surfaces*, II, J. Reine Angew. Math. **374** (1987), 72–168.

[8] V.B. Demyanov, *Pairs of quadratic forms over a complete field with discrete norm with a finite field of residue classes*, Izv. Akad. Nauk SSSR. Ser. Mat. **20** (1956), 307–324.

[9] D.R. Heath-Brown, *Zeros of Pairs of Quadratic forms*, preprint available at arXiv:1304.3894.

Burgess bounds for short mixed character sums

Lillian Pierce
(joint work with Roger Heath-Brown)

Let $\chi(n)$ be a non-principal character of modulus q, and consider the character sum

$$S(N,H) = \sum_{N<n\leq N+H} \chi(n).$$

The Pólya-Vinogradov inequality provides the bound

$$|S(N,H)| \ll q^{1/2}\log q,$$

which is nontrivial only if the length H of the character sum is longer than $q^{1/2+\epsilon}$. In a classic series of papers (see for example [1]), Burgess introduced a method for bounding short character sums that results in the following well-known bound: for any $r \geq 1$ and q cube-free, or for any $r \leq 3$ and q a general modulus,

$$S(N,H) \ll H^{1-\frac{1}{r}} q^{\frac{r+1}{4r^2}+\epsilon},$$

for any $\epsilon > 0$, uniformly in N. This provides a nontrivial estimate for $S(N,H)$ as soon as $H > q^{1/4+\epsilon}$. Burgess bounds have found valuable applications in a range of settings, and it would be highly desirable to develop variations of the Burgess method for mixed character sums of the form

$$\sum_{N<n\leq N+H} e_q(f_1(n)\overline{f_2(n)})\chi(f_3(n)\overline{f_4(n)}),$$

for appropriate polynomials $f_1, \ldots, f_4$. However, it has proved difficult to handle sums involving χ evaluated at anything other than a linear function of n.

This talk presents new work in progress on sums of the form

$$\sum_{N<n\leq N+H} e(f(n))\chi(n),$$

where χ is a non-principal character to a prime modulus q and f is a real-valued polynomial of degree $d \geq 1$. The main novelty of our approach, which is inspired by Chang [2], is that we are able to apply recent work on Vinogradov's mean value theorem. Define $J_{r,d}(X)$ to be the number of solutions to the system of Diophantine equations given by

$$x_1^m + \cdots + x_r^m = x_{r+1}^m + \cdots + x_{2r}^m, \qquad 1 \leq m \leq d,$$

where $1 \leq x_1, \ldots, x_{2r} \leq X$, for some bounded range X. The main conjecture in the setting of Vinogradov's mean value theorem states that for every $r \geq 1, d \geq 1$ and $\epsilon > 0$,

$$J_{r,d}(X) \ll X^{\epsilon}(X^r + X^{2r-\frac{1}{2}d(d+1)}). \tag{1}$$

Conditional on this bound for $J_{r,d}(X)$, we prove that for all $r > \frac{1}{2}d(d+1)$ and $H < q^{\frac{1}{2}+\frac{1}{4(r-\frac{1}{2}d(d+1))}}$,

$$\sum_{N<n\leq N+H} e(f(n))\chi(n) \ll H^{1-\frac{1}{r}} q^{\frac{r+1-\frac{1}{2}d(d+1)}{4r(r-\frac{1}{2}d(d+1))}+\epsilon}.$$

For $d = 1, 2$, the bound (1) holds true trivially, for all $r \geq 1$ and thus our result is unconditional when f is of degree 1 or 2. For $d \geq 3$, due to the work of Wooley [4], the bound (1) is now known for $r \geq d^2 - 1$, and as a consequence our result is unconditional in this range as well. In the intermediate range $\frac{1}{2}d(d+1) < r < \frac{1}{4}(d^2+1)$ and $d \geq 3$, partial results may be derived from the work of Ford and Wooley [3].

References

[1] D. A. Burgess, *The distribution of quadratic residues and non-residues,* Mathematika **4** (1957) 106-112.

[2] M.-C. Chang, *An estimate of incomplete mixed character sums,* in "An Irregular Mind," Bolyai Soc. Math. Stud., **21** (2010) 243-250.

[3] K. B. Ford and T. D. Wooley, *On Vinogradov's mean value theorem: strongly diagonal behaviour via efficient congruencing,* (2013) preprint.

[4] T. Wooley *Vinogradov's mean value theorem via efficient congruencing II*, Duke Math. J. **162** (2013) 673-730.

On Polignac numbers and the difference of consecutive primes

Janos Pintz

The recent theorem of Zhang showed the existence of infinitely many bounded gaps between consecutive primes, namely, gaps not exceeding $7 \cdot 10^7$. This bound was reduced to approximately five thousand by the recent Polymath project of T. Tao.

Zhang's result is based on the following three main pillars. First we introduce a few definitions.

Definition. *A k-tuple $\mathcal{H} = \{h_i\}_{i=1}^k$ of distinct non-negative integers is called admissible if it does not cover all residue classes modulo any prime p.*

Definition. *A number ϑ is called a level of distribution of primes if for any* $A, \varepsilon > 0$

$$\sum_{q\leq X^{\vartheta-\varepsilon}} \max_{\substack{a \\ (a,q)=1}} \left| \sum_{\substack{p=a(q) \\ p\leq X}} \log p - \frac{X}{\varphi(q)} \right| \ll_{A,\varepsilon} \frac{X}{\log^A X}. \tag{1}$$

Bombieri and Vinogradov proved that $\vartheta = 1/2$ is a level of distribution of primes. Elliott and Halberstam (1966) conjectured that this is true for $\vartheta = 1$ too.

Definition. *Conjecture* EH(ϑ) *asserts that ϑ is a level of distribution of primes.*

Definition. *m is a Polignac number if $d_n = p_{n+1} - p_n = m$ infinitely often.*

Polignac's conjecture (1849). *Every positive integer is a Polignac number.*

The first pillar of Zhang's theorem is the result of Goldston, Yıldırım and the author ($d_n = p_{n+1} - p_n$, $\{p_i\}_{i=1}^{\infty} = \mathcal{P}$ the set of primes).

Theorem 1 (GPY, 2005/2009). *Suppose* $\mathrm{EH}(\vartheta)$ *with some* $\vartheta > \frac{1}{2}$. *Then we have for any admissible k-tuple* $\mathcal{H}$ *at least two primes in* $n + \mathcal{H}$ *for infinitely many values* n. *Consequently we have* $\liminf\limits_{n\to\infty} d_n \leq C(\vartheta)$ *and, equivalently, there is at least one Polignac number.*

The condition $\mathrm{EH}(\vartheta)$ can be weakened as shown in a joint work of Y. Motohashi and the author in 2006/2008 (A smoothed GPY sieve, *Bull. London Math. Soc.* **40** (2008), no. 2, 298–310, arXiv:math/0602599, Feb. 27, 2006). (Let $P^+(n)$ denote the largest prime factor of n.)

Theorem 2 (MP 2006/2008). *In Theorem 1 it is sufficient to assume* $\mathrm{EH}(\vartheta)$, *that is* (1), *for smooth moduli* $q \leq X^{\vartheta-\varepsilon}$ *for which* $P^+(q) \leq X^{\delta}$, *and for any* q *for residue classes* a *satisfying* $I(a) := \prod\limits_{i=1}^{k}(a + h_i) \equiv 0 \pmod q$ *if* $k \geq k_0(\delta)$.

Remark. *This result is attributed by Y. Zhang to himself and its proof appears in his manuscript (* Ann. Math.*, to appear).*

Theorem 3 (Zhang). *The condition of Theorem 2 is true for* $\vartheta = 1/2 + 1/584$ *and* $\delta = 1/292$. *Consequently we have* $\liminf\limits_{n\to\infty} d_n \leq 7 \cdot 10^7$, *and there is at least one Polignac number not exceeding* $7 \cdot 10^7$. *Further there are at least two primes in translates* $n + \mathcal{H}$ *of any admissible k-tuple* $\mathcal{H}$ *for infinitely many values of* n *in case of* $k > 3.5 \cdot 10^6$.

Using an argument of the author (Lemma 4 in his article in "An irregular mind. Szemerédi is 70", Springer, 2010, p. 537) together with a more general form of the arguments of Theorem 3 of Zhang and its improvement by Tao's project, the following strengthening of Theorem 3 can be shown. (Let $P^-(n)$ be the smallest prime factor of n.)

Theorem 4 (J. Pintz, arXiv:1305.6289). *Let* $k \geq 720$, $\mathcal{H}$ *an admissible k-tuple,* $h_i \ll \log N$, $N > N_0(k)$. *Then there are at least*

$$c_1(k, \mathcal{H}) \frac{N}{\log^k N}$$

numbers $n \in [N, 2N)$ *such that* $n + \mathcal{H}$ *contains at least two primes and almost primes in all other components satisfying* $P^-(n + h_i) > N^{c_2(k)}$ *for* $i = 1, 2, \ldots, k$.

Remark. *A similar version to the above-mentioned crucial Lemma 4 of the author appears in the book Opera de Cribo of Friedlander–Iwaniec published also in 2010.*

Whereas the original Theorem 3 of Zhang yields only one Polignac number, by the aid of Theorem 4 we can show

Theorem 5 (J. Pintz, arXiv:1305.6289). *There are infinitely many Polignac numbers. In fact, they have a positive lower density* $> 10^{-7}$.

Theorem 6 (J. Pintz, arXiv:1305.6289)**.** *There exists an ineffective C such that we have always at least one Polignac number between X and $X+C$ for any X. (All gaps between consecutive Polignac numbers are uniformly bounded.)*

Erdős proved in 1948 the inequality

$$\liminf_{n\to\infty} \frac{d_{n+1}}{d_n} \le 1-c_0 < 1+c_0 \le \limsup \frac{d_{n+1}}{d_n} \tag{2}$$

with a very small positive value c_0 and conjectured that the $\liminf = 0$ and the $\limsup = \infty$.

Theorem 7 (J. Pintz, arXiv:1305.6289)**.** $\liminf\limits_{n\to\infty} \dfrac{d_{n+1}}{d_n} = 0$*,* $\limsup \dfrac{d_{n+1}}{d_n} = \infty$*.*
Further, we have even

$$\liminf_{n\to\infty} \frac{d_{n+1}\log n}{d_n} < \infty, \qquad \limsup_{n\to\infty} \frac{d_{n+1}}{d_n \log n} > 0. \tag{3}$$

In general it is difficult to show anything for three consecutive differences. However, we can show

Theorem 8 (J. Pintz, arXiv:1305.6289)**.** $\limsup\limits_{n\to\infty} \dfrac{\min(d_{n-1}, d_{n+1})}{d_n(\log n)^c} = \infty$ *with* $c = 1/720$*.*

Since the Prime Number Theorem implies

$$\frac{1}{N}\sum_{n=1}^{N} \frac{d_n}{\log n} = 1, \tag{4}$$

it is interesting to investigate the normalized distribution of d_n, $d_n/\log n$. Erdős conjectured more than 50 years ago that the set of limit points,

$$J = \left\{ \frac{d_n}{\log n} \right\}' = [0,\infty], \tag{5}$$

but no finite limit point was known until 2005, when we showed $0 \in J$ with Goldston and Yıldırım. This was rather strange since Erdős (1955) and Ricci (1954) proved that J has positive Lebesgue measure. A partial answer to the conjecture of Erdős is

Theorem 9 (J. Pintz, arXiv:1305.6289)**.** *There is an (ineffective) constant c^* such that*

$$[0, c^*] \subset J. \tag{6}$$

The above result raises the question whether considering a finer distribution $d_n/f(n)$ with a monotonically increasing function $f(n) \le \log n$, $f(n) \to \infty$ the same phenomenon is still true. The answer is yes.

Theorem 10 (J. Pintz, arXiv:1305.6289)**.** *Let $f(n) \leq \log n$, $f(n) \to \infty$ be an increasing function,*

$$J_f = \left\{ \frac{d_n}{f(n)} \right\}' . \tag{7}$$

Then there is an (ineffective) constant c_f^* such that

$$[0, c_f^*] \subset J. \tag{8}$$

Zhang's theorem shows the existence of infinitely many generalized twin prime pairs with a difference at most $7 \cdot 10^7$, while the theorem of Green and Tao shows the existence of arbitrarily long (finite) arithmetic progressions in the sequence of primes. A common generalization of these two results is given below. (Let p' denote the prime following p.)

Theorem 11 (J. Pintz, arXiv:1305.6289)**.** *There exists an even $d \leq 5500$ with the following property. For any k there is a k-term arithmetic progression of primes such that $p' = p + d$ for all elements of the progression.*

The density of $\zeta(\frac{1}{2} + it)$ and other applications

Maksym Radziwill

We describe a general method to understand, unconditionally, the value distribution of long Dirichlet polynomials in the complex plane. There are two applications of the method, both on the assumption of the Riemann Hypothesis.

- First application: There exists a constant $C > 0$ such that the curve drawn by $t \mapsto \log \zeta(\frac{1}{2} + it)$ in $\mathbb{C}$ intersects every circle $\{z : |z - \alpha| = C\}$ of radius C, with $\alpha \in \mathbb{C}$. In fact we obtain the following quantitative statement: Given a rectangle $\mathcal{R}$ with both sides greater than C,
$$\text{meas}\big\{T \leq t \leq 2T : \log \zeta(\tfrac{1}{2} + it) \in \mathcal{R}\big\} \asymp \frac{T \text{meas}\{\mathcal{R}\}}{\log \log T}$$
provided that the vertices of $\mathcal{R}$ are $o(\sqrt{\log \log T})$.
- Second application: Let $X(T)$ be the number of sign changes of $S(T) := \frac{1}{\pi} \Im \log \zeta(\frac{1}{2} + it)$ in an interval of length T. Then,
$$X(T) \asymp \frac{T \log T}{\sqrt{\log \log T}}$$
This improves on earlier work of Selberg, where the lower bound was weaker by a factor of $(\log \log T)^{-A}$, with $A > 0$ a large constant, and the upper bound was weaker by a factor of $\log \log \log T$.

The method is inspired by a recent method to deal with moments of L-functions discovered in joint work of the author with Soundararajan, and independently by Harper (we refer the reader to the abstracts of Soundararajan and Harper's talks).

The distribution of nuclear numbers

Olivier Robert
(joint work with G. Tenenbaum and C. Stewart)

For each positive integer n, we denote by $k(n)$ its kernel (or radical), e.g. its largest squarefree divisor. The notion of kernel of an integer appears in various problems and conjectures, and in particular plays a central role in the *abc* conjecture, stated by Masser and Oesterlé in 1985.

Our aim is to present here recent results about the distribution function $N(x,y)$ counting the number of the integers less than x whose kernel does not exceed y.

This study motivates the terminology introduced in the title : we shall call *nuclear number* an integer with a small kernel, and more precisely y-nuclear to specify that the kernel does not exceed y.

1) The study of $N(x,y)$ is a joint work with G. Tenenbaum, see [1].

We give an asymptotic formula for $N(x,y)$ in the domain

$$H_\varepsilon := \{(x,y) \in \mathbb{R}\colon \exp\big((\log\log x)^\varepsilon \leq y \leq x\big)\}$$

as x tends to $+\infty$. The methods essentially uses the saddle-point method in two variables.

For large values of y, the result extends an explicit estimate obtained by Squalli in 1985 [3], where $N(x,y)/y$ is essentially a function of $\log(x/y)$ related to the distribution of $\log(n/k(n))$. With that respect, we also produce the exact domain of validity of this estimate.

For small values of y, the estimate gives the expected term in the saddle-point method, involving the saddle-point in two variables, the Dirichlet series associated to the problem of $N(x,y)$, and the Hessian. This part involves the saddle-point method in its direct version.

For intermediate values, we use the indirect saddle-point method, and we describe precisely the transition factor.

Finally, we produce a global result in the whole considered domain, and we explain how the general estimate, even in the non-explicit form yields local estimates : namely we may explicitely compare $N(2x,y)$ and $N(x,2y)$ to $N(x,y)$, which produces a non trivial intrinsic result.

It is also of interest to mention a weaker result, but in the global domain : by similar methods, we give an asymptotic formula for $\log\big(N(x,y)/y\big)$ as $x \to +\infty$, uniformly for $2 \leq y \leq x$.

However, it should be mentionned that except for small values of y, the asymptotic behaviour of $N(x,y)$ outside of the domain H_ε is still an open problem.

2) As an illustration of the methods and some of the results involving $N(x,y)$, we present a refinement of the *abc* conjecture. Our argument is based on the Borel-Cantelli theorem, and only uses the following heuristic : we assume that for

a, b coprime, the kernels $k(a)$, $k(b)$ and $k(a+b)$ are independent random variables. We then introduce the estimates for $N(x, y)$ by deriving from our assumption that $k(a+b)$ behaves like the kernel of a generic integers of size $a+b$. The classical *abc* conjecture involves a term k^ε where $k = k(ab(a+b))$. Our refinement of this conjecture replaces the term k^ε by a function $F(k)$ for which essentially ε is replaced by $1/\sqrt{(\log k)(\log\log k)}$.

This last part is a joint works with C. Stewart and G. Tenenbaum, see [2].

References

[1] O. Robert & G. Tenenbaum, "Sur la répartition du noyau d'un entier", to appear in Indag. Math.

[2] O. Robert, C. L. Stewart & G. Tenenbaum, "A refinement of the *abc* conjecture", preprint

[3] H. Squalli, "Sur la répartition du noyau d'un entier", PHD thesis, University of Nancy I, defended on November 18th 1985

Connections between analytic number theory and the arithmetic of polynomials over function fields

Zeev Rudnick

The polynomial ring $\mathbb{F}_q[t]$ over a finite field $\mathbb{F}_q$ with q elements shares several properties with the ring of integers $\mathbb{Z}$, for instance a qualitative aspect is that it has unique factorization into irreducibles. A quantitative aspect is an analogue of the Prime Number Theorem (PNT), namely the Prime Polynomial Theorem. Recall that the PNT states that the number $\pi(x)$ of primes $p \leq x$ is asymptotically equal to $\mathrm{Li}(x) := \int_2^x dt/\log t \sim x/\log x$, and the Riemann Hypothesis is equivalent to the assertion that the remainder term $\pi(x) - \mathrm{Li}(x)$ is smaller than $x^{1/2+o(1)}$. The Prime Polynomial Theorem asserts that the number of monic irreducible polynomials of degree n is $q^n/n + O(q^{n/2}/n)$. This corresponds to the PNT if we map $x \leftrightarrow q^n$, recalling that x is the number of integers up to x and q^n is the number of monic polynomials of degree n.

Our lecture concerns further quantitative analogues, such as:

1. An old conjecture of Chowla on the autocorrelation of the Möbius function has attracted a lot of attention recently [10]. A simple case (which is considered completely out of reach) is the statement that $\mu(n)$ and $\mu(n+1)$ are uncorrelated, that is

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n\leq N} \mu(n)\mu(n+1) = 0.$$

In a recent paper with Dan Carmon [2], we prove a function field version of Chowla's conjecture in the limit of a large finite field: Fix $r > 1$, $n > 1$. Then for any choice of distinct polynomials $\alpha_1, \ldots, \alpha_r \in \mathbb{F}_q[t]$ (q odd), with $\max \deg \alpha_j < n$, and $\epsilon_i \in \{1, 2\}$, not all even

$$\lim_{q\to\infty} \frac{1}{q^n} \sum_{F\in\mathcal{M}_n} \mu(F+\alpha_1)^{\epsilon_1} \ldots \mu(F+\alpha_r)^{\epsilon_r} = 0,$$

where we denote by $\mathcal{M}_n$ the set of monic polynomials in $\mathbb{F}_q[t]$ of degree n (note that $\#\mathcal{M}_n = q^n$). The rate of convergence is uniform in $\alpha_1, \dots, \alpha_r$.

2. Together with Julio Andrade and Lior Bary Soroker [1], we study a function-field analogue of a classical problem in analytic number theory, currently wide open, concerning the auto-correlations of divisor functions. Let $d_r(n)$ be the number of representations of n as a product of r positive integers ($d_2 = d$ is the standard divisor function). Several authors have studied the "additive divisor problem", which is to get bounds, or asymptotics, for the sum (where $h \neq 0$ is fixed for this discussion)

$$D_r(X; h) := \sum_{n \leq X} d_r(n) d_r(n+h).$$

This is of importance in several problems of analytic number theory, in particular in relation to computing the moments of the Riemann ζ-function on the critical line, see [3].

The case $r = 2$, which is the only one solved so far, has a long history: Ingham [6] computed the leading term, and Estermann [4] gave an asymptotic expansion

$$D_2(X; h) \sim X P_2(\log X; h) + O(X^{11/12} (\log X)^3) \ , \tag{1}$$

where

$$P_2(u; h) = \frac{1}{\zeta(2)} \sigma_{-1}(h) u^2 + a_1(h) u + a_2(h) \ ,$$

$\sigma_{-1}(h) = \sum_{d|h} d^{-1}$, and $a_1(h)$, $a_2(h)$ are very complicated coefficients.

For $r \geq 3$ it is conjectured that

$$D_r(X; h) \sim X P_{2(r-1)}(\log X; h) \ , \tag{2}$$

where $P_{2(r-1)}(u; h)$ is a polynomial in u of degree $2(r-1)$, whose coefficients depend on h (and r). However to date one is very far from being able to even get good upper bounds for individual h. Moreover, even a conjectural description of the polynomials $P_{2(r-1)}(u; h)$ is difficult to obtain, see [7, 3].

We study the mean values of $d_r(f) d_r(f+h)$ over $\mathcal{M}_n$ in the limit $q \to \infty$, showing that for $0 \neq h \in \mathbb{F}_q[t]$, and $n > \deg h$,

$$\frac{1}{q^n} \sum_{f \in \mathcal{M}_n} d_r(f) d_r(f+h) = \binom{n+r-1}{r-1}^2 + O(q^{-1/2}).$$

Note that $\binom{n+r-1}{r-1}^2$ is a polynomial in n of degree $2(r-1)$ with leading coefficient $1/[(r-1)!]^2$. For $r = 2$ we obtain agreement with Estermann's result (1) under the correspondence $\log X \leftrightarrow n$, in the sense that we also get a quadratic polynomial $\binom{n+1}{1}^2 = n^2 + 2n + 1$, whose leading coefficient agrees with the limit as $q \to \infty$ of the function field interpretation of the leading coefficient $\sigma_{-1}(h)/\zeta(2)$ of (1). Likewise, at least the leading coefficient of the polynomial $P_{2(r-1)}(u, h)$ can be interpreted in a way that allows to compare with the polynomial $\binom{n+r-1}{r-1}^2$ and thus confirm the conjecture (2).

3. Together with J. Keating, we established [8] a function field analogue of a conjecture of Goldston and Montgomery [5] on the variance of the number of prime polynomials in short intervals. The conjecture, as refined by Montgomery and Soundararajan [9], is that the variance of primes in short intervals (in the range $X^\epsilon < H < X^{1-\epsilon}$) is

$$\frac{1}{X}\int_1^X \left| \sum_{n\in[x,x+H]} \Lambda(m) - H \right|^2 dx \sim H(\log X - \log H - C_0) \tag{3}$$

where $C_0 = \gamma + \log 2$, with γ being Euler's constant. Assuming the Riemann Hypothesis and the (”strong”) pair correlation conjecture, Goldston and Montgomery proved (3) without the secondary term $-C_0H$, that is with the RHS of (3) replaced by $H(\log X - \log H)$.

We prove a function field analogue [8]: Let $||f|| := q^{\deg f}$ be the norm of a polynomial. The analogue of a short interval around a polynomial $A \in \mathbb{F}_q[t]$ of degree n, is the set of polynomials $\{f : ||f - A|| \le q^h\}$, where $0 \le h < n$, whose cardinality is $H := q^{h+1}$. We show that for $h < n - 3$,

$$\frac{1}{q^n}\sum_{A\in\mathcal{M}_n} \left| \sum_{||f-A||\le q^h} \Lambda(f) - q^{h+1} \right|^2 \sim H(n-h-2) + o(1)) \tag{4}$$

as $q \to \infty$.

We may compare (4) with (3) if we make the dictionary

$$X \leftrightarrow q^n, \quad H \leftrightarrow q^{h+1}, \quad \log X \leftrightarrow n,$$

the conclusion being that (4) is precisely the analogue of the conditional result of Goldston and Montgomery.

References

[1] J. C. Andrade, L. Bary Soroker and and Z. Rudnick, *The additive divisor problem over the rational function field*, in preparation.

[2] D. Carmon and Z. Rudnick *The autocorrelation of the Möbius function and Chowla's conjecture for the rational function field*, The Quarterly Journal of Mathematics 2013; doi: 10.1093/qmath/has047

[3] J. B. Conrey and S. M. Gonek, *High Moments of the Riemann Zeta-Function*, Duke Math. J. 107, 577–604 (2001).

[4] T. Estermann, *Über die Darstellungen einer Zahl als Differenz von zwei Produkten.* Journal für die reine und angewandte Mathematik 164 (1931): 173–182.

[5] D. A. Goldston, and H. L. Montgomery, *Pair correlation of zeros and primes in short intervals.* Analytic number theory and Diophantine problems (Stillwater, OK, 1984), 183–203, Progr. Math., 70, Birkhäuser Boston, Boston, MA, 1987.

[6] A. E. Ingham, *Mean-value theorems in the theory of the Riemann Zeta-function*, Proc. London Math. Soc. (2) 27 (1928), 273–300.

[7] A. Ivić, *On the ternary additive divisor problem and the sixth moment of the zeta-function*, Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995), 205–243, London Math. Soc. Lecture Note Ser., 237, Cambridge Univ. Press, Cambridge, 1997.

[8] J. P. Keating and Z. Rudnick. *The variance of the number of prime polynomials in short intervals and in residue classes.* International Mathematics Research Notices 2012; doi: 10.1093/imrn/rns220.

[9] H.L. Montgomery and K. Soundararajan, *Beyond pair correlation.* Paul Erdos and his mathematics, I (Budapest, 1999), 507–514, Bolyai Soc. Math. Stud., 11, János Bolyai Math. Soc., Budapest, 2002.

[10] P. Sarnak, *Three lectures on Möbius randomness*, (2011) available at http://www.math.ias.edu/files/wam/2011/PSMobius.pdf

Integral points of cubic hypersurfaces

Per Salberger

The following conjecture is due to Heath-Brown [1].

Conjecture. *Let $f(x_1,...,x_n) \in \mathbb{Z}[x_1,...,x_n]$, $n \geq 3$ be a polynomial such that its homogeneous part F of maximal degree d is absolutely irreducible over $\mathbb{Q}$. Let $n(f;B)$ be the number of integral n-tuples $x = (x_1,...,x_n) \in [-B,B]^n$ with $f(x) = 0$. Suppose that $d \geq 2$. Then, $n(f;B) = O_{d,n,\varepsilon}(B^{n-2+\varepsilon})$.*

One needs some hypothesis on F as $n(f;B) >> B^{n-2+1/d}$ for $f(x_1,...,x_n) = x_1 - x_n^d$. The conjecture is then in some sense best possible as f may be of the form $x_{n-1}g + x_n h$ and $n(f;B) \gg B^{n-2}$ for such f.

The conjecture was proved for $d \geq 6$ in [1] and for $d \geq 4$ in [5]. One reduces in both papers to the case $n = 3$ by a hyperplane section argument. One may then apply Heath-Brown's p-adic determinant method [3] for $d \geq 6$. The case when $d = 4, 5$ is harder and requires the global determinant method in [5]. For $d = 2$, the conjecture follows easily from [1, lemma 13]. It thus only remains to prove the conjecture for cubic polynomials.

If n is large and the leading form F is not too singular, then it is better to apply versions of the circle method. It was shown by Heath-Brown [2] that $n(f;B) = O_F(B^{n-3+15/(n+5)})$ and $n(f;B) = O_{d,n}(B^{n-3+15/(n+5)} + B^{n-2})$ provided that F is nonsingular of degree $d \geq 3$. I then obtained the sharper bounds $O_F(B^{n-3+9/(n+2}(\log B)^{n/2})$ and $O_{d,n}(B^{n-3+9/(n+2}(\log B)^{n/2} + B^{n-2})$ for such f in an unpublished preprint [4] from 2006. This proves the conjecture for $n \geq 7$, thereby saving three variables for polynomials with leading non-singular form.

I have recently obtained an even sharper bound.

Theorem. *Let $f(x_1,...,x_n) \in \mathbb{Z}[x_1,...,x_n]$, $n \geq 5$ be a polynomial of degree $d \geq 3$ such that $F = f_d$ defines a non-singular hypersurface in $\mathbb{P}^{n-1}$. Then,*

$$n(f;B) = O_{F,\varepsilon}(B^{n-3+9/(n+3)+\varepsilon})$$

and

$$n(f;B) = O_{d,n,\varepsilon}(B^{n-3+9/(n+3)+\varepsilon} + B^{n-2}).$$

In particular $n(f;B) = O_{d,n,\varepsilon}(B^{n-2+\varepsilon})$ if $n \geq 6$.

To prove this, I use Heath-Brown's q-analog of van der Corput's AB-process in [2]. This discrete circle method is used to give uniform upper estimates for the number of congruences $f = 0 \pmod q$ in boxes $[-B, B]^n$ for two carefully chosen primes p and q. One needs thereby a precise knowledge of the distribution of $\mathbb{F}_q$-points in boxes on the complete intersections defined by $f = 0 \pmod q$ and $f^h = 0 \pmod q)$) , where

$$f^h(x_1, ..., x_n) = (f(x_1 + ph_1, ..., x_n + ph_n) - f(x_1, ..., x_n))/p$$

for n-tuples $h = (h_1, ..., h_n) \in \mathbb{Z}^n$ with $|h_i| \ll B/p$.

The main new ingredient in the proof of the theorem (compared to [4]) is that we average over all q in a dyadic interval $[Q, 2Q]$ with Q of order $B^{2n/(n+3)}$. The prime p is fixed and of order $B^{n/(n+3)}$.

Corollary. *Let $f(x_1, ..., x_n) \in \mathbb{Z}[x_1, ..., x_n]$, $n \geq 6$ be a polynomial of degree $d \geq 3$ such that $F = f_d$ defines a hypersurface in $\mathbf{P}^{n-1}$ with singular locus of codimension at least 5. Then $n(f; B) = O_{d,n,\varepsilon}(B^{n-2+\varepsilon})$.*

This follows from the theorem by means of a hyperplane section argument.

References

[1] T.D.Browning, R.Heath-Brown and P. Salberger: Counting rational points on algebraic varieties, Duke Mathematical Journal 132(2006), 545 – 578.

[2] D.R.Heath-Brown: The density of rational points on non-singular hypersurfaces. Proc. Ind. Acad. Sci. 104(1994), 13-29.

[3] D.R.Heath-Brown: The density of rational points on curves and surfaces. Ann. of Math. 155(2002), 553-595.

[4] P.Salberger: Integral points on hypersurfaces of degree at least three, unpublished preprint from 2006.

[5] P.Salberger: Counting rational points on projective varieties, submitted.

Unlikely intersections

Igor E. Shparlinski

(joint work with J. Bourgain, M.-C. Chang, J. Cilleruelo, D. Gómez-Pérez, M. Z. Garaev J. Hernández, S. V. Konyagin. A. Ostafe, A. Zumalacárregui)

An amazingly large number of problems in number theory and its application to cryptography and computer science can be formulated as the following generic question: *given two sets $\mathcal{A}$ and $\mathcal{B}$ defined by two seemingly unrelated conditions, prove that the intersection $\mathcal{A} \cap \mathcal{B}$ is sparse*. The term "unlikely intersections" for problems of this type has been introduced by Bombieri, Masser and Zannier [3], see also [4]. The most commonly occurring in number theory and its application are the following examples of the sets $\mathcal{A}$ and $\mathcal{B}$:

- an interval of h consecutive integers $\mathcal{I} = \{u + i \ : \ i = 1, \dots, h\}$,
- a multiplicative subgroup $\mathcal{G}$,
- an algebraic variety $\mathcal{V}$.

Higher dimensional analogues of these sets, and also value sets $f(\mathcal{S})$ of a given polynomial f on one the above sets $\mathcal{S}$ have also been considered. Here we are mostly interested in the case when these sets are taken in a prime finite field $\mathbb{F}_p$.

Typically, for any "reasonable" sets $\mathcal{A}, \mathcal{B} \subseteq \mathbb{F}_p$, *the Weil bound* implies

$$\#(\mathcal{A} \cap \mathcal{B}) = \frac{\#\mathcal{A}\#\mathcal{B}}{p} + O(p^{1/2+o(1)})$$

which provides a nontrivial information on $\#(\mathcal{A} \cap \mathcal{B})$ if $\#\mathcal{A}\#\mathcal{B} \geq p^{3/2+\varepsilon}$ for some fixed $\varepsilon > 0$. Here we are mostly interested in much thinner sets, in particular when $\#\mathcal{A}\#\mathcal{B} < p$, so one expects $\mathcal{A} \cap \mathcal{B} = \emptyset$.

So far, most of the attention has been directed to estimating $\#(\mathcal{I} \cap \mathcal{G})$ for an interval $\mathcal{I}$ and a multiplicative subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ and also intersections of several closely related sets, see [2, 6, 7, 8, 10, 11, 16, 23, 26] and references therein. Their applications include a series of results on *fixed points of the discrete logarithm* [10, 11], non-vanishing *Fermat quotients* [5, 12, 25, 29, 30], *pseudopowers* [9] and the distribution of *digits in g-ary expansions* of rational fractions [31]. Note that recent results of Shkredov [26, 27, 28] immediately lead to improvements of the estimates from [5, 9, 12, 25, 29, 30] and probably have many other applications (the results of [31] are already based on [26]). The size of the intersection $\#(f(\mathcal{I}) \cap \mathcal{G})$ for $f \in \mathbb{F}_p[X]$ with $\deg f \geq 2$, an interval $\mathcal{I}$ and a multiplicative subgroup $\mathcal{G} \subseteq \mathbb{F}_p^*$ has been considered in [21].

In a series of works [14, 18, 19, 22] various bounds on the size of the intersection $\#(f(\mathcal{I}) \cap g(\mathcal{J}))$ are given for two polynomials $f, g \in \mathbb{F}_p[X]$ and intervals $\mathcal{I}, \mathcal{J}$. Even the case of $\deg g$ is already nontrivial and has numerous applications, for example, to the *diameters of trajectories* of polynomial dynamical systems and to the distribution of *visible points* (sometimes also called *primitive points*) on curves. The case of $\deg f = 3$, $\deg g = 2$ has interesting applications in studying the *distribution of isomorphic elliptic curves* in some families over $\mathbb{F}_p$.

Studying intersections of zero sets of varieties with Cartesian products of intervals and multiplicative subgroups is also a very challenging and important direction, see [13, 15, 17, 18, 19], for some results and further references.

Question 1. *Estimate the size of the intersection of polynomials images of two subgroups $\#(f(\mathcal{G}) \cap g(\mathcal{H}))$ for $f, g \in \mathbb{F}_p[X]$ and $\mathcal{G}, \mathcal{H} \subseteq \mathbb{F}_p^*$.*

Question 1 is still *open* even in the simplest case $g(X) = X$, $\mathcal{G} = \mathcal{H}$ (for $f(X) = aX + b$, $g(X) = X$, $\mathcal{G} = \mathcal{H}$, see [26]).

An interesting feature of this area is the methods it uses. It certainly relies on well expected methods like additive combinatorics in finite fields bounds of sums of additive and multiplicative characters. However, it also employs such "unlikely" tools as *the Bombieri-Pila bound* [1], the version of Wooley [32, 33] of *Vinogradov's Mean Value Theorem* and effective *Hilbert's Nullstellensatz* [20, 24].

These questions are also of interest in arbitrary finite fields $\mathbb{F}_q$ and infinite fields (such as $\mathbb{F}_q[X]$, $\mathbb{R}$ and $\mathbb{C}$), in residue rings $\mathbb{Z}/m\mathbb{Z}$ and in matrix rings. However many of the above tools do not have adequate analogues in these settings. For example, it is important to establish a function field analogue of the Bombieri-Pila bound [1, Theorem 4] for the number of integral points on plane algebraic curves.

Question 2. *Let $K = \mathbb{F}_q(T)$ and let $F(X,Y) \in K[X,Y]$ be absolutely irreducible with* $\deg F = d$. *Obtain an upper bound on the number of solutions to the equations $F(x,y) = 0$ in polynomials $x(T), y(T) \in \mathbb{F}_q[T]$ of degree at most n (as $n \to \infty$).*

References

[1] E. Bombieri and J. Pila, 'The number of integral points on arcs and ovals', *Duke Math. J.*, **59** (1989), 337–357.

[2] J. Bourgain, 'On the distribution of the residues of small multiplicative subgroups of $\mathbb{F}_p$', *Israel J. Math.*, **172** (2009), 61–74.

[3] E. Bombieri, D. Masser and U. Zannier. 'On unlikely intersections of complex varieties with tori', *Acta Arith.*, **133** (2008), 309-323.

[4] E. Bombieri, D. Masser and U. Zannier. *Some problems of unlikely intersections in arithmetic and geometry*, Princeton Univ. Press, Princeton, NJ, 2012.

[5] J. Bourgain, K. Ford, S. V. Konyagin and I. E. Shparlinski, 'On the divisibility of Fermat quotients', *Michigan Math. J.*, **59** (2010), 313–328.

[6] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, 'On the hidden shifted power problem', *SIAM J. Comp.*, **41** (2012), 1524–1557.

[7] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, 'On congruences with products of variables from short intervals and applications', *Proc. Steklov Math. Inst.*, **280** (2013), 67–96.

[8] J. Bourgain, M. Z. Garaev, S. V. Konyagin and I. E. Shparlinski, 'Multiplicative congruences with variables from short intervals', *J. d'Analyse Math.*, (to appear).

[9] J. Bourgain, S. Konyagin, C. Pomerance and I. E. Shparlinski, 'On the smallest pseudopower', *Acta Arith.*, **140** (2009), 43–55.

[10] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Product sets of rationals, multiplicative translates of subgroups in residue rings and fixed points of the discrete logarithm', *Intern. Math. Res. Notices*, **2008** (2008), Article rnn090, 1–29. (Corrigenda: *Intern. Math. Res. Notices*, **2009** (2009), 3146–3147).

[11] J. Bourgain, S. V. Konyagin and I. E. Shparlinski, 'Distribution of elements of cosets of small subgroups and applications', *Intern. Math. Res. Notices*, **2012** (2012), Article rnn097, 1968–2009.

[12] M.-C. Chang, 'Short character sums with Fermat quotients', *Acta Arith.*, **152** (2012), 23–38.

[13] M.-C. Chang, 'Elements of large order in prime finite fields', *Bull. Aust. Math. Soc.*, **88** (2013), 169–176.

[14] M.-C. Chang, J. Cilleruelo, M. Z. Garaev, J. Hernández, I. E. Shparlinski and A. Zumalacárregui, 'Points on curves in small boxes and applications', *Preprint*, (available from `http://arxiv.org/abs/1111.1543`).

[15] M.-C. Chang, B. Kerr, I. E. Shparlinski and U. Zannier, 'Elements of large order on varieties over prime finite fields', *Preprint*, 2013.

[16] J. Cilleruelo and M. Z. Garaev, 'Concentration of points on two and three dimensional modular hyperbolas and applications', *Geom. and Func. Anal.*, **21** (2011), 892–904.

[17] J. Cilleruelo, M. Z. Garaev, A. Ostafe and I. E. Shparlinski, 'On the concentration of points of polynomial maps and applications', *Math. Zeit.*, **272** (2012), 825–837.

[18] J. Cilleruelo and I. E. Shparlinski, 'Concentration of points on curves in finite fields', *Monatsh. Math.*, **171** (2013), 315–327.

[19] J. Cilleruelo, I. E. Shparlinski and A. Zumalacárregui, 'Isomorphism classes of elliptic curves over a finite field in some thin families', *Math. Res. Letters*, **19** (2012), 335–343.

[20] C. D'Andrea, T. Krick and M. Sombra, 'Heights of varieties in multiprojective spaces and arithmetic Nullstellensätze', *Annales Sci. de l'ENS* (to appear).

[21] D. Gómez-Pérez and I. E. Shparlinski, 'Subgroups generated by polynomials in finite fields', *Preprint*, 2013, 1-11.

[22] B. Kerr, 'Solutions to polynomial congruences in well shaped sets', *Bull. Aust. Math. Soc.*, (to appear).

[23] S. V. Konyagin and I. E. Shparlinski, 'On the consecutive powers of a primitive root: Gaps and exponential sums', *Mathematika*, **58** (2012), 11–20.

[24] T. Krick, L. M. Pardo, and M. Sombra, 'Sharp estimates for the arithmetic Nullstellensatz', *Duke Math. J.*, **109** (2001), 521–598.

[25] A. Ostafe and I. E. Shparlinski, 'Pseudorandomness and dynamics of Fermat quotients', *SIAM J. Discr. Math.*, **25** (2011), 50–71.

[26] I. D. Shkredov, 'Some new inequalities in additive combinatorics', *Preprint*, 2012 (available from `http://arxiv.org/abs/1208.2344`).

[27] I. D. Shkredov, 'On Heilbronn's exponential sum', *Quart. J. Math.*, (to appear).

[28] I. D. Shkredov, 'New bounds for Heilbronn's exponential sum', *Preprint*, 2013 (available from `http://arxiv.org/abs/1302.3839`).

[29] I. E. Shparlinski, 'On the value set of Fermat quotients', *Proc. Amer. Math. Soc.*, **140** (2012), 1199–1206.

[30] I. E. Shparlinski, 'On vanishing Fermat quotients and a bound of the Ihara sum', *Kodai Math. J.*, **32** (2009), 172–177.

[31] I. E. Shparlinski and W. Steiner, 'On digit patterns in expansions of rational numbers with prime denominator', *Quart. J. Math.*, (to appear).

[32] T. D. Wooley, 'Vinogradov's mean value theorem via efficient congruencing', *Ann. Math.*, **175** (2012), 1575–1627.

[33] T. D. Wooley, 'Vinogradov's mean value theorem via efficient congruencing, II', *Duke Math. J.*, **162** (2013), 673–730.

Moments of zeta and L-functions

Kannan Soundararajan

A classical problem in number theory asks for an understanding of the moments, $\int_0^T |\zeta(1/2+it)|^{2k}dt$, of the Riemann zeta-function, where k is any real positive number. Asymptotics are known here only when $k=1$ and $k=2$, and until the work of Keating and Snaith in 1998 it was difficult even to conjecture an answer. With the work of Keating and Snaith [8], and refinements by Conrey, Farmer, Keating, Rubinstein and Snaith [3], there are now well developed conjectures for what the right asymptotics should be. Furthermore there are important analogs of this conjecture for central values of L-functions in many families. The last ten years have seen a lot of progress on these classical questions, and in my talk I surveyed some of these recent results. The progress has been in three directions: getting asymptotics for small moments in families of L-functions, general techniques to produce lower bounds in many families, and general upper bounds (conditional on the Riemann hypothesis) for many families.

Regarding asymptotics for moments, in work with Conrey and Iwaniec, I [4] showed that the sixth moment of all Dirichlet L-functions with conductor up to Q (with a mild averaging in t-aspect) may be computed. This result is in accordance with the conjectures of Keating and Snaith for the sixth moment of $\zeta(s)$: in particular, the constant 42 in the leading order asymptotics was observed. Recently, Chandee and Li [2] have carried out an analogous calculation for the eighth moment of Dirichlet L-functions (now assuming GRH) and confirmed the conjectured constant of 24024 here. In work with Matt Young, I [13] give another result of this flavor, computing the second moment of quadratic twists of a modular form on GRH; it is a tantalizing open problem to achieve this unconditionally.

Now we turn to the problem of obtaining lower bounds for moments. For the Riemann zeta-function this is classical, going back to Titchmarsh, Ramachandra and Heath-Brown. More recently Rudnick and I [11] developed a method that gave lower bounds of the right order of magnitude for any family of L-functions where a little more than the first moment can be evaluated. Our method worked for all rational k, and the bounds depended on the height of the rational k. With Maksym Radziwill, I [9] recently extended this method so as to obtain bounds that vary continuously with k, and in particular obtaining lower bounds for irrational k as well. Even for $\zeta(s)$, these continuous lower bounds are new. Our understanding of lower bounds may be summarized as follows: Whenever some moment of L-functions in a family is known (with a little room to spare), one may obtain the correct lower bounds for all larger moments. This leaves open only the problem of obtaining lower bounds for small moments, and this problem is of interest as it is related to the problem of non-vanishing of L-functions. In some special cases, the problem of small moments has also been handled satisfactorily; for example, in work of Chandee and Li [2].

Finally, we consider the problem of obtaining upper bounds for moments. Some years back, I [12] developed a method that gave, on GRH, an upper bound for moments in families of L-functions that was sharp except for a factor of $(\log)^{\epsilon}$. Recent beautiful work by Harper [6] has refined this, and now one has sharp upper bounds for moments of L-functions conditional on GRH. Independently of Harper, Radziwill and I [10] had been developing a closely related technique which showed that whenever some moment in a family of L-functions was known (with a little to spare) then one obtains upper bounds of the correct order of magnitude for all smaller moments. Already for $\zeta(s)$ this is new, and gives unconditional upper bounds for all moments below the fourth of the Riemann zeta-function; previously this was known on RH due to Heath-Brown [7]. Furthermore, our work gives upper bounds of the right order of magnitude for moments (below the first) of quadratic twists of a modular form (or elliptic curve). This provides some new information about the size of Shafarevich-Tate groups of quadratic twists of an elliptic curve, confirming the upper bounds in some conjectures of Delaunay [5].

References

[1] V. Chandee and X. Li. Lower bounds for small fractional moments of Dirichlet L-functions. To appear in IMRN.

[2] V. Chandee and X. Li. The eighth moment of Dirichlet L-functions. Preprint.

[3] J.B. Conrey, D.W. Farmer, J.P. Keating, M.O. Rubinstein, and N.C. Snaith.

[4] J.B. Conrey, H. Iwaniec, and K. Soundararajan. The sixth power moment of Dirichlet L-functions. *GAFA* 22 (2012) 1257–1288.

[5] C. Delaunay. Moments of the orders of Tate-Shafarevich groups. *Int. J. Number Theory* (2005) 243–264.

[6] A. Harper. Sharp conditional bounds for moments of the Riemann zeta function. Preprint.

[7] D.R. Heath-Brown. Fractional moments of the Riemann zeta function. *J. London Math. Soc.* 24 (1981) 65–78.

[8] J.P. Keating and N.C. Snaith. Random matrix theory and $\zeta(1/2+it)$. *Comm. Math. Phys.* 214 (2000) 57–89.

[9] M. Radziwill and K. Soundararajan. Continuous lower bounds for moments of zeta and L-functions. *Mathematika.* (2013), 119–128.

[10] M. Radziwill and K. Soundararajan. Upper bounds for moments of zeta and L-functions. In preparation.

[11] Z. Rudnick and K. Soundararajan. Lower bounds for moments of L-functions. *Proc. Natl. Acad. Sci.* (2005) 6837–6838.

[12] K. Soundararajan. Moments of the Riemann zeta-function. *Annals of Math.* 170 (2009) 981–993.

[13] K. Soundararajan and M. Young. The second moment of quadratic twists of modular L-functions. *J. Eur. Math. Soc.* 12 (2010) 1097–1116.

On the Waring-Goldbach problem for fourth powers

Lilu Zhao

The general philosophy underlying applications of the Hardy-Littlewood circle method suggests that whenever s and k are positive integers with $s \geq k+1$, and n is a large natural number satisfying the necessary local conditions, then n should be represented as the sum of s kth powers of prime numbers. It is established in [2] that every sufficiently large positive integer congruent to 13 modulo 240 can be represented as the sum of 13 fourth powers of prime numbers. This improves upon the earlier result of Kawada and Wooley [1] with 14 variables.

Suppose that $k \geq 3$. Let $g(\alpha) = \sum_{P<p\leq 2P} e(p^k\alpha)$ and $h(\alpha) = \sum_{U<p\leq 2U} e(p^k\alpha)$. We consider $\int_{\mathfrak{m}} g(\alpha)G(\alpha)h(\alpha)d\alpha$, where $\mathfrak{m} \subset [0,1)$ and $G(\alpha)$ is an integrable function of period one. The conventional method may treat the integration as follows. One has

$$\Big|\int_{\mathfrak{m}} g(\alpha)G(\alpha)h(\alpha)d\alpha\Big| \leq \big(\sup_{\alpha\in\mathfrak{m}} |g(\alpha)|\big)\, \mathcal{J}, \tag{1}$$

where

$$\mathcal{J} := \mathcal{J}(\mathfrak{m}) \quad = \quad \int_{\mathfrak{m}} \big|G(\alpha)h(\alpha)\big| d\alpha.$$

Subject to the condition $P^{k2^{1-k}} \leq U \leq P$, we establish a new estimate

$$\int_{\mathfrak{m}} g(\alpha)G(\alpha)h(\alpha)d\alpha \ll (P^{4-k+\varepsilon}U^2)^{\frac14}\Big(\int_{\mathfrak{m}} \big|G(\alpha)\big|^2 d\alpha\Big)^{\frac14}\mathcal{J}^{\frac12} + P^{1-2^{-k}+\varepsilon}\mathcal{J}. \tag{2}$$

On ignoring the contribution from $(P^{4-k+\varepsilon}U^2)^{\frac14}\Big(\int_{\mathfrak{m}} \big|G(\alpha)\big|^2 d\alpha\Big)^{\frac14}\mathcal{J}^{\frac12}$, our conclusion is as strong as (1) by assuming that

$$\sup_{\alpha\in\mathfrak{m}} |g(\alpha)| \quad \ll \quad P^{1-2^{-k}+\varepsilon}. \tag{3}$$

One may also compare our conclusion to

$$(4)\qquad \int_{\mathfrak{m}} g(\alpha)G(\alpha)h(\alpha)d\alpha \ll \Big(\int_{\mathfrak{m}} \big|g(\alpha)^4h(\alpha)^2\big|d\alpha\Big)^{1/4}\Big(\int_{\mathfrak{m}} \big|G(\alpha)\big|^2d\alpha\Big)^{1/4}\mathcal{J}^{1/2}.$$

On ignoring the second term $P^{1-2^{-k}+\varepsilon}\mathcal{J}$, our conclusion is as strong as (4) provided that

$$(5)\qquad \int_{\mathfrak{m}} \big|g(\alpha)^4h(\alpha)^2\big|d\alpha \quad\ll\quad P^{4-k+\varepsilon}U^2.$$

It is worth to pointing out that both (3) and (5) are still open for $k=4$ if $\mathfrak{m}$ is the type of minor arcs.

For suitable minor arcs $\mathfrak{m}$, Kawada and Wooley [1] established that

$$\sup_{\alpha\in\mathfrak{m}}|g(\alpha)| \quad\ll\quad P^{1-2^{-k-1}+\varepsilon}.$$

In fact, the following type of estimate was employed by Kawada and Wooley [1]

$$\Big|\int_{\mathfrak{m}} g(\alpha)^2G(\alpha)h(\alpha)d\alpha\Big| \le \big(\sup_{\alpha\in\mathfrak{m}}|g(\alpha)^2|\big)\,\mathcal{J} \ll P^{2-2^{-k}+\varepsilon}\,\mathcal{J}.$$

By verifying that the contribution from first term on the right hand side of (2) is acceptable, we obtain a desired estimate for $\int_{\mathfrak{m}} g(\alpha)G(\alpha)h(\alpha)d\alpha$. Therefore, we are able to save one variable.

References

[1] K. Kawada and T. D. Wooley, *On the Waring-Goldbach problem for fourth and fifth powers*, Proc. Lond. Math. Soc. (3) **83** (2001), 1–50.

[2] L. Zhao, *On the Waring-Goldbach problem for fourth and sixth powers*, Proc. Lond. Math. Soc., accepted.

Problem session

1. Hugh Montgomery Let $c(0)=1$, $c(2n)=c(n)$, and $c(2n+1)=(-1)^nc(n)$. Thus the $c(n)$ are the Rudin–Shapiro coefficients, and $P_k(z)=\sum_{0\le n<2^k}c(n)z^n$ is the k^{th} Rudin–Shapiro polynomial. It is classical that $|P_k(z)|\le 2^{(k+1)/2}$ when $|z|=1$. Thus the maximum modulus of the trigonometric polynomial $P_k(e(\theta))$ is not more than $\sqrt{2}$ times its root-mean-square. Saffari has conjectured that $|P_k(e(\theta))|^2$ is asymptotically uniformly distributed in the interval $[0,2^{k+1}]$. He further noted that his conjecture would follow if it could be shown that

$$\int_0^1 |P_k(e(\theta))|^{2m}\,d\theta \sim \frac{2^{m(k+1)}}{m+1}$$

as $k\to\infty$, for each positive integer m. For $1\le m\le 26$ this has been achieved by Doche and Habsieger (Moments of the Rudin–Shapiro polynomials, *J. Fourier Anal. Appl.* **10** (2004), 497–505). We now propose a stronger conjecture, that the curve $P_k(e(\theta))$ is asymptotically uniformly distributed in the disc $|z|\le 2^{(k+1)/2}$.

We further note that this conjecture would follow if in addition to the above it could be shown that

$$M_{m,n}(k) := \int_0^1 P_k(e(\theta))^m P_k(e(-\theta))^n \, d\theta = o\big(2^{(m+n)k/2}\big)$$

as $k \to \infty$ for all pairs m, n of distinct positive integers. In this direction it has been shown that $M_{2,1}(k)$ satisfies a linear recurrence of order all of whose eigenvalues have absolute value 2, so that $M_{2,1}(k) \ll 2^k$.

2. Roger Heath–Brown The quantitative form of the Twin Prime Conjecture proposes that

$$\pi_2(x) := \#\{p \le x \,:\, p+2 \text{ prime}\} \sim C_2 \int_2^x \frac{dt}{\log^2 t}\,.$$

A stronger quantitative form of the conjecture states that

$$\pi_2(x) = C_2 \int_2^x \frac{dt}{\log^2 t} + O(1)\,.$$

Prove or disprove this.

3. Heath–Brown Let $S = \{n \,:\, q|n \implies q \not\equiv 3 \pmod 4\}$. This set contains infinitely many pairs of consecutive integers, say x^2, x^2+1. Now let $T = \{n \,:\, p|n \implies p \not\equiv 1 \pmod 4\}$. Can one show that the set T also contains infinitely many pairs of consecutive integers?

4. Brian Conrey Call this an *abc* conjecture, also known as the sum-product conjecture. Let $SP(n)$ denote the number of solutions of the equation $abc + a + b + c = n$ in positive integers. Show that for every $\varepsilon > 0$ there is a $C(\varepsilon)$ such that $SP(n) < C(\varepsilon)n^\varepsilon$. Bob Vaughan says that this would imply the solution of a problem concerning Egyptian fractions. It is easy to show that if $SP(n) = 0$, then n is prime.

5. Brian Conrey Show that a primitive degree 3 L-function must have infinitely many zeros on the critical line, or give an example of such a function with this property.

6. Greg Martin Consider the assertion that if $\sigma > 0$ and $\zeta(\sigma + it) = 0$, then t is rational. Show that this is false.

7. Igor Shparlinski Let $f(q)$ denote the number of representations of q in the form $q = a^2 + b$ where b is a positive integer composed entirely of primes $\equiv 1 \pmod 3$. We know that $f(q) < q^{1/2+o(1)}$. For prime q, $q \equiv 11 \pmod{12}$, we know that $f(q) > q^{1/2+o(1)}$. Give an asymptotic formula for $f(q)$, or for the mean value of $f(q)$.

8. Zeev Rudnick Let A be an arc of length R^θ of a circle of radius R and center 0. We conjecture that if $\theta < 1$, then there is a $C(\theta)$ such that A contains at most $C(\theta)$ lattice points. For $\theta = 1/3$ this was known to Jarnik. J. Cilleruelo and A.

Córdoba (Trigonometric polynomials and lattice points, *Proc. Amer. Math. Soc.* **115** (1992), 899–905) proved the conjecture for $\theta < 1/2$. D. S. Ramana (Arcs with no more than two integer points on conics, *Acta Arith.* **143** (2010), 197–210) showed that $C(\theta) < 2002/(1/2 - \theta)$ for $\theta < 1/2$. SG \$100 is offered for a proof when $\theta = 1/2$, and US \$100 is offered for a proof for all $\theta < 1$. Miguel Walsh's recent improvement of the work of Bombieri and Pila may give $\theta = 1/2$.

9. Trevor Wooley Let

$$S(q,a) = \sum_{r=1}^{q} e(ar^k/q)\,.$$

We know that if $(a,q) = 1$, then $S(q,a) \ll q^{1-1/k}$. Vaughan and Wooley define

$$T(q,a) = \sum_{r=1}^{q} (1/2 - r/q) e(ar^k/q)\,.$$

It is easy to show that if k is even, then $T(q,a) = -1/2$. When k is odd and $(a,q) = 1$, we know that $T(q,a) \ll_\varepsilon q^{1-1/k+\varepsilon}$. The problem is to determine the true order of $T(q,a)$. In this connection it may be helpful to note that

$$T(q,a) = \frac{1}{2}S(q,a) - \frac{1}{q}T^*(q,a)$$

where

$$T^*(q,a) = \sum_{r=1}^{q} re(ar^k/q) = \frac{1}{2}(q+1)S(q,a) + \sum_{b=1}^{q} \frac{S(q,a,b)}{1 - e(b/q)}$$

and

$$S(q,a,b) = \sum_{r=1}^{q} e((ar^k + br)/q)\,.$$

10. Tim Browning Estimate

$$\sum_{\substack{|x|\le N,\ |y|\le N,\ |z|\le N \\ y^2 z = x^3 + axz^2 + bz^3,\ (x,y,z)=1}} d(x)\,.$$

11. Per Salberger Let $F_0, \ldots, F_m$ be $m{+}1$ polynomials of degree d in $(x_0, \ldots, x_n)$ with no common zero. Then $(F_0, \ldots, F_m)$ defines a morphism $f : \mathbb{P}^n \to \mathbb{P}^m$. On $\mathbb{P}^m$ we define a natural height $H : \mathbb{P}^m(\mathbb{Q}) \to \mathbb{Z}$, by sending an integral primitive $m+1$-tuple $(x_0, \ldots, x_m)$ to $\max |x_i|$. Let $B \ge 1$ and

$$n_f(B) = \#\{x \in \mathbb{P}^n(\mathbb{Q}) \,:\, H(f(x)) \le B\}\,.$$

It is then an immediate consequence of the theory of heights that

$$n_f(B) = O_f\big(B^{(n+1)/d}\big)\,.$$

We conjecture that if f is a closed immersion, then

$$n_f(B) = O_{d,n,\varepsilon}\big(B^{(n+1)/d+\varepsilon}\big)\,.$$

This is easy to prove if $d = 1$, and is also known if $n = 1$. A proof of this would contribute to give better uniform bounds for the number of rational points of bounded height on general projective varieties.

12. Kevin Ford Prove that there exist infinitely many solutions in primes of

$$\prod_{j=1}^{k}(p_j + 1) = \prod_{i=1}^{\ell}(q_i - 1)\,.$$

Here k and ℓ may vary, but the p_j are distinct and the q_i are distinct. The point here is that we would have squarefree m and n such that $\sigma(m) = \phi(n)$.

13. Dan Goldston Prove that

$$\sum_{n \le x} \Lambda(n)\Lambda(n+2) = c_2 x + 2(\psi(x) - x) + \Omega(\log^2 x)\,.$$

On the subject of the Goldbach problem, we let

$$r(n) = \sum_{n_1+n_2=n} \Lambda(n_1)\Lambda(n_2)\,.$$

Following work of Fujii, Bhownik, Schlage–Puchta, Languosio, and Zaccagnini we know (on RH) that

$$\sum_{n \le x} \big(r(n) - n - 2(\psi(n) - n)\big) = O\big(x(\log x)^3\big),$$

even though the individual terms in the sum are not small.

14. Chowla conjectured that if χ is a Dirichlet character, then $L(\sigma, \chi) \neq 0$ for $\sigma > 0$. The case $\sigma = 1/2$ is of particular interest. On GRH, Murty has shown that the proportion of $\chi \pmod q$ such that $L(1/2, \chi) \neq 0$ is at least $1/2$. Improve on this.

Reporter: Jörg Brüdern

Participants

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

Prof. Dr. Yuri Bilu
A2X, IMB
Université Bordeaux I
351, cours de la Liberation
33405 Talence Cedex
FRANCE

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

Julia Brandes
School of Mathematics
University of Bristol
University Walk
Bristol BS8 1TW
UNITED KINGDOM

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
Bunsenstr. 3-5
37073 Göttingen
GERMANY

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

Prof. Dr. Brian Conrey
American Institute of Mathematics
360 Portage Ave.
Palo Alto, CA 94306
UNITED STATES

Prof. Dr. Regis de la Breteche
U.F.R. de Mathématiques
Case 7012
Université de Paris 7
Bâtiment Sophie Germain
75251 Paris Cedex 13
FRANCE

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

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

Prof. Dr. Kevin Ford
Dept. of Mathematics, University of
Illinois at Urbana-Champaign
273 Altgeld Hall, MC-382
1409 West Green Street
Urbana, IL 61801-2975
UNITED STATES

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

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

Prof. Dr. Daniel A. Goldston
Department of Mathematics
San Jose State University
San Jose CA 95192-0103
UNITED STATES

Prof. Dr. Steve Gonek
Department of Mathematics
University of Rochester
Rochester, NY 14627
UNITED STATES

Dr. Adam J. Harper
Department of Pure Mathematics
and Mathematical Statistics
University of Cambridge
Wilberforce Road
Cambridge CB3 0WB
UNITED KINGDOM

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

Prof. Dr. Harald Helfgott
Dept. de Mathématiques et Applications
École Normale Superieure
45, rue d'Ulm
75230 Paris Cedex 05
FRANCE

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

Prof. Dr. Koichi Kawada
Department of Mathematics
Faculty of Education
Iwate University
Morioka 020-8550
JAPAN

Prof. Dr. Sergei V. Konyagin
Department of Mechanics &
Mathematics
Moscow State University
Leninskiye Gory, Main Building
119 991 Moscow GSP-1
RUSSIAN FEDERATION

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

Prof. Dr. Angel V. Kumchev
Towson University
Department of Mathematics
8000 York Road
Towson, MD 21252-001
UNITED STATES

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

Dr. Steve Lester
Department of Mathematics
School of Mathematical Sciences
Tel Aviv University
Ramat Aviv, Tel Aviv 69978
ISRAEL

Prof. Dr. Akos Magyar
Department of Mathematics
University of British Columbia
121-1984 Mathematics Road
Vancouver BC V6T 1Z2
CANADA

Prof. Dr. Helmut Maier
Abteilung Zahlentheorie und
Wahrscheinlichkeitstheorie
Universität Ulm
Helmholtzstrasse 18
89069 Ulm
GERMANY

Dr. Oscar Marmon
Mathematisches Institut
Georg-August-Universität Göttingen
Bunsenstr. 3-5
37073 Göttingen
GERMANY

Prof. Dr. Greg Martin
Department of Mathematics
University of British Columbia
121-1984 Mathematics Road
Vancouver BC V6T 1Z2
CANADA

Dr. Kaisa Matomäki
Dept. of Mathematics & Statistics
University of Turku
Room 117
20014 Turku
FINLAND

Dr. Lilian Matthiesen
Département de Mathématiques
Université Paris Sud (Paris XI)
91405 Orsay Cedex
FRANCE

James A. Maynard
Centre de Recherches Mathématiques
Université de Montreal
Station Centre-Ville
P.O. Box 6128
Montreal, Quebec H3C 3J7
CANADA

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

Prof. Dr. Ritabrata Munshi
School of Mathematics
Tata Institute of Fundamental
Research
Homi Bhabha Road
Mumbai 400 005
INDIA

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
Hausdorff Center for Mathematics
Endenicher Allee 62
53115 Bonn
GERMANY

Prof. Dr. Janos Pintz
Alfred Renyi Institute of Mathematics
Hungarian Academy of Sciences
P.O.Box 127
1364 Budapest
HUNGARY

Dr. Sean Prendiville
School of Mathematics
University of Bristol
University Walk
Bristol BS8 1TW
UNITED KINGDOM

Maksym Radziwill
Institute for Advanced Study
Einstein Drive 1
Princeton NY 08540
UNITED STATES

Dr. Michail Th. Rassias
Departement Mathematik
ETH-Zentrum
Rämistr. 101
8092 Zürich
SWITZERLAND

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

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

Prof. Dr. Igor E. Shparlinski
Department of Pure Mathematics
UNSW
Sydney NSW 2052
AUSTRALIA

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

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

Boqing Xue
Department of Mathematics
Shanghai Jiao Tong University
Shanghai 200 240
CHINA

Dr. Lilu Zhao
School of Mathematics
Hefei University of Technology
Tunxi Road 193
Hefei 230 009
CHINA