Mathematisches Forschungsinstitut Oberwolfach

Report No. 14/2008

Analytic Number Theory

Organised by
Jörg Brüdern, Stuttgart
Hugh L. Montgomery, Ann Arbor
Robert C. Vaughan, Penn State

March 9th – March 15th, 2008

Abstract. The meeting on analytic number theory brings together leading experts from various active subbranches of the field, including L-functions, counting points on varieties by the circle method or geometric means, sieves, distribution of primes.

Mathematics Subject Classification (2000): 11xx.

Introduction by the Organisers

It was an exciting week at the Forschungsinstitut, with reports of important new developments, and intense work on a variety of fronts. The atmosphere was warm and relaxed, almost convivial, and certainly more cooperative than competitive, although the mutual seriousness of purpose was constantly evident.

Of all the new results announced at the meeting, three stand out for special mention:

Jerzy Kaczorowski and Alberto Perelli have shown that there is no member of the Selberg Class with degree in the open interval $(1, 2)$. The Selberg Class is an attempt to describe, by means of functional equations and Euler products, those functions for which one feels the Riemann Hypothesis should be true. It is presumed that eventually it will turn out that the Selberg Class is synonymous with the set of automorphic L-functions, but we are very far from proving this. The degree, which relates to the sum of the arguments of the gamma function factors in the functional equation, is conjectured always to be an integer. The Riemann zeta function has degree 1, and H.-E. Richert showed that there is no member with degree < 1. More recently it had been shown that there is no member with degree in the interval $(1, 5/3)$. This is a central problem, that many people

have attacked, so the realization of $(1, 2)$ is a remarkable step forward, albeit a modest advance when compared with the enormous task ahead of us.

The Prouhet–Thue–Morse sequence has been independently discovered three times, in 1851, 1906, and 1921, respectively. Prouhet related the sequence to number theory, Thue applied it to combinatorics on words, and Morse to differential geometry. Let $w(n)$ denote the 'binary weight of n', which is to say the number of 1's in the binary expansion of n. Thus $w(0) = 0$, $w(2n) = w(n)$, and $w(2n+1) = w(2n)+1$. Put $t_n = 0$ if $w(n)$ is even, and $t_n = 1$ if n is odd. Thus the word $t_0t_1t_2\ldots$ is $0110100110010110100\ldots$. The power series generating function of $(-1)^{w(n)}$ can be written in closed form:

$$\sum_{n=0}^{\infty}(-1)^{w(n)}z^n = \prod_{k=0}^{\infty}\left(1 - z^{2^k}\right) \qquad (|z| < 1)\,.$$

Clearly, $\left|\sum_{0\le n\le N}(-1)^{w(n)}\right| \le 1$ for all N; thus the integers are very equally divided between those for which $w(n)$ is even and those for which $w(n)$ is odd. In 1967, Gelfond (famous for work in transcendence) asked whether $w(p)$ is (asymptotically) equally even and odd, as p ranges over primes $p \le x$, $x \to \infty$. The Prime Number Theorem concerns the leading binary digits of p, and Dirichlet's theorem on primes in arithmetic progression relates to the trailing digits. As concerns $(-1)^{w(p)}$, one is dealing simultaneously with *all* binary digits of p. Many researchers have worked on this problem without success, including at least one of the conference organizers. Some years ago a solution was announced in C. R. Paris, but this was followed neither by a proof nor a retraction. Now at last we have a solution: Joël Rivat and Christian Mauduit have cleverly seen how to show that $\sum_{p\le x}(-1)^{w(p)} = o(\pi(x))$ as $x \to \infty$.

Consider the Pell equation $x^2 - dy^2 = \pm 1$, which relates to the units in the real quadratic number field $\mathbb{Q}(\sqrt{d})$. If d is divisible by a prime $p \equiv 3 \pmod 4$, then the equation $x^2 - dy^2 = -1$ has no solution. If d is a prime number $\equiv 1 \pmod 4$, then $x^2 - dy^2 = -1$ *does* have a solution. The number of $d \le x$ for which d is composed entirely of primes $p \equiv 1 \pmod 4$ is $\asymp x/\sqrt{\log x}$; thus the case of d prime is negligible among these discriminants. In a spectacular *tour de force*, Etienne Fouvry and Jürgen Klüners have shown that the 'negative Pell equation' $x^2 - dy^2 = -1$ has a solution for a positive proportion of discriminants d composed entirely of primes $\equiv 1 \pmod 4$.

The advances described above could not have been anticipated, and are at once surprising and gratifying. And just a few years before, the team of Goldston, Pintz and Yıldırım excited the world with their proof that $p_{n+1} - p_n = o(\log p_n)$ infinitely often. This brings us a little closer to twin primes. Since $p_{n+1} - p_n$ is $\log p_n$ on average, it is reasonable to consider the distribution of $(p_{n+1} - p_n)/\log p_n$. We conjecture that this quantity is asymptotically distributed like an exponential random variable, with density e^{-x}. It would follow that every number in $[0, \infty]$ is a limit point of the numbers $(p_{n+1} - p_n)/\log p_n$. In the 1930's it was shown

that $+\infty$ is a limit point, but it was only with the work of GPY that we could for the first time name a finite real number (namely 0) that is a limit point of this sequence. The GPY technology has been scrutinized, and has matured, but the team had their heads together for long hours during the conference, with the promise of further results.

Other highly active subareas that were represented at the meeting include additive combinatorics and the circle method, rational points on varieties, spectral decompositions for L-functions, sieve methods, and others.

The vast array of activity, the overload of talent, the extreme unpredictability of advances all make it challenging to select a fruitful mix of participants. On this occasion we feel that we could not have done better. Several participants, after the evening problem session, said that it was the best such session that they had ever experienced at Oberwolfach—more open, frank, and productive.

This meeting is in the tradition of Oberwolfach meeting organized by Theodor Schneider in the 1960's and 1970's that some us remember. We hope to emulate his vision as best possible in the modern times by taking a broad view and only the most gifted invitees.

Workshop: Analytic Number Theory

Table of Contents

Antal Balog (joint with Andrew Granville and Kannan Soudararajan)
Multiplicative Functions in Arithmetic Progressions 677

William D. Banks (joint with Ahmet M. Güloğlu, C. Wesley Nevans)
On the Lehmer conjecture 678

Valentin Blomer (joint with Gergely Harcos)
Spectral Decomposition of Shifted Convolution Sums 679

Régis de la Bretèche (joint with Tim Browning)
Counting rational points on a non-singular del Pezzo surface of degree 4 682

T.D. Browning
Cubic hypersurfaces with additional structure 683

Rainer Dietmann
Simultaneous Diophantine approximation by square-free numbers 684

Christian Elsholtz
Multiplicative decompositions of shifted primes 686

Kevin Ford (joint with Sergei V. Konyagin, Florian Luca)
Prime chains and Pratt trees 687

Étienne Fouvry (joint with J. Klüners)
On the negative Pell equation 688

John Friedlander
Sifting short intervals 690

Dan Goldston
Gaps between primes 691

Friedrich Götze (joint with Gregory Margulis, Andrei Zaitsev)
Indefinite Quadratic Forms and the Multivariate Central Limit Theorem 694

Sidney Graham (joint with Hugh Montgomery)
The Ideal Sieve 696

Harald A. Helfgott
Growth in SL_3 *and elsewhere* 698

D.R. Heath-Brown
Zeros of Cubic and Quartic Forms 699

Christopher Hughes (joint with Eduardo Dueñez, David W. Farmer, Sara Froehlich, Francesco Mezzadri, Toan Phan)
The horizontal distribution of zeros of the derivative of the Riemann zeta function 701

Martin Huxley
Configurations of Lattice Points 703

Aleksandar Ivić
Hybrid moments of the zeta-function on the critical line 705

Matti Jutila
Atkinson's formula for Hardy's function 708

Jerzy Kaczorowski (joint with Alberto Perelli)
Nonexistence of L-functions of degree $1 < d < 2$ 710

Jianya Liu (joint with Peter Sarnak)
Prime or almost-prime solutions to quadratic equations 712

Helmut Maier (joint with Ulirike Vorhauer)
Intervals on the critical line, in which the Riemann zeta function assumes only small values 713

Hugh L. Montgomery
The Combinatorics of moment calculations 714

Yoichi Motohashi
Complete Spectral Decomposition of the Mean Value of any Automorphic L-function — A unified approach 715

Scott T. Parsell
New estimates for multidimensional Weyl sums 718

Alberto Perelli (joint with J.Kaczorowski and G.Molteni)
A converse theorem for Dirichlet L-functions 719

János Pintz
Gaps between primes and Goldbach numbers 721

Olivier Ramaré
Eigenvalues in the large sieve inequality 722

Joël Rivat (joint with Christian Mauduit)
The sum of digits of primes and squares 723

Zeév Rudnick (joint with Dmitry Faifman)
Statistics of zeros for families of zeta functions of curves over a finite field 726

Jan-Christoph Schlage-Puchta (joint with Gautami Bhowmik, Immanuel Halupczok)
An improved version of the inductive method for zero-sum problems 727

Igor E. Shparlinski (joint with Jean Bourgain, Kevin Ford and Sergei V. Konyagin)
Fermat Quotients 729

Craig V. Spencer
Diophantine inequalities in function fields 731

R. C. Vaughan (joint with T. D. Wooley)
Higher order terms in Waring's problem 733

Mark Watkins
Uniform distribution of $(cx)^{3/2} \pmod 1$ *for* $c \in \mathbf{Q}$ 735

Trevor D. Wooley (joint with Yu-Ru Liu)
The circle method in function fields 737

Cem Yalçın Yıldırım (joint with Moubariz Z. Garaev)
Some observations on the zeros of the Riemann zeta-function 739

Abstracts

Multiplicative Functions in Arithmetic Progressions

Antal Balog
(joint work with Andrew Granville and Kannan Soudararajan)

The problem we are going to discuss in this talk is to determine, for multiplicative functions f with $|f(n)| \le 1$, estimates for the mean values

$$\frac{1}{x/q} \sum_{\substack{n\le x \\ n\equiv a \bmod q}} f(n). \tag{1}$$

One can expect a well distribution result in the form

$$\sum_{\substack{n\le x \\ n\equiv a \bmod q}} f(n) \sim \frac{1}{\phi(q)} \sum_{\substack{n\le x \\ (n,q)=1}} f(n), \tag{2}$$

however this does not always reflects the truth. For example, if the so called Siegel–zeros do exist then the primes are unevenly distributed in certain residue classes and this irregularity supposedly affects (2) as well. Actually, there is a much simpler example against (2), namely $f(n)$ being a character mod q. We develop a theory that handles all cases rather uniformly. We will show that for any fixed $\epsilon > 0$ there exists a (big) A such that

$$\Big| \sum_{\substack{n\le x \\ n\equiv a \bmod q}} f(n) \Big| \le \epsilon \frac{x}{q} \tag{3}$$

for all $(a,q) = 1$ for all $q \le x^{1/A}$, except possibly those q that are multiples of some exceptional modulus r. Moreover, if such a modulus r exists then there is also a primitive character χ_1 mod r such that

$$\sum_{\substack{n\le x \\ n\equiv a \bmod q}} f(n) = \chi_1(a) \sum_{\substack{n\le x \\ n\equiv 1 \bmod q}} f(n) + O(\epsilon\frac{x}{q}) = \frac{\chi_1(a)}{\phi(q)} \sum_{\substack{n\le x \\ (n,q)=1}} f(n)\overline{\chi_1(n)} + O(\epsilon\frac{x}{q}) \tag{4}$$

whenever $(a,q) = 1$, $r|q$, $q \le x^{1/A}$.

The exceptional character χ_1, if it exists, is determined by means of the following distance function.

$$D^2(f,g;x) = \sum_{p\le x} \frac{1 - \Re f(p)\overline{g(p)}}{p}. \tag{5}$$

If this distance is small then $f(p)$ is close to $g(p)$ most of the time, and so $f(n)$ pretends to be $g(n)$ by their multiplicativity. Our main result can be read as follows; either there is a primitive character χ_1 mod r and a real number t such that $f(n)$ pretends to be $\chi_1(n)n^{it}$, in which case both χ_1 and t are unique and (4) holds, or f is unpretentious and (3) holds.

The proof is based on Halász's Theorem on the mean value of multiplicative functions, on the study of the above distance function (5), and on the fact that a periodic "almost multiplicative" function is almost a character.

On the Lehmer conjecture

William D. Banks
(joint work with Ahmet M. Güloğlu, C. Wesley Nevans)

Let $\varphi(n)$ be the *Euler function*, which is defined as usual by

$$\varphi(n) = n \prod_{p \mid n} \left(1 - p^{-1}\right) \qquad (n \ge 1).$$

In 1932, D. H. Lehmer [3] asked whether there are any *composite* numbers for which $\varphi(n) \mid n - 1$, and the answer to this question is still unknown.

In a series of papers (see [4, 5, 6]) C. Pomerance considered the problem of bounding the cardinality of $L(x) = L \cap [1, x]$, where L is the (possibly empty) set of composite numbers n such that $\varphi(n) \mid n - 1$. In his third paper [6] Pomerance established the bound

$$\#L(x) \ll x^{1/2} (\log x)^{3/4} \tag{1}$$

and remarked that

> *There is still clearly a wide gap between the possibility that $L = \emptyset$ and* (1)*, for the latter does not even establish that the members of L are as scarce as squares!*

Refinements of the underlying method of [6] led to subsequent improvements of the bound (1) by Shan [7], who showed that

$$\#L(x) \ll x^{1/2} (\log x)^{1/2} (\log\log x)^{-1/2},$$

and by Banks and Luca [1], who established the bound

$$\#L(x) \ll x^{1/2} (\log\log x)^{1/2}.$$

In a recent work [2], we have used similar techniques to show that the members of L are indeed *scarcer than squares*, i.e., that $\#L(x) = o(x^{1/2})$ as $x \to \infty$. More precisely, we have shown the following:

Theorem. *For any fixed $\epsilon > 0$ the bound*

$$\#L(x) \ll \frac{x^{1/2}}{(\log x)^{\Theta - \epsilon}}$$

holds, where $\Theta = 0.129398\cdots$ is the least positive solution to the equation

$$2\Theta(\log\Theta - 1 - \log\log 2) = -\log 2.$$

References

[1] W. D. Banks and F. Luca, *Composite integers n for which $\varphi(n) \mid n-1$*, Acta Math. Sinica, English Series **23** (2007), no. 10, 1915–1918.
[2] W. D. Banks, A. Güloğlu and W. Nevans, *On the congruence $n \equiv a \pmod{\varphi(n)}$*, preprint, 2008.
[3] D. H. Lehmer, *On Euler's totient function*, Bull. Amer. Math. Soc. **38** (1932), 745–757.
[4] C. Pomerance, *On the congruences $\sigma(n) \equiv a \pmod{n}$ and $n \equiv a \pmod{\varphi(n)}$*, Acta Arith. **26** (1974/75), no. 3, 265–272.
[5] C. Pomerance, *On composite n for which $\varphi(n) \mid n-1$*, Acta Arith. **28** (1975/76), no. 4, 387–389.
[6] C. Pomerance, *On composite n for which $\varphi(n) \mid n-1$, II*, Pacific J. Math. **69** (1977), no. 1, 177–186.
[7] Z. Shan, *On composite n for which $\varphi(n) | n-1$*, J. China Univ. Sci. Tech. **15** (1985), 109–112.

Spectral Decomposition of Shifted Convolution Sums

Valentin Blomer
(joint work with Gergely Harcos)

Given an arithmetic function $\alpha : \mathbb{N} \to \mathbb{C}$ and an integer $h \in \mathbb{N}$, it is interesting to study the shifted convolution Dirichlet series

$$\sum_{n=1}^{\infty} \frac{\alpha(n)\overline{\alpha(n+h)}}{n^s}. \tag{1}$$

This is more or less equivalent to studying sums like $\sum_{m-n=h} \alpha(n)\overline{\alpha(m)}W(m,n)$ for sufficiently nice weight functions W. The investigation of such Dirichlet series may be motivated by several reasons: one can be interested in the underlying arithmetic problem (think of $\alpha = \Lambda$ and $h = 2$). Moreover, shifted convolution sums arise naturally as off-diagonal terms of the second moment of L-functions. Finally, the Dirichlet series (1) may have some underlying structue (e.g. a spectral decomposition) which one would like to exhibit.

As an example, let us look at Hecke eigenvalues $\lambda(n)$ of some holomorphic cusp form $f \in S_k(N, \chi)$. Let

$$P_h(z,s) := \sum_{\gamma \in \Gamma_\infty \backslash \Gamma_0(N)} \Im(\gamma z)^s e(-h\Re\gamma z).$$

This is a weight 0 Poincaré series. Using the Rankin-Selberg unfolding technique, one derives the integral representation ([17])

$$\frac{(2\pi)^{s+k-1}}{\Gamma(s+k-1)} \langle P_h(.,s), y^k|f|^2\rangle = \sum_{m-n=h} \frac{\lambda(n)\overline{\lambda(m)}(nm)^{(k-1)/2}}{(n+m)^{s+k-1}}. \tag{2}$$

This can now be decomposed with respect to the non-Euclidean Laplacian and meromorphically continued. There are numerous applications of such a deompo-sition, see for example [9, 13, 15] to name just a few. But this is not the end of

the story, and Selberg [17] states: *"We cannot make much use of this function at present."* Two problems remain: (a) because of the Γ-factor, it is not at all clear how to derive polynomial growth estimates on vertical lines. This has been achieved by Good [9] and in a more general context by Sarnak [15]. (b) If the $\lambda(n)$ come from an arbitrary irreducible cuspidal representation over GL_2 (not necessarily from the discrete series), this approach breaks down, not only for technical reasons, but for unavoidable conceptual reasons, see [10] for more details. It should, however, be noted that these difficulties can often be overcome in practice by approximate formulae with sufficiently manageable error terms, see in particular Jutila [11, 12] and Sarnak [16].

Here we proceed differently and obtain a way to obtain an exact spectral decomposition of the right hand side of (2). Let $G = GL_2^+(\mathbb{R})$ and Γ a congruence subgroup (for simplicity $\Gamma = SL_2(\mathbb{Z})$). Then we have a G-equivariant decomposition of the type $L^2(\Gamma\backslash G) = \int V_\pi d\pi$ where on the discrete spectrum the measure $d\pi$ is just the counting measure. Our approach relies on two important ingredients: inspired by Motohashi [14], we use the Whittaker model

$$V_\pi \ni \phi \mapsto W_\phi = \int_0^1 \phi\left(\begin{pmatrix} \cdot & x \\ 0 & 1 \end{pmatrix}\right) e(-x)dx \in L^2\left(\mathbb{R}_{>0}, dy/y\right).$$

This is a Hilbert space isomorphism, and the scalar products are related by a proportionality constant that is essentially $L(1, \mathrm{ad}^2\pi)$ (for the continuous spectrum, one may use this as a definition of a natural scalar product on V_π). Inspired by Bernstein/Reznikov [2] and Venkatesh [18], we use Sobolev norms on V_π^∞ which are an elegant tool to ensure absolute convergence and rapid decay of various series, provided the relavant vectors and weight functions are sufficiently smooth. The details are not obvious, but it turns out that without too much technical effort we can obtain the following result [3]:

Theorem 1. *Let $k \geq 60$ be any integer, Let $h \in \mathbb{N}$, and $\lambda(n)$ Hecke eigenvalues of any irreducible cuspidal representation over GL_2 of conductor 1. Then there exist holomorphic functions F_π (depending on k) such that*

$$\sum_{m-n=h} \frac{\lambda(n)\overline{\lambda(m)}(nm)^{(k-1)/2}}{(n+m)^{s+k-1}} = h^{1/2-s} \int \lambda_\pi(h) F_\pi(s) d\pi$$

and

$$\int |F_\pi(s)| d\pi \ll |s|^{22}, \quad \frac{1}{2} + \varepsilon \leq \Re s \leq \frac{3}{2}.$$

This can be generalized to arbitrary conductor and central character without much effort, and also to number fields (where other methods are much harder to implement). In this way one can prove [5]:

Theorem 2. *Let $K/\mathbb{Q}$ be a totally real number field of class number 1, π and irreducible cuspidal representation over GL_2 and χ a Größencharacter of conductor $\mathfrak{q}$. Then*

$$L(s, \pi \otimes \chi) \ll_{\pi,s} (N\mathfrak{q})^{\frac{1}{2}-\frac{1}{8}(1-2\theta)}$$

for $\Re s = 1/2$, and $\theta < 1/9$ an admissible exponent for the Ramaunjan-Petersson conjecture.

The class number one restriction can be removed with more effort. Subconvexity for twisted L-functions over number fields was first obtained in an unpublished manuscript of Cogdell, Piatetskii-Shapiro and Sarnak, and very recently by Venkatesh [18]. Our method is entirely different and gives a stronger exponent than either of the above mentioned results. This should be compared with the situation over $\mathbb{Q}$, see [6, 4]. Theorem 2 has a number of further applications:

- bounds for Fourier coefficients of half-integral weight modular forms over number fields [1];
- the representation of integers by ternary quadratic forms and Hilbert's eleventh problem [7];
- equidistribution of a certain family of Heegner points on the modular surface $PSL_2(\mathcal{O})\backslash\mathcal{H}^d$. [8].

References

[1] E. M. Baruch, Z. Mao, *Central value of automorphic L-functions*, GAFA **17** (2007), 333-384

[2] J. Bernstein, A. Reznikov, *Sobolev norms of automorphic functionals*, Int. Math. Res. Not. **2002**, 2155–2174

[3] V. Blomer, G. Harcos, *The spectral decomposition of shifted convolution sums*, to appear in Duke Math. J.

[4] V. Blomer, G. Harcos, *Hybrid bound for twisted L-functions*, to appear in J. Reine Angew. Math.

[5] V. Blomer, G. Harcos, *Twisted L-functions over number fields, and Hilbert's eleventh problem*, in preparation

[6] V. Blomer, G. Harcos, P. Michel, *A Burgess-like subconvex bound for twisted L-functions (with Appendix 2 by Z. Mao)*, Forum Math. **19** (2007), 61–105

[7] J. Cogdell, *On sums of three squares*, J. Théor. Nombers Bordeaux **15** (2003), 33-44

[8] P. Cohen, *Hyperbolic equidistribution problems on Siegel 3-folds and Hilbert modular varieties*, Duke Math. J. **129** (2005), 87-127

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

[10] G. Harcos, *New bounds for aitomorphic L-functions*, Ph.D. thesis, Princeton 2003

[11] M. Jutila, *Lectures on a method in the theory of exponential sums*, Tata Institute of Fundamental Research Lectures on Mathematics and Physics 80, Springer-Verlag, Berlin, 1987

[12] M. Jutila, *The additive divisor problem and its analogs for Fourier coefficients of cusp forms. I*, Math. Z. **223** (1996), 435–461; *II*, ibid. **225** (1997), 625–637

[13] Y.-K. Lau, J. Liu, Y. Ye, *A new $k^{2/3+\varepsilon}$ for Rankin-Selberg L-functions for Hecke congruence subgoups*, Int. Math. Res. Pap. **2006**, Art.ID 35090, 78pp.

[14] Y. Motohashi, *A note on the mean value of the zeta and L-function. XIV*, Proc. Japan Acad. Ser. A Math. Sci. **80** (2004), 28–33

[15] P. Sarnak, *Integrals of products of eigenfunctions*, Int. Math. Res. Not. **1994**, 251–260

[16] P. Sarnak, *Estimates for Rankin–Selberg L-functions and quantum unique ergodicity*, J. Funct. Anal. **184** (2001), 419–453

[17] A. Selberg, *On the estimation of Fourier coefficients of modular forms*, Proc. Sympos. Pure Math., Vol. VIII, 1–15, Amer. Math. Soc., Providence, RI, 1965
[18] A. Venkatesh, *Sparse equidistribution problems, period bounds, and subconvexity*, to appear.

Counting rational points on a non-singular del Pezzo surface of degree 4

Régis de la Bretèche
(joint work with Tim Browning)

A del Pezzo surface of degree 4 can be viewed as the zero locus of a suitable pair of quadratic forms $Q_1,\ Q_2 \in \mathbb{Z}[x_1, ..., x_5]$. In collaboration with Tim Browning, I began a programme to count rational points of bounded height on these surfaces. The tools involved come from arithmetical geometry and analytic number theory.

The Manin conjecture [1] predicts precise asymptotic formulae for the growth rate of the counting function

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

as $B \to \infty$, where H is a height function metrized by a choice of norm $\|\cdot\|$ on $\mathbb{R}^5$, and $U \subset X$ is the Zariski open subset formed by deleting the 16 lines from X.

We shall explain the resolution of this conjecture in the special case that X is defined by the pair of quadratic forms

$$Q_1(\mathbf{x}) := x_0x_1 - x_2x_3, \quad Q_2(\mathbf{x}) := x_0^2 + x_1^2 + x_2^2 - x_3^2 - 2x_4^2.$$

It is clear that X is non-singular. It will be convenient to work with the choice of norm

$$\|\mathbf{x}\| := \max\left\{\sqrt{3}|x_0|, \sqrt{3}|x_1|, \sqrt{3}|x_2|, \sqrt{3}|x_3|, \sqrt{x_3^2 + 2x_4^2}\right\},$$

for any $\mathbf{x} = (x_0, \dots, x_4) \in \mathbb{R}^5$.

Our main result is the following.

Theorem 1. *There exists a constant $C > 0$ such that*

$$N_{U,H}(B) = CB(\log B)^4\big(1 + o(1)\big),$$

as $B \to \infty$.

An easy calculation reveals that Pic $(X) \cong \mathbb{Z}^5$, so that this asympotic formula is in agreement with Manin's prediction.

One of the key tools in the proof of Theorem 1 involves the geometry of numbers. This permits us to prove also an asymptotic formula for

$$S(X) = \sum_{\mathbf{x} \in \mathbb{Z}^2 \cap X\mathcal{R}} \tau(L_1(\mathbf{x})L_2(\mathbf{x})Q(\mathbf{x}))$$

when L_1, L_2, Q and $\mathcal{R}$ satisfy the following hypotheses:

(i) $\mathcal{R}$ is an open, bounded and convex region, with a piecewise continuously differentiable boundary,

(ii) L_1, L_2 are two non-proportional binary linear form and Q is binary quadratic form which is irreducible avec $\mathbb{Q}[\mathbf{x}]$,
(iii) $L_i(\mathbf{x}) > 0$ and $Q(\mathbf{x}) > 0$ for all $\mathbf{x} \in \mathcal{R}$.

With these conditions in mind we have the following auxilliary result.

Theorem 2. *Let $\varepsilon > 0$ and $L_1, L_2, Q, \mathcal{R}$ satisfying (i)-(iii). When $X \geq 2$, we have*

$$S(X) = 2C'\mathrm{meas}(\mathcal{R})X^2(\log X)^3 + O\big(X^2(\log X)^{2+\varepsilon}\big), \tag{1}$$

where C' is an explicit constant that can be defined as an Eulerian product.

References

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

Cubic hypersurfaces with additional structure

T.D. Browning

Let $X \subset \mathbb{P}^{n-1}$ be a cubic hypersurface, given as the zero locus of a cubic form $C \in \mathbb{Z}[x_1, \ldots, x_n]$. A basic goal in number theory is to try and determine conditions under which the set of rational points $X(\mathbb{Q})$ on X is non-empty. When C is diagonal it follows from the work of Baker [1] that X has $\mathbb{Q}$-rational points as soon as $n \geq 7$. At the opposite end of the spectrum, when absolutely no assumptions are made about the shape of C, there is the recent work of Heath-Brown [5], ensuring that $n \geq 14$ variables are enough to secure this fact. It is natural to try and establish intermediate results in which the existence of rational points is guaranteed for cubic hypersurfaces in fewer than 14 variables when certain assumptions are made about the structure of the hypersurface.

Let $m \leq n$ be a positive integer. We will say that an integral cubic form C in n variables "splits off an m-form" if there exist non-zero cubic forms C_1, C_2 with integer coefficients such that

$$C(x_1, \ldots, x_n) = C_1(x_1, \ldots, x_m) + C_2(x_{m+1}, \ldots, x_n),$$

identically in $x_1, \ldots, x_n$. We will merely say that C "splits off a form" if C splits off an m-form for some $1 \leq m \leq n$. With this in mind we have the following result.

Theorem 1. *Let $X \subset \mathbb{P}^{n-1}$ be a hypersurface defined by a cubic form that splits off a non-singular form, with $n \geq 13$. Then $X(\mathbb{Q}) \neq \emptyset$.*

Any non-zero cubic form in only 1 variable is non-singular. Hence we may combine work of Fowler [4] with an application of Theorem 1 to cubic forms of the shape

$$C(x_1, \ldots, x_m) - ay^3,$$

in order to deduce the following.

Theorem 2. *Let $C \in \mathbb{Z}[x_1, \dots, x_n]$ be a non-degenerate cubic form in $n \geq 12$ variables. Then C represents every non-zero rational number.*

The expected range is $n \geq 8$ here, since the relevant cubic form always has non-trivial p-adic zeros for n in this range.

The proof of Theorem 1 uses the Hardy–Littlewood circle method, and employs many of the contributions to the theory of cubic exponential sums that have been made during the last fifty years. In addition to this, when the cubic form splits off a non-singular m-form with m small, the minor arc analysis takes advantage of recent joint work of the author with Heath-Brown [2], in order to estimate rational points of bounded height on certain auxiliary non-singular cubic hypersurfaces.

With more work it is possible to relax the condition that one of the forms be non-singular in Theorem 1, as the following result shows.

Theorem 3. *Let $X \subset \mathbb{P}^{n-1}_{\mathbb{Q}}$ be a hypersurface defined by a cubic form that splits off an m-form, with $m \neq 5$ and $n \geq 13$. Then $X(\mathbb{Q}) \neq \emptyset$.*

This is still work in progress and it seems very likely that the case $m = 5$ will be handled satisfactorily in due course. The proof of Theorem 3 relies upon Theorem 1 to handle the case in which one of the forms is non-singular. When both are singular, and one of them has a relatively small number of variables, the classification of singular cubic hypersurfaces is brought into play. In particular, when the cubic form splits off a singular 4-form, the work of Coray and Tsfasman [3] (although there are many other authors who have worked on this topic) can be used to restrict attention to forms which define a cubic surface containing exactly 3 singular points, all of which are conjugate over some cubic extension of $\mathbb{Q}$. This in turn forces the cubic hypersurface to have even more structure, to the extent that a renewed application of the circle method yields the result.

References

[1] R. C. Baker, *Diagonal cubic equations, II*, Acta Arith. **53** (1989), 217–250.

[2] T. D. Browning and D. R. Heath-Brown, *The density of rational points on non-singular hypersurfaces, II*, Proc. London Math. Soc. **93** (2006), 273–303.

[3] D. F. Coray and M. A. Tsfasman, *Arithmetic on singular Del Pezzo surfaces*, Proc. London Math. Soc. **57** (1988), no. 1, 25–87.

[4] J. Fowler, *A note on cubic equations*, Proc. Cambridge Philos. Soc. **58** (1962), 165–169.

[5] D. R. Heath-Brown, *Rational points on cubic hypersurfaces*, Invent. Math. **170** (2007), 199–230.

Simultaneous Diophantine approximation by square-free numbers

Rainer Dietmann

Improving on results by Balog/Perelli ([2]) and Harman ([4]), Heath-Brown ([5]) showed that for any irrational real number α there are infinitely many square-free integers n such that $||n\alpha|| \ll n^{-2/3+\epsilon}$ where $|| \cdot ||$ denotes distance to the nearest integer. Baker, Brüdern and Harman ([1]) considered the more general problem of simultaneous Diophantine approximation with square-free numbers.

In [1] they proved that if $\alpha_1, \ldots, \alpha_s$ are real algebraic numbers which are "weakly compatible" such that $1, \alpha_1, \ldots, \alpha_s$ span a linear space of dimension $d \geq 2$ over the rationals, then for any $A < \frac{1}{d(d-1)}$ there are infinitely many square-free numbers n satisfying $||\alpha_i n|| < n^{-A}$ $(1 \leq i \leq s)$. The "weakly compatible" condition here is necessary and is always true if $\alpha_1, \ldots, \alpha_s$ are $\mathbf{Q}$-linearly independent, in which case the bound takes the shape $||\alpha_i n|| \ll n^{-1/(s(s+1))+\epsilon}$. In this generic situation of linearly independent $\alpha_1, \ldots, \alpha_s$ we can establish a much stronger result. As in [1], we can generalize to numbers $\alpha_1, \ldots, \alpha_r$ being "not very well approximable", meaning that for every $\epsilon > 0$ there are only finitely many solutions of

$$\prod_{i=1}^{r} ||q\alpha_i|| \leq q^{-1-\epsilon}$$

in positive integers q. This condition is satisfied for almost all $\alpha_1, \ldots, \alpha_r$. Our main result is that if $\alpha_1, \ldots, \alpha_r$ are not very well approximable real numbers, then there are infinitely many positive square-free integers n such that

$$||n\alpha_i|| \ll n^{-\frac{2}{3r}+\epsilon} \ (1 \leq i \leq r),$$

where the implied O-constant depends only on $\alpha_1, \ldots, \alpha_r$ and ϵ. This generalizes Heath-Brown's result under suitable assumptions to $r > 1$. Moreover, even without the restriction to square-free n no better bound than $n^{-1/r}$ would be possible, so the exponent is of the right order of magnitude in r, in contrast to any other known result on simultaneous Diophantine approximation with, say, k-th powers or primes. Whereas Baker, Brüdern and Harman used exponential sums in their proof, our method is essentially elementary and relies on lattice point counting arguments in combination with a result by Bombieri, Granville and Pintz ([3]) showing that there are few squares in arithmetic progression.

References

[1] Baker, R.C., Brüdern, J., Harman, G., *Simultaneous diophantine approximation with square-free numbers*, Acta Arith. **LXIII** (1993), 51–60.

[2] Balog, A., Perelli, A., *Diophantine approximation by square-free numbers*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **11** (1984), 353–359.

[3] Bombieri, E., Granville, A., Pintz, J., *Squares in arithmetic progression*, Duke Math. J. **66** (1992), 369–385.

[4] Harman, G., *Diophantine approximation with square-free integers*, Math. Proc. Cambridge Philos. Soc. **95** (1984), 381–388.

[5] Heath-Brown, D.R., *Diophantine approximation with square-free numbers*, Math. Z. **187** (1984), 335–344.

Multiplicative decompositions of shifted primes

Christian Elsholtz

The divisibility of shifted primes is a well studied subject, and there are important applications to cryptography. It is generally expected that there are infinitely many Sophie German primes. This means that sets A_2 satisfying $A_1A_2+1 \subset P$, where $A_1 = \{1,2\}$, can be infinitely large. Here A_1A_2 denotes the product set and P denotes the set of primes. Also, Carmichael numbers can be derived from parametrized families, for example, if $6n+1, 12n+1, 18n+1$ are prime simultaneously, then $m = (6n+1)(12n+1)(18n+1)$ is a Carmichael number. This means, with $A_1 = \{6, 12, 18\}$, sets A_2 with $A_1A_2+1 \subset P$ can be infinitely large.

In this talk we study asymptotic multiplicative decompositions of the set of shifted primes, or of shifted copies of sequences that are multiplicatively defined. We prove that there are no two sets of integers A_1, A_2, with $\min_i(|A_i|) \geq 2$, such that

$$A_1A_2 + c = P'$$

holds, where the set P' coincides with the set of primes for sufficiently large elements. Here c is any non-zero integer. Similarly, let $Q(T)$ denote the set of integers with prime factors in a set T with counting function

$$T(N) = \tau \frac{N}{\log N} + O(\frac{N}{(\log N)^2}),$$

where $0 < \tau < 1$. Then $A_1A_2 + c = Q'(T)$ (in the above sense) cannot hold.

In the additive case, the author had previously proved [1] that the set of primes P does not have an asymptotic additive decomposition into three sets, i.e. there are no three sets of integers A_1, A_2, A_3, with $\min_i(|A_i|) \geq 2$ such that $A_1 + A_2 + A_3 = P'$.

The methods of proof include Wirsing's mean value theorem, Gallagher's larger sieve, and Montgomery's large sieve, which the author used in [2] to prove upper bounds $E_k(N)$ on the number of long prime k-tuples in the interval $[1, N]$. Here k may depend on N. While for k coming close to $\frac{\log N}{\log\log N}$, the upper bound $E_k(N)$ is an extension of the upper bound $c_k \frac{N}{(\log N)^k}$, known from small sieve estimates for constant k, we use in the proof that for $k \sim (\log N)^r, r > 1$, the upper bound $E_k(N)$ is about $N^{1/2+1/(r+1)}$, i.e. saves a power of N. For more details in the case $r = 1$ see [3].

The details of the talk will appear in [4].

References

[1] C. Elsholtz, *The inverse Goldbach problem*, Mathematika 48 (2001), 151-158

[2] C. Elsholtz, *Combinatorial prime number theory - A study of the gap structure of the set of primes*, Habilitationsschrift 2002, TU Clausthal.

[3] C. Elsholtz, *Upper bounds for prime k-tuples of size* $\log N$ *and oscillations*, Arch. Math. 82 (2004), 33-39.

[4] C. Elsholtz, *Multiplicative decomposability of shifted sets*, Bull. London Math. Soc., 40 (2008), 97–107.

Prime chains and Pratt trees

Kevin Ford
(joint work with Sergei V. Konyagin, Florian Luca)

Prime chains. Impose on the set of primes a partial ordering, with $p \prec q$ if $q \equiv 1 \pmod{p}$. We study properties of the chains with respect to this partial ordering, the *prime chains*. An example is $3 \prec 13 \prec 53 \prec 107 \prec 643$.

In the special case $p_{j+1} = 2p_j + 1$ for every j, the prime chain is called a *Cunningham Chain* of length k. We study $k(p)$, the length of the longest Cunningham Chain starting with p. The prime k-tuples conjecture implies that $k(p)$ is unbounded, and assuming Artin's conjecture for primes which have 2 as a primitive root, we show that $k(p) = O(\log p)$. Unconditionally, we prove results of the type $k(p) = O((\log p)^{1-c})$ for all but $O(x^{1-d})$ primes $p \le x$, for suitable constants $c > 0, d > 0$.

We also analyze $P(x)$, the number of prime chains with $p_k \le x$ (k is variable). We prove $x(\log x)^{-0.36} \ll P(x) \ll x$, and prove an asymptotic for $P(x)$ conditional on a quantitative form of the Elliott-Halberstam conjecture. This is closely related to problems about high iterates of Euler's function [2].

Motivated by an application to the local injectivity of the Carmichael λ-function, we give upper bounds on $P(x;p)$, the number of prime chains with $p_1 = p$ and $p_k \le x$ (again, k may vary). Using a novel sieve method based on matrices of Dirichlet series, we show that $P(x;p) \ll_\varepsilon (x/p)^{1+\varepsilon}$ for every $\epsilon > 0$.

Pratt trees. The *Pratt tree* for a prime p is the structure of all odd primes which lie "below" p with respect to the above partial ordering, i.e. the tree with root node labelled p, and below p are links to the Pratt trees for odd primes q which divide $p-1$. It was first considered by Pratt [7] in connection with certificates of primality.

Let $D(p)$ be the depth (height) of the Pratt tree with root p, that is, the length of the longest chain of odd primes with $p_k = p$. For example, $D(107) = 4$. A trivial upper bound is $D(p) \le \lfloor \frac{\log p}{\log 2} \rfloor$. It has been suggested that $D(p)$ has order $\log\log p$ for almost all p [5], where the problem is connected with high iterates of Carmichael's λ-function. We prove that $D(p) \gg \log\log p$ for almost all p, and, using a high-dimensional sieve and fine analysis of averages of the singular series attached to families of prime chains, we show that $D(p) = O((\log p)^{0.9622})$ for almost all p.

Assuming that the prime factors of a random shifted prime $p - 1 \approx x$ are distributed in the same way as a random integer $n \approx x$ (the so-called Poisson-Dirichlet distribution), we are lead to a probabilistic model of Pratt trees. The model can be described in terms of a *random fragmentation* or as a *branching random walk*. Results about branching random walks (e.g., [6]) suggest that $D(p) = \mathrm{e}\log\log p + O(\log\log\log p)$ for most primes p, and that $D(p)$ is *tight* with respect to its median; i.e., there is a function $f(p)$ so that for every $\varepsilon > 0$ there is an M so that $|D(p) - f(p)| > M$ with probability $\le \varepsilon$.

All the aforementioned results will appear in the paper [4].

Local injectivity of the Carmichael λ-function. In 2006, Banks, Friedlander, Luca, Pappalardi and Shparlinski [1] conjectured that for every positive m there is an integer $n \neq m$ with $\lambda(n) = \lambda(m)$. The corresponding conjecture for Euler's function, the Carmichael conjecture, remains unproven after 100 years. In [3], we deduce this conjecture from the Extended Riemann Hypothesis for Dirichlet L-functions, and come "close" to proving this conjecture unconditionally. More precisely, if for every prime power p^a $(a \geq 1)$ there is a prime q with $p^a \| (q-1)$ and the Pratt tree for q has a certain property, then this conjecture about $\lambda(n)$ is true, and we prove the existence of such a q for $p^a \geq K$, where K is an effective (but enormous) constant. The proof uses the upper bounds for $P(x;p)$ from [4].

References

[1] W. D. Banks, J. Friedlander, F. Luca, F. Pappalardi and I. E. Shparlinski, *Coincidences in the values of the Euler and Carmichael functions*, Acta Arith. **122** (2006), 207–234.

[2] P. Erdős, A. Granville, C. Pomerance, and C. Spiro, *On the normal behavior of the iterates of some arithmetic functions*, in Analytic Number Theory, Proceedings of a conference in honor of Paul T. Bateman, Birkhäuser, Boston, 1990, 165–204.

[3] K. Ford and F. Luca, *The number of solutions of* $\lambda(x) = n$, preprint (2008).

[4] K. Ford, S. V. Konyagin and F. Luca, *Prime chains and Pratt trees*, preprint (2008).

[5] G. Martin and C. Pomerance, *The iterated Carmichael λ-function and the number of cycles of the power generator*, Acta Arith. **188** (2005), 305–335.

[6] C. McDiarmid, *Minimal positions in a branching random walk*, Ann. Appl. Prob. **5** (1995), no. 1, 128–139.

[7] V. Pratt, *Every prime has a succinct certificate*, SIAM J. Comput. **4** (1975), no. 3, 214–220.

On the negative Pell equation

Étienne Fouvry

(joint work with J. Klüners)

Consider the so–called negative Pell equation

$$(NPE(d)) \qquad x^2 - dy^2 = -1,$$

where d is a squarefree positive integer and where x and y are integer unknowns. It is well known that we can restrict to d without prime divisor $\equiv 3 \bmod 4$ and that the solvability of $(NPE(d))$ is equivalent to the fact that $\sqrt{d}$ has an odd period in its expansion in continued fraction or to the fact that $\mathbb{Q}(\sqrt{d})$ has a fundamental unit ϵ_d with its norm satisfying $N(\epsilon_d) = -1$. We prefer this last aspect since it has a rich algebraic structure. So we introduce the set

$$\mathcal{D} := \big\{ D > 0 \,;\ D \text{ is a fundamental discriminant},\ p \mid D \Rightarrow p \not\equiv 3 \bmod 4 \big\}$$

and the counting functions

$$\mathcal{D}(X) := \big| \big\{ D \in \mathcal{D} \,;\ D \leq X \big\} \big|,$$

and

$$\mathcal{D}^-(X) := \big|\big\{D \in \mathcal{D};\ D \le X,\ N(\epsilon_D) = -1\big\}\big|.$$

The asymptotic behavior of $\mathcal{D}(X)$ can be treated by classical methods, since it is very near from Landau's Theorem on sums of two squares, more precisely one has $\mathcal{D}(X) \sim c_0 X/\sqrt{\log X}$, for some positive constant c_0 $(X \to \infty)$. The corresponding question for $\mathcal{D}^-(X)$ appears much more delicate. Stevenhagen ([10]) has built a convincing probabilistic model which led him to conjecture that

$$\mathcal{D}^-(X) \sim (1-\alpha)\mathcal{D}(X)\ (X \to \infty),$$

where $\alpha := \prod_{j=1}^{\infty}(1+2^{-j})^{-1} = \ .4194224\cdots$. We prove

Theorem 1. *([2], [3]) As $X \to \infty$, we have the inequalities*

$$\big(\frac{5\alpha}{4} - o(1)\big)\,\mathcal{D}(X) < \mathcal{D}^-(X) < (2/3 + o(1))\,\mathcal{D}(X).$$

We now give some ideas of the proof. Let C_D and Cl_D respectively be the narrow and the ordinary ideal class group of the ring of integers of $\mathbb{Q}(\sqrt{D})$. Let $\mathrm{rk}_{2^k}(G)$ be the 2^k–rank of the finite abelian group G. Recall first that

$$N(\epsilon_D) = -1 \iff \mathrm{C}_D = \mathrm{Cl}_D.$$

To obtain the upper bound of Theorem 1, we use the implication

$$\mathrm{C}_D = \mathrm{Cl}_D \Rightarrow \mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{Cl}_D),$$

and for the lower bound the implications

$$\mathrm{rk}_4(\mathrm{C}_D) = 0 \Rightarrow \mathrm{C}_D = \mathrm{Cl}_D,$$

and

$$\big(\mathrm{rk}_4(\mathrm{C}_D) = \mathrm{rk}_4(\mathrm{Cl}_D) = 1 \text{ and } \mathrm{rk}_8(\mathrm{C}_D) = 0\big) \Rightarrow \mathrm{C}_D = \mathrm{Cl}_D.$$

To detect the values of $2^{\mathrm{rk}_4(\mathrm{C}_D)}$ and of $2^{\mathrm{rk}_4(\mathrm{Cl}_D)}$ (and of the corresponding moments $2^{k\,\mathrm{rk}_4(\mathrm{C}_D)}$ and $2^{k\,\mathrm{rk}_4(\mathrm{Cl}_D)}$) we interpret rather old results of Reichardt, Redei and Scholz ([5], [6], [7], [8], [9],...) in terms of sums of Jacobi symbols, or of quartic symbols associated to the factorizations of D. The oscillations of these characters are controlled in a classical way. The main term gives birth to interesting combinatorial questions which can be solved by geometric considerations in characteristic 2, inspired by [4] and already exploited in [1]. This approach is strong enough to give the distribution law of the function $D \in \mathcal{D} \mapsto (\mathrm{rk}_4(\mathrm{C}_D), \mathrm{rk}_4(\mathrm{Cl}_D))$.

Some partial results are also given for the distribution law of the function $D \in \mathcal{D} \mapsto \mathrm{rk}_8(\mathrm{C}_D)$.

References

[1] E. Fouvry and J. Klüners, *On the 4–rank of class groups of quadratic number fields*, Inv. Math., **167**, 455–513, (2007).

[2] E. Fouvry and J. Klüners, *On the negative Pell equation*, Ann. of Math., (to appear), (2007).

[3] E. Fouvry and J. Klüners, *The parity of the period of the continued fraction of $\sqrt{d}$*, preprint, (2008).

[4] D.R. Heath–Brown, *The size of Selmer groups for the congruent number problem, II* Inv. Math., **118**, 331–370, (1994).
[5] L. Redei, *Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren invarianten der absoluten Klassengruppe im quadratischen Zahlkörper*, J. Reine Angew. Math. **171**, 55–60, (1934).
[6] L. Redei, *Eine obere Schranke der Anzahl der durch vier teilbaren invarianten der absoluten Klassengruppe im quadratischen Zahlkörper,* J. Reine Angew. Math. **171**, 61–64, (1934).
[7] L. Redei, *Über die Pellsche Gleichung* $t^2 - du^2 = -1$, J. Reine Angew. Math. **173**, 193–221, (1935).
[8] L. Redei and H. Reichardt, *Die Anzahl der durch* 4 *teilbaren Invarianten der Klassengruppe eines beliebigen quadraticshen Zahlkörpers,* J. Reine Angew. Math. **170**, 69–74, (1933).
[9] A. Scholz, *Über die Lösbarkeit der Gleichung* $t^2 - Du^2 = -4$, Math. Z. **39**, 95–111 (1935).
[10] P. Stevenhagen, *The number of real quadratic fields with units of negative norms,* Experiment. Math., **2**, 121–136, (1993).

Sifting short intervals

John Friedlander

We report on some very old work of our own and on some recent developments of it obtained in joint work with Henryk Iwaniec (see [1] and the references therein for the former and [2] for the latter.)

The Brun sieve gives the bound

$$\pi(x) - \pi(x-w) \ll w/\log w$$

for the number of primes in the short interval $(x-w, x]$, and for $w > x^{\varepsilon}$ this gives the expected order but not for shorter intervals. We investigate the question of how short an interval one can successfully treat if one asks only for results valid in intervals $(y-w, y]$ for most y in $(x, 2x)$.

Proposition 1. *Let* λ_d, $1 \le d \le D$ *be real with* $\lambda_1 = 1$, $|\lambda_d| \le 1$. *Let* $A > 0$, $1 \le w \le x/D^2(\log x)^{2A+8}$ *and*

$$\theta_n = \sum_{d|n} \lambda_d, \quad \gamma_d = d^2 \sum_{\substack{h=1 \\ (h,d)=1}}^{\infty} \frac{1}{h^2} \sin^2\Big(\frac{\pi h w}{d}\Big).$$

Then

$$\int_x^{2x} \Big| \sum_{y-w<n\le y} \theta_n - w \sum_d \frac{\lambda_d}{d} \Big|^2 dy = \frac{2x}{\pi^2} \sum_d \gamma_d \Big(\sum_{m \equiv 0 \bmod d} \frac{\lambda_m}{m} \Big)^2 + O(xw(\log x)^{-A}).$$

We apply proposition 1 to the situation where the λ_d are upper or lower bound beta-sieve weights for suitable β. In this case the left-hand side is just the mean square $\int_x^{2x} |R(D,y)|^2\, dy$ for the remainder encountered in sieving the interval $(y-w, y]$ by the primes $p < z$, and the main term on the right can be shown to satisfy the bound $\ll xw(\log z)^{-1}$. As a result we obtain

Proposition 2. *Let $2 \le z \le x^{1/20}$, $w = \eta(x)\log z$ where $\eta(x) \to \infty$ as $x \to \infty$. Then, denoting $P(z) = \prod_{p<z} p$, we have*

$$\sum_{\substack{y-w<n\le y \\ (n,P(z))=1}} 1 \asymp \frac{w}{\log z}$$

for all y with $x < y \le 2x$ apart from a set of measure $O(x\eta(x)^{-1})$.

Note that the intervals in question are the shortest ones for which one could reasonably expect such a result to hold.

Taking $z = x^{1/20}$ we find that the above intervals have some integers with no more than 19 prime factors and satisfy

$$\pi(y) - \pi(y-w) \ll \frac{w}{\log x}.$$

The question of 'suitable β' has now been studied in greater detail and as a result the number of prime factors can be reduced from 19 to 4. Then, using also deep estimates for bilinear forms of Kloosterman fractions, it can be further reduced to 3.

References

[1] J.B. Friedlander. Moments of sifted sequences. Math. Annalen 267 (1984) 101–106.
[2] J.B. Friedlander and H. Iwaniec, Sieve methods (provisional title), in preparation.

Gaps between primes

Dan Goldston

In early 2005, J. Pintz, C. Y. Yıldırım and I [1] proved that

$$\liminf_{n\to\infty} \left(\frac{p_{n+1} - p_n}{\log p_n} \right) = 0. \tag{1}$$

Thus there are infinitely often two primes closer than any fraction of the average spacing between primes. More precisely, we later proved

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{(\log p_n)^{1/2}(\log\log p_n)^2} < \infty. \tag{2}$$

The method used to prove these results involves two steps: approximating prime tuples with truncated divisor sums, and then detecting primes using a positivity argument.

Let n be a natural number and consider the k-tuple

$$(n + h_1, n + h_2, \ldots, n + h_k), \tag{3}$$

where $\mathcal{H} = \{h_1, h_2, \ldots, h_k\}$ is a set composed of distinct non-negative integers. If every component of the tuple is a prime we call this a *prime tuple*. In general, the tuple in (3) can be a prime tuple for more than one n only if $\nu_{\mathcal{H}}(p) < p$ for all primes p, where $\nu_{\mathcal{H}}(p)$ is the number of distinct residue classes modulo p occupied by the integers in $\mathcal{H}$. If this condition holds we say that $\mathcal{H}$ is *admissible*

and we call the tuple (3) an *admissible tuple*. It is a long-standing conjecture of Hardy and Littlewood that admissible tuples will infinitely often be prime tuples, and further there is an asymptotic formula for the number of such tuples given by

$$\big|\{n \le N : (n+h_1, n+h_2, \dots, n+h_k) \text{ is a prime tuple}\}\big| \sim \mathfrak{S}(\mathcal{H})\frac{N}{(\log N)^k}, \tag{4}$$

where

$$\mathfrak{S}(\mathcal{H}) := \prod_p \left(1-\frac{1}{p}\right)^{-k}\left(1-\frac{\nu_{\mathcal{H}}(p)}{p}\right) \tag{5}$$

is the singular series associated with $\mathcal{H}$.

In our method the information on primes we make use of is their distribution in arithmetic progressions. Let

$$\theta(N;q,a) = \sum_{\substack{n\le N\\ n\equiv a(\mathrm{mod}\, q)}} \theta(n), \quad \text{where } \theta(n) = \begin{cases} \log n, & \text{if } n \text{ is prime,}\\ 0, & \text{otherwise.}\end{cases} \tag{6}$$

The Bombieri-Vinogradov theorem states that for any $A > 0$ there is a $B = B(A)$ such that, for $Q = N^{\frac{1}{2}}(\log N)^{-B}$,

$$\sum_{q\le Q}\max_{\substack{a\\(a,q)=1}}\left|\theta(N;q,a)-\frac{N}{\phi(q)}\right| \ll \frac{N}{(\log N)^A}. \tag{7}$$

More generally, we say that the primes have an *admissible level of distribution* ϑ (or *satisfy a level of distribution* ϑ) if (7) holds for any $A > 0$ and any $\epsilon > 0$ with

$$Q = N^{\vartheta-\epsilon}. \tag{8}$$

Elliott and Halberstam conjectured that the primes have the maximal admissible level of distribution 1, while by the Bombieri-Vinogradov theorem we have immediately that 1/2 is an admissible level of distribution for the primes.

We can now state our first result: *If* the primes satisfy a level of distribution $\vartheta > \frac{1}{2}$ then there is an absolute constant $M(\vartheta)$ for which

$$p_{n+1} - p_n \le M(\vartheta), \quad \text{for infinitely many } n. \tag{9}$$

More generally, we proved the following result related to the prime tuple conjecture.

Theorem 1. *Suppose the primes have level of distribution $\vartheta > 1/2$. Then there exists an explicitly calculable constant $C(\vartheta)$ depending only on ϑ such that any admissible k-tuple with $k \ge C(\vartheta)$ contains at least two primes infinitely often. Specifically, if $\vartheta \ge 0.971$, then this is true for $k \ge 6$.*

Since the 6-tuple $(n, n+4, n+6, n+10, n+12, n+16)$ is admissible, the Elliott-Halberstam conjecture implies that

$$\liminf_{n\to\infty}(p_{n+1}-p_n) \le 16. \tag{10}$$

The approximation we use for detecting primes in tuples is

$$\Lambda_R(n;\mathcal{H},\ell)=\frac{1}{(k+\ell)!}\sum_{\substack{d\mid P_{\mathcal{H}}(n)\\ d\le R}}\mu(d)\left(\log\frac{R}{d}\right)^{k+\ell}, \tag{11}$$

where $|\mathcal{H}|=k$, and $P_{\mathcal{H}}(n)=(n+h_1)(n+h_2)\cdots(n+h_k)$. The parameter ℓ is critical to the success of the method. To detect primes we square our approximation (11) to obtain a non-negative approximations (since Λ_R is often negative), and then compute

$$\sum_{n\le N}\Lambda_R(n;\mathcal{H},\ell)^2\sim\frac{1}{(k+2\ell)!}\binom{2\ell}{\ell}\mathfrak{S}(\mathcal{H})N(\log R)^{k+2\ell}, \tag{12}$$

valid $R\ll N^{\frac12}(\log N)^{-B(M)}$ and $R,N\to\infty$, and

$$\sum_{n\le N}\Lambda_R(n;\mathcal{H},\ell)^2\theta(n+h_i)\sim\frac{2}{(k+2\ell+1)!}\binom{2\ell+1}{\ell}\mathfrak{S}(\mathcal{H})N(\log R)^{k+2\ell+1}. \tag{13}$$

valid for $R\ll N^{\frac{\vartheta}{2}-\epsilon}$, and $R,N\to\infty$, where ϑ is an admissible level of distribution of primes in arithmetic progressions. The singular series $\mathfrak{S}(\mathcal{H})$ is the same as in the Hardy-Littlewood conjecture (4) and is positive.

Here is how we prove there are two primes in tuples if $\vartheta>\frac12$. Using the two asymptotic formulas above we compute

(14)

$$\begin{aligned}\mathcal{S}:&=\sum_{n=N+1}^{2N}\left(\sum_{i=1}^{k}\theta(n+h_i)-\log 3N\right)\Lambda_R(n;\mathcal{H},\ell)^2\\ &\sim\left(\frac{2k}{k+2\ell+1}\frac{2\ell+1}{\ell+1}\log R-\log 3N\right)\frac{1}{(k+2\ell)!}\binom{2\ell}{\ell}\mathfrak{S}(\mathcal{H})N(\log R)^{k+2\ell}.\end{aligned}$$

The tuple $\mathcal{H}$ will contain at least two primes if $\mathcal{S}>0$, since here $\theta(n+h_i)<\log 3N$ and every term in S will be negative unless the sum over i sometimes contains two non-zero terms. But $S>0$ when, letting $R=N^{\vartheta/2-\epsilon}$,

$$\frac{k}{k+2\ell+1}\frac{2\ell+1}{\ell+1}\vartheta>1, \tag{15}$$

and if $k,\ell\to\infty$ with $\ell=o(k)$, then the left-hand side has the limit 2ϑ, and thus (15) holds for any $\vartheta>1/2$ if we choose k and ℓ appropriately depending on ϑ. This proves the first part of Theorem 1. If $\vartheta>20/21$, we see that (15) holds with $\ell=1$ and $k=7$, which proves that every 7 tuple has two primes in it infinitely often assuming this level of distribution. Finally, these results just fail in the unconditional case when $\vartheta=\frac12$, but one can pick up an extra factor of h if we sum over all k-tuples with $1\le h_1,h_2,\dots,h_k\le h$ and use

$$\sum_{1\le h_1,h_2,\dots,h_k\le h}\Lambda_R(n;\mathcal{H}_k,\ell)^2 \tag{16}$$

as the weight in $\mathcal{S}$. If $h=\epsilon\log N$ we then gain enough to prove (1).

References

[1] D. A. Goldston, J. Pintz and C. Y. Yıldırım, *Primes in Tuples I,* Annals of Math. to appear.

Indefinite Quadratic Forms and the Multivariate Central Limit Theorem

Friedrich Götze

(joint work with Gregory Margulis, Andrei Zaitsev)

Distribution of Values of Indefinite Irrational Forms. Let $Q[x]$ denote an indefinite *irrational* form with signature (p,q), $\quad q \geq 3$, and dimension $d = p+q \geq 5$. Consider a finite d-dimensional box $I_s := [-\sqrt{s}, \sqrt{s}]^d$. The number of lattice vectors $m \in \mathbb{Z}^d \cap I_s$ in this box such that the values of the quadratic form $Q[m]$ are contained in $[a, a+\delta]$, $\quad a \in \mathbb{R}$, $\delta > 0$ fixed, were intensively studied for box sizes going to infinity in connection with the so called Oppenheim problem. The distribution of values of indefinite forms on such boxes of integer vectors are locally uniformly distributed for all dimensions $d \geq 5$. More precisely, as s tends to infinity,

$$\Delta_s^-(\delta) := \frac{\sharp\{m \in I_s \cap \mathbb{Z}^d : \, a \leq Q[m] \leq a+\delta\}}{\mathrm{vol}\{x \in I_s : \, a \leq Q[x] \leq a+\delta\}} - 1 = o(1)$$

This has been shown in [EMM98] for $q \geq 3$ with an non effictive error term based on ergodic limit theorems. Effective error bounds depending on the diophantine properties of the coefficients of $Q[x]$ have been shown in [BG99a] for $d \geq 9$. The analogous problem of local uniformity of the distribution of *irrational* positive definite forms, i.e.

$$\Delta_s^+(\delta) := \frac{\sharp\{m \in \mathbb{Z}^d : \, s \leq Q[m] \leq s+\delta\}}{\mathrm{vol}\{x \in \mathbb{R}^d \, s \leq Q[x] \leq s+\delta\}} - 1 = o(1)$$

(as s tends to infinity) has been proved in [Göt04] for $d \geq 5$ using effective error bounds. (See also [BG97] for $d \geq 9$).

Combining the methods of the latter papers and quantitative arguments using uniform distribution on unipotent subgroups, effective error bounds are derived for irrational indefinite forms and $\Delta_s^-(\delta), d \geq 5$, as s tends to infinity, in a recent paper by Götze, Margulis (2008).

The methods used rely on inequalities for theta sums and effective bounds from the geometry of numbers for convex bodies $B_{s,t}$ defined by norms of type $\|m - t\,Qn\|s^{1/2} + s^{-1/2}\|n\|$ on $\Lambda = \mathbb{Z}^d \times \mathbb{Z}^d$. This norm may be described as the Euclidean norm of an element of a tranformed lattice $\Lambda_{s,t}$ obtained from Λ by the action of a representation of diagonal and unipotent subgroups of $SL_2(\mathbb{R})$. The bounds are expressed as averages over a compact subgroup of $SL_2(\mathbb{R})$ of the reciprocal powers of the maximal volume of d-dimensional sublattices of $\Lambda_{s,t}$. Effective error bounds are then obtained by a recursion $s \to 2s$ of such averages involving harmonic analysis bounds for integrals over the circle.

The resulting bounds are based on diophantine appoximation of the coefficient matrix Q and allow for example to derive efficient bounds for the size of nontrivial solutions $m \in \mathbb{Z}^d$ of diophantine inequalities of the type $|Q[m]| < \epsilon$ in terms of of $\epsilon^{-\kappa}$ for some $\kappa > 2$.

The multivariate Central Limit Theorem for Quadratic Forms. A further application of these analytic methods concerns the long standing problem of determining optimal rates of convergence in the multivariate central limit theorem in $\mathbb{R}^d, d \geq 5$ for quadratic forms.

Let $X, X_1, \ldots X_N \in \mathbb{R}^d$ denote i.i.d. random vectors in $\mathbb{R}^d, d \leq \infty$ such that $\mathbf{E}X = 0, \quad \beta_4 = \mathbf{E}|X|^4 < \infty$. Consider the distribution of the normalized sum $S_N := N^{-1/2}(X_1 + \ldots + X_N)$, assuming that S_N converges weakly to a nondegerate multivariate Gaussian random vector S on $\mathbb{R}^d$. Assume that $Q : \mathbb{R}^d \to \mathbb{R}^d$ is a symmetric operator with $\ker \mathrm{Q} = 0$. We study the distribution the quadratic form $Q[x] := \langle Qx, x\rangle$ applied to S_N.

In a recent joint paper with A. Zaitsev it shown that the optimal rate of convergence in the central limit theorems for quadratic forms is of optimal order $O(n^{-1})$ for all dimensions $d \geq 5$. For these dimensions we have more precisely:

$$\begin{aligned} \Delta_N \quad := \quad & \sup_r |\mathbb{P}\{Q[S_N] \leq r\} - \mathbb{P}\{Q[S] \leq r\}| = \mathcal{O}\left(N^{-1}\right), \quad \text{and} \\ & \sup_r \mathbb{P}\{Q[S_N] \in [r, r+\epsilon]\} = \mathcal{O}(\epsilon + N^{-1}) \end{aligned}$$

The implied bounds of Δ_N are effective for $5 \leq d < \infty$ and ineffective for $d = \infty$.

For the application to probability, that is approximations for distribution functions rather then concentration bounds, the uniform avarages over the unipotent resp. circle subgroup of $SL_2(\mathbb{R})$ mentioned above have to be replaced by integration over the harmonic measure on $\mathbb{R}$ using reparametrization and the geometry of $SL_2(\mathbb{R})$, combined with addaptions of transfer results from probability to number theory as developed in [BG96, BG97, BG99b].

References

[BG96] Bentkus, V., and Götze, F., *Optimal rates of convergence in the CLT for quadratic forms*, Ann. Prob., **1**, 466–490, 1996.

[BG97] Bentkus, V. and F. Götze. *On the lattice point problem for ellipsoids.* Acta Arith., 80(2):101–125, 1997.

[BG97] Bentkus, V. and F. Götze. *Uniform rates of convergence in the CLT for quadratic forms in multidimensional spaces.* Probab. Theory Related Fields, 109(3):367–416, 1997.

[BG99a] Bentkus, V. and F. Götze. *Lattice point problems and distribution of values of quadratic forms.* Ann. of Math. (2), 150(3):977–1027, 1999.

[BG99b] Bentkus, V. and F. Götze. *Optimal bounds in non-Gaussian limit theorems for U-statistics.* Ann. Probab., 27(1):454–521, 1999.

[Göt04] F. Götze. *Lattice point problems and values of quadratic forms.* Invent. Math., 157(1):195–226, 2004.

[Mar97] G. A. Margulis. *Oppenheim conjecture.* In *Fields Medallists' lectures*, volume 5 of *World Sci. Ser. 20th Century Math.*, pages 272–327. World Sci. Publishing, River Edge, NJ, 1997.

[EMM98] Eskin, A., G. Margulis and S. Mozes. *Upper bounds and asymptotics in a quantitative version of the Oppenheim conjecture.* Ann. of Math. (2), 147(1):93–141, 1998

The Ideal Sieve

Sidney Graham
(joint work with Hugh Montgomery)

Our goal is to construct extremal upper and lower bound sieves in certain simple contexts. Let $\mathcal{A}$ be a finite set of integers, and suppose that each $n \in \mathcal{A}$ is equipped with a non-negative weight w_n. Let $\mathcal{P}$ be a finite set of primes and define P to be the product of all primes in $\mathcal{P}$. A sieve is a method for deriving upper or lower bounds for

$$S_1 = \sum_{\substack{n\in\mathcal{A}\\(n,P)=1}} w_n,$$

given information about the sums

$$W_d = \sum_{\substack{n\in\mathcal{A}\\d|n}} w_n.$$

The estimates of the W_d take the form

$$\frac{f(d)}{d}X - R_d^- \le W_d \le \frac{f(d)}{d}X + R_d^+$$

for $d|P$, where $f(d)$ is a non-negative multiplicative function. In practice, it is usually the case that there is some z for which the quantities R_d are small (at least on average) for $d < z$. We idealize this situation by assuming that $R_d^{\pm} = 0$ for $d < z$ and $R_d = \infty$ for $d \ge z$. By homogeneity, we may normalize to $X = 1$.

We say λ_d is an *upper bound sifting function* if

$$\sum_{d|n} \lambda_d \ge \begin{cases} 1 & \text{if } n = 1,\\ 0 & \text{otherwise.}\end{cases} \tag{1}$$

Similarly, we say that λ_d is a *lower bound sifting function* if the inequality in (1) is reversed. These definitions may also be expressed in terms of $\theta_n := \sum_{d|n} \lambda_d$. By the fundamental duality theorem of linear programming,

$$\max_{w_n} S_1 = \min_{\lambda_d\in\mathcal{L}^+} \sum_{d|P} \frac{\lambda_d f(d)}{d}, \text{ and } \min_{w_n} S_1 = \max_{\lambda_d\in\mathcal{L}^-} \sum_{d|P} \frac{\lambda_d f(d)}{d},$$

where the w_n run over all choices that satisfy $W_d = f(d)/d$, and $\mathcal{L}^+$ ($\mathcal{L}^-$) denotes the set of all upper (lower) bound sifting functions. Among such sifting functions, we seek those that minimize (or maximize) $\sum_{d|P} \lambda_d f(d)/d$.

For a given $r|P$, let

$$S_r = \sum_{\substack{n\in\mathcal{A}\\(n,P=r)}} w_n.$$

Then for any $d|P$,

$$W_d = \frac{f(d)}{d} = \sum_{r|P/d} S_{rd}.$$

Using Möbius inversion, we may also express the S_r in terms of the A_d. We now rephrase our problem in terms of the S_r, and we ignore the set $\mathcal{A}$ and the weights w_n. We say that a set $\{S_r : r|P\}$ is *admissible* if $S_r \geq 0$ for all $r|P$ and if $\sum_{r|P/d} S_{rd} = \frac{f(d)}{d}$ for all $d|P, d \leq z$. Our goal is to identify extremal λ_d and companion S_r.

We follow Selberg [1, Section 13] in focusing on the following special case. Let R be a positive integer, and suppose that all $p \in \mathcal{P}$ satisfy $z^{1/(R+1)} < p \leq z^{1/R}$. We also stipulate that there is some constant κ such that

$$\sum_{p|P} \frac{f(p)}{p} \sim \kappa, \text{ and } \sum_{p|P} \frac{f(p)^2}{p^2} = o(1)$$

as $z \to \infty$. Selberg proved that the extremal λ_d. depend only on $\omega(d)$. We give another proof of this fact. Our proof has two advantages over Selberg's. The first is that we give a procedure for identifying extremal S_d. The second is that our proof gives a more efficient procedure for finding the extremal λ_d.

Since the extremal λ_d depend only on $\omega(d)$, so do the extremal θ_d. Write $\theta(\ell) = \theta_d$ when $\omega(d) = \ell$. When $R = 1$, the optimal lower bound θ is $\theta(\ell) = 1 - \ell$. We prove that this is optimal by taking $S_1 = 1 - \kappa$, $S_p = f(p)/p$, and $S_d = 0$ otherwise. When $R = 2$, the optimal upper bound θ is given by

$$\theta(\ell) = \left(1 - \frac{\ell}{r}\right)\left(1 - \frac{\ell}{r+1}\right),$$

where $r = [\kappa + 1]$. We prove that this is optimal by taking the admissible set with $S_1 = 1 - 2\kappa/r + \kappa^2/(r(r+1))$,

$$S_d = \begin{cases} \frac{f(d)}{d}\frac{(r-1)!(r-\kappa)}{\kappa^{r-1}} & \text{if } \omega(d) = r, \\ \frac{f(d)}{d}\frac{(r-1)!(\kappa+1-r)}{\kappa^{r-1}} & \text{if } \omega(d) = r+1, \end{cases}$$

and 0 otherwise.

A natural quantiy to consider is v_R, which is defined as the least upper bound of those κ for which there is a non-trivial lower bound sieve. Our calculations show tht t $v_1 = v_2 = 1$, and $v_3 = v_4 = 2$, and $v_5 = 3.117\ldots$. Selberg proved that $\left[\frac{R+1}{2}\right] \leq v_R < R$ for all R, and he conjectured that $v_R \sim \frac{1}{2}R$. We have done computer calculations for v_R for $R \leq 39$, and our computations support Selberg's conjecture.

References

[1] A. Selberg, "Lectures on Sieves," in: *Collected Papers Vol. II*, pp. 65–247, Springer, 1992.

Growth in $\mathbf{SL_3}$ and elsewhere

Harald A. Helfgott

People mean different things by growth.

1 *Growth in graphs.* Let Γ be a graph. How many vertices can be reached from a given vertex in a given amount of time?
2 *Growth in infinite groups.* Let A be a set of generators of an infinite group G. Let $B(t)$ be the number of elements that can be expressed as products of at most t elements of A. How does $B(t)$ grow as $t \to \infty$?
3 *Random walks in groups.* Let A be a set of generators of a finite group G. Start with $x = 1$, and, at each step, multiply x by a random element of A. After how many steps is x close to being equidistributed in G?
4 *More on growth in graphs.* Let Γ be a graph. Consider its adjacency matrix. What lower bounds can one give for the difference between its two largest eigenvalues?
5 *Growth in arithmetic combinatorics.* Let G be an abelian group. Let $A \subset G$. How large is $A + A$ compared to A, and why? In general, let G be a group. Let $A \subset G$. How large[1] is $A \cdot A \cdot A$ compared to A, and why?

Question (5) has been extensively studied in the abelian setting. Some time ago, I started studying it for non-abelian groups, and proved [He] that every set of generators of $G = \mathrm{SL}_2(\mathbb{F}_p)$ grows: $|A \cdot A \cdot A| > |A|^{1+\epsilon}$, $\epsilon > 0$, provided that $|A| < |G|^{1-\delta}$, $\delta > 0$. (Here $|S|$ is the number of elements of a set S.) This answers question (1) immediately in the case of the Cayley graph of $\mathrm{SL}_2(\mathbb{F}_p)$; the bounds obtained are strong enough to constitute the first proved case of Babai's conjecture. Questions (3) and (4) are closely related to each other, and somewhat more indirectly to (1) and (5); my result on (5) for SL_2 gives non-trivial bounds for (3) and (4). In the interim, Bourgain and Gamburd ([BG]) have shown how to obtain rather good bounds for (3) and (4) from what I got on (5).

I have now proved for SL_3 what I proved for SL_2.

Main Theorem. *Let $G = \mathrm{SL}_3$. Let $K = \mathbb{Z}/p\mathbb{Z}$, p a prime. Let $A \subset G(K)$ be a set of generators of $G(K)$.*

Suppose $|A| < |G(K)|^{1-\delta}$, $\delta > 0$. Then

$$|A \cdot A \cdot A| \gg |A|^{1+\epsilon},$$

where $\epsilon > 0$ and the implied constant depend only on δ.

The proof is entirely elementary. The tools - such as they are - come from arithmetic combinatorics, and, indeed, part of the standard arithmetic-combinatorial toolbox has had to be rethought in the process. At the same time, the structure of groups of Lie type is now in the forefront, and some links with the techniques used in the study of growth in infinite groups are becoming clearer.

[1] In the non-abelian case, there are technical reasons why it makes more sense to consider $A \cdot A \cdot A$ rather than $A \cdot A$. The product $A \cdot A$ could be small "by accident".

References

[BG] J. Bourgain and A. Gamburd, Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$, *Ann. of Math.* **167**, 625–642.

[He] H. A. Helfgott, Growth and generation in $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$, *Ann. of Math.* **167** (2008), 601–623.

Zeros of Cubic and Quartic Forms

D.R. Heath-Brown

Let $F(\mathbf{x}) = F(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$ be a form of degree d. We are interested in the following two questions. Under what circumstances can we assert that F must have a non-trivial zero in $\mathbb{Z}^n$? How does the counting function

$$N(B) := \#\{\mathbf{x} \in \mathbb{Z}^n : F(\mathbf{x}) = 0, \max |x_i| \le B\}$$

behave as $B \to \infty$?

When F is quadratic the first question is answered by the Hasse-Minkowski Theorem:- F has a non-trivial zero in $\mathbb{Z}^n$ if and only if there is a non-trivial zero over $\mathbb{R}$ and over each p-adic field $\mathbb{Q}_p$. (In the latter case we say F has zeros everywhere locally.) As to the second question, for non-singular quadratics F we have $N(B) \sim c_F B^{n-2}$ for a suitable positive constant c_F, whenever F is indefinite and $n \ge 5$. (For $n = 3$ or 4 a modified asymptotic formula holds.)

When F has higher degree we have fairly good understanding only for diagonal forms. When $d = 3$ the form will always have non-trivial zeros in $\mathbb{Z}^n$ for $n \ge 7$ (see Baker [1]), while for $d = 4$ and $n \ge 12$ there are non-trivial zeros in $\mathbb{Z}^n$ if and only if F has zeros everywhere locally. (This follows from work of Vaughan [11]).

For non-diagonal forms one has the following theorem of Birch [2].

Theorem. *If F is non-singular, with $n \ge 1 + (d-1)2^d$, then*

$$N(B) = c_F B^{n-d} + o(B^{N-d}).$$

Here the constant c_F is positive if and only if F has zeros everywhere locally.

For $d = 3$ this requires $n \ge 17$. However results of Hooley [8], [9] show that $n \ge 9$ is enough. Moreover the local conditions are satisfied as soon as $n \ge 10$, see Lewis [10]. Indeed there are forms in 9 variables for which the local conditions are not satisfied.

The situation for $d = 4$ is less satisfactory. Birch's result requires $n \ge 49$, and it is only recently that there has been any progress in improving this. Browning and Heath-Brown [3] have succeeded in showing that $N(B) \gg B^{n-4}$ for non-singular forms that have solutions everywhere locally, as soon as $n \ge 41$. However there remains the problem of proving the existence of p-adic points. Brauer showed in general that for every degree d there exists an n_d such that F has non-trivial p-adic solutions whenever $n \ge n_d$. Unfortunately the proof uses multiply nested inductions which lead to value for n_d which is "not even astronomical". A very

much neater form of the argument has been given by Wooley [12], which shows that

$$n > d^{2^d}$$

suffices, but even this is rather large. Recent work by the author [7] allows $n_4 = 9145$, and indeed for $p \geq 11$ there are p-adic solutions as soon as $n \geq 121$.

One can also ask what happens if we drop the non-singularity condition. Here there are examples of the type

$$F(\mathbf{x}) = x_1 G_1(x_1, \ldots, x_n) + x_2 G_2(x_1, \ldots, x_n)$$

for which any vector $(0, 0, a_2, \ldots, a_n)$ is a solution. For such forms we will have $N(B) \gg B^{n-2}$ so that the growth rate cannot be of the form described by Birch's Theorem. In the case of cubic forms Davenport [4] circumvented this difficulty, by classifying forms as "geometrically good" or "geometrically bad". He was able to show that cubic forms which are geometrically bad have a nontrivial zero in $\mathbb{Z}^n$ for any n. For geometrically good cubic forms he showed that $N(B) \sim cB^{n-3}$ with a positive c, as soon as $n \geq 16$. Hence any cubic form in $n \geq 16$ variables has a non-trivial integer zero, whether the form is bad or good.

Recent work of the author [6] improves this by allowing any $n \geq 14$. The proof builds on Davenport's ideas, but estimates the exponential sums via van der Corput's inequality in certain cases.

One might ask whether any analogous statements can be proved for quartic forms. However not even the assumption that the form has *non-singular* zeros everywhere locally is enough to ensure the existence of a non-trivial integer solution, no matter how large one takes n. This is shown by the example

$$F(\mathbf{x}) = x_1^4 - 17x_2^4 - 2(x_3^2 + x_4^2 + \ldots + x_n^2)^2,$$

which has non-singular solutions over $\mathbb{R}$ and over every $\mathbb{Q}_p$, as soon as $n \geq 6$. However there is only the trivial solution in $\mathbb{Z}$. Underlying this example is the fact that the curve $2z^2 = x^4 - 17y^4$ is a counter-example to the Hasse Principle. The above form F occurs in recent work by Dietmann and Elsholtz [5], but may be older.

References

[1] R.C. Baker, Diagonal cubic equations. II. *Acta Arith.,* 53 (1989), 217–250.
[2] B.J. Birch, Forms in many variables. *Proc. Roy. Soc. Ser. A,* 265 (1961/1962), 245–263.
[3] T.D. Browning and D.R. Heath-Brown, Rational points on quartic hypersurfaces. *J. Reine Angew. Math.,* (to appear).
[4] H. Davenport, Cubic forms in sixteen variables. *Proc. Roy. Soc. Ser. A,* 272 (1963), 285–303.
[5] R. Dietmann and C. Elsholtz, Sums of two squares and a power. (In preparation).
[6] D.R. Heath-Brown, Cubic forms in 14 variables. *Invent. Math.,* 170 (2007), 199–230.
[7] D.R.Heath-Brown, Zeros of p-adic forms. (In preparation)
[8] C. Hooley, On nonary cubic forms. *J. Reine Angew. Math.,* 386 (1988), 32–98.
[9] C. Hooley, On nonary cubic forms. III. *J. Reine Angew. Math.,* 456 (1994), 53–63.
[10] D.J. Lewis, Cubic homogeneous polynomials over p-adic number fields. *Ann. of Math.,* (2), 56 (1952), 473–478.
[11] R.C. Vaughan, A new iterative method in Waring's problem. *Acta Math.,* 162 (1989), 1–71.

[12] T.D. Wooley, On the local solubility of Diophantine systems. *Compositio Math.,* 111 (1998), 149–165.

The horizontal distribution of zeros of the derivative of the Riemann zeta function

Christopher Hughes

(joint work with Eduardo Dueñez, David W. Farmer, Sara Froehlich, Francesco Mezzadri, Toan Phan)

Information on the horizontal distribution of the zeros of the the derivative of the Riemann zeta function yields information on the zeros of the zeta function itself. For example showing that there are no non-trivial zeros to the left of the critical line would imply the Riemann Hypothesis. Therefore it is of interest to study their distribution.

We adopt the m^+ and m^- notation due to Soundararajan. Let $N_1(T)$ denote the number of non-trivial zeros of $\zeta'(s)$ up to height T. Soundararajan [6] defined

$$m^+(x) = \limsup_{T\to\infty} \frac{1}{N_1(T)} \# \left\{ \rho' \ : \ \zeta'(\rho') = 0 \ , \ 0 < \Im(\rho') \leq T \ , \ \Re(\rho') \leq \frac{1}{2} + \frac{x}{\log T} \right\}$$

and $m^-(x)$ defined similarly, but with $\liminf$.

He conjectured that $m^+(x) = m^-(x) =: m(x)$ for all x, and that $m(x)$ is a continuous function which is 0 for $x \leq 0$ and tends to 1 as $x \to \infty$.

Some results were already known about the m, m^+, and m^- functions, the most famous of which is Speiser's Lemma [7]. This states that the Riemann Hypothesis is equivalent to there being no non-real zeros of $\zeta'(s)$ lying to the left of the critical line, $\Re(s) = 1/2$. This clearly implies $m(x) = 0$ for $x < 0$, and if almost all the zeta zeros are simple (it is believed they all are), then $m(0) = 0$ too. Unconditionally, the work of Levinson and Montgomery [3] shows that $m^+(x) \to 0$ as $x \to -\infty$.

For large x, the work of Conrey and Ghosh [1] shows that $m^+(x) < 1$ for all x.

It is believed that random matrix theory can be used to model the Riemann zeta function (see the survey articles in [5] for example). Mezzadri [4] found the random matrix equivalent of $m(x)$, namely the radial distribution of the zeros of the derivative of the characteristic polynomial of a random unitary matrix. His results suggest that

$$m(x) \sim 1 - \frac{1}{x} \quad \text{as } x \to \infty$$

which means that $m(x)$ cannot come from a distribution with a mean.

We are interested in $m(x)$ for x near 0. Soundararajan [6] showed that, under RH, $m^-(x) > 0$ for $x > 2.6$. Zhang [8] removed the need for RH at the cost of showing the positivity of $m^-(x)$ only for sufficiently large x. He also showed, assuming RH and assuming the proportion of consecutive zeros of $\zeta(s)$ with gaps an arbitrary constant smaller than the mean gap is non-zero, that $m^-(x) > 0$ for

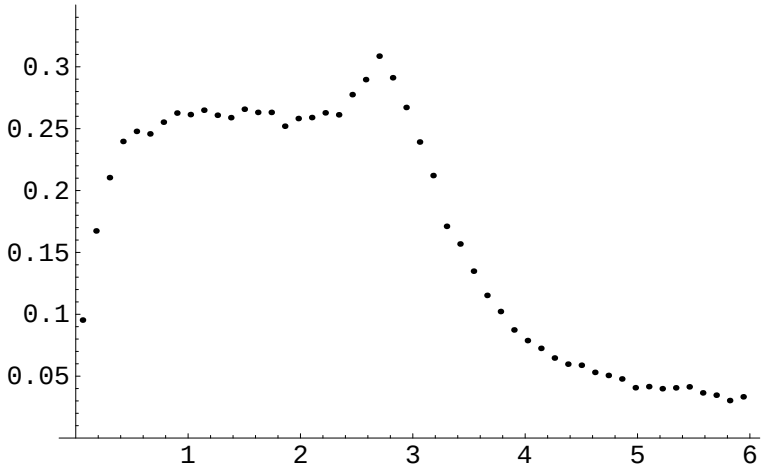


FIGURE 1. Normalized distribution of the real part of the zeros of $\zeta'(s)$. Data is for the approximately 100000 zeros with imaginary part in $[10^6, 10^6 + 60000]$.

all $x > 0$. Feng [2] removed the need for RH in the last result, but still needs to assume the existence of a positive proportion of small gaps.

For more on m, m^+, and m^- and the connection between small gaps between zeta zeros and zeros of the derivative of zeta, see the talk of Cem Yıldırım from the same Oberwolfach meeting.

In work very much still in progress, we show that if the Riemann Hypothesis is true, and if the distribution for small gaps between zeros of the zeta function is as predicted by random matrix theory, then

$$m^-(x) \geq \frac{8}{9\pi} x^{3/2} + O(x^{5/2}) \quad \text{as } x \to 0$$

We have also numerically computed the density function underlying $m(x)$ for zeros with height around one million. We find that the horizontal distribution of the zeros of the derivative appear to have a strange Bactrian distribution, although it is not clear whether the double-hump remains as $T \to \infty$. This is seen in Figure 1.

As sketch of the proof of our result goes as follows: We consider two very close together zeros of the Riemann zeta function, with heights $t \pm \pi\theta/\log t$. Using the Hadamard product for zeta, we solve $\frac{\zeta'}{\zeta}(\rho') = 0$ as a series expansion in θ, assuming ρ' is close to the midpoint of the two zeros. That is, we assume

$$\rho' = \frac{1}{2} + \frac{1}{\log t} \sum_{j=1}^{\infty} b_j \pi^{2j} \theta^{2j} + it$$

where the b_j can be complex.

Using the fact that the zeta zeros come in symmetric pairs, we show that

$$b_1 = \frac{1}{4} + O\left(\frac{1}{\log t}\right)$$

and inserting the assumption (from random matrix theory) that the probability density that two zeta zeros have gap $2\pi\theta/\log t$ is approximately

$$\left(\frac{\pi^2}{3} - \frac{\pi^2}{3(\log t)^2}\right)\theta^2 + O(\theta^4)$$

this leads to

$$m^-(x) \geq \int_0^x \left(\frac{4}{3\pi}s^{1/2} + O(s^{3/2})\right) ds = \frac{8}{9\pi}x^{3/2} + O(x^{5/2})$$

References

[1] Conrey J. B. and Ghosh A. Zeros of derivatives of the Riemann zeta-function near the critical line *Analytic Number Theory: Proc. Conf. in Honor of P. T. Bateman (Allenton Park, Ill., 1989) (Prog. Math. vol 85)* B. C. Berndt *et. al.* eds., Birkhäuser Inc., Boston, pp. 95–110 (1990).

[2] Feng S. A note on the zeros of the derivative of the Riemann zeta function near the critical line. *Acta Arith.* **120**, 59–68 (2005).

[3] Levinson N. and Montgomery H. L. Zeros of the derivatives of the Riemann zeta-function *Acta Math.* **133**, 49–65 (1974).

[4] Mezzadri F. Random matrix theory and the zeros of $\zeta'(s)$. *J. Phys. A: Math. Gen.* **36**, 2945–2962 (2003).

[5] *Recent perspectives in random matrix theory and number theory. LMS Lecture Note Series, 322.* Mezzadri F. and Snaith N. C. Eds. Cambridge University Press, Cambridge, 2005.

[6] Soundararajan K. The horizontal distribution of the zeros of $\zeta'(s)$. *Duke Math. J.* **91**, 33–59 (1998).

[7] Speiser A. Geometrisches zur Riemannschen Zetafunktion *Math. Ann.* **110** 514–21 (1934).

[8] Zhang Y. On the zeros of $\zeta'(s)$ near the critical line, *Duke Math. J.* **110**, 555-572 (2001).

Configurations of Lattice Points

Martin Huxley

Let Λ be a lattice in the plane , and let S be a closed convex bounded plane region containing the origin, an 'oval'. Let $S(r, P)$ be the set obtained by enlarging S by a factor r, then translating S by the vector $\overrightarrow{OP}$. We call $S(r, P)$ an 'S-oval'. Let $J(r, P)$ be the set of points of Λ in $S(r, P)$, and let $N(r, P)$ be the magnitude of the set $J(r, P)$. We call $J(r, P)$ a configuration, and $N(r, P)$ its weight. For large r the weight $N(r, P)$ is approximately Ar^2. The mathematical questions are: how many configurations of S-ovals occur, and how does the lattice discrepancy $N(r, P) - Ar^2$ vary? Behind this is a question in artificial intelligence: $J(r, P)$ is the image taken by a digital camera. How easily can $J(r, P)$ be identified as a possible S-oval?

At this level of generality, we can transform Λ into the square lattice of integer points, changing the shape of the oval S, but not the number of configurations or their weights.

Problem A (area by counting squares, including the Gauss circle problem). Suppose that the oval S has a sufficiently smooth boundary curve C. Estimate $N(r, P)$ accurately.

Theorem A (Huxley 2003). *Under C^3 smoothness conditions,*

$$N(r, P) = Ar^2 + \mathrm{O}\left(r^{\kappa+\epsilon}\right); \qquad \kappa = 131/208 = 0,6298\cdots.$$

Here as usual $\mathrm{O}(r^\epsilon)$ stands for some function of r that grows slower than any power of r; in this case a power of a logarithm.

Problem B (Žunić). For fixed size r, how many different configurations $J(r, P)$ occur as the point P varies (different up to translation by an integer vector)? The configurations correspond loosely to regions in a domains diagram.

Theorem B (Huxley, Žunić 2008). *Let r be fixed. Under C^3 smoothness conditions and the Triangle Condition, the number $K(r)$ of configurations is*

$$K(r) = Br^2 + \mathrm{O}\left(r^{\kappa+\epsilon}\right).$$

The Triangle Condition (for fixed size r) says that the boundary curve $C(r, P)$ of the oval $S(r, P)$ cannot pass through three distinct integer points for any point P. The result of Theorem B is also true for circles without the Triangle Condition, by a special argument.

Problem C (Žunić). How many different configurations $J(r, P)$ have $N(r, P) = n$ (there are $K(n)$ such configurations, say), or $N(r, P) \le N$ (there are $M(N)$ such configurations, say)? As in Problem B, different means different up to translation by an integer vector. For fixed weight n, the configurations with $N(r, P) = n$ correspond to connected regions in a domains diagram.

Theorem C (Huxley, Žunić, submitted). *If the boundary C contains no straight line segment with rational gradient, then*

$$L(n) \le 2n - 1, \qquad M(N) \le N^2.$$

If the boundary C satisfies the Quadrangle Condition, then we have equality.

The Quadrangle Condition says that the boundary curve $C(r, P)$ of the oval $S(r, P)$ cannot pass through four distinct integer points for any size r and any point P. For the circle, which does not satisfy the Quadrangle Condition, Huxley and Konyagin (submitted) have

$$M(N) = N^2 - \mathrm{O}\left(N^{3/2}\right).$$

Work in progress aims to find connections between these three problems.

Theorem D (Huxley, Kolountzakis, Žunić). *Under C^4 smoothness conditions, the number $T(R)$ of different sets of three integer points (different up to translation by an integer vector) for which there is an S-oval $S(r, P)$, with $r \le R$ and with these three integer points on the boundary, satisfies*

$$T(R) = A^2R^4 + \mathrm{O}\left(R^3\right).$$

For circles the remainder term is

$$\mathrm{O}\left(R^{2+\kappa+\epsilon}\right).$$

Theorem E (Huxley, Konyagin). *For S the unit circle, the number $Q(R)$ of different sets of four integer points (different up to translation by an integer vector) for which there is a circle $S(r,P)$, with $r \le R$ and with these four integer points on the boundary, satisfies*

$$Q(R) = \frac{32(3+\sqrt{2})}{21\zeta(3)}\zeta\left(\frac{3}{2}\right)L\left(\frac{3}{2},\chi\right)R^3 + \mathrm{O}\left(R^{76/29+\epsilon}\right),$$

where $\zeta(s)$ is the Riemann zeta function, and $L(s,\chi)$ is the non-trivial Dirichet L-function modulo 4. We note that in Theorem E we have $76/29 = 2,6207\cdots < 2+\kappa$.

References

[1] *M.N. Huxley*, Area, Lattice Points, and Exponential Sums, London Math. Soc. Monographs 13, Oxford University Press, Oxford, 1996.

[2] *M.N. Huxley*, The integer points close to a curve III, in Number Theory in Progress, de Gruyter, Berlin 1999, 911-940.

[3] *M.N. Huxley*, Exponential sums and lattice points III, Proc. London Math. Soc., (3) **87** (2003), 591-609.

[4] *M.N. Huxley*, The integer points in a plane curve, Functiones et Approximatio, **37** (2007), 7-25.

[5] *M.N. Huxley, S.V. Konyagin*, Cyclic polygons of integer points, submitted to Acta Arithmetica

[6] *M.N. Huxley, J. Žunić*, Different digitizations of displaced discs, Foundations of Computational Mathematics, **6** (2006), 255-268.

[7] *M.N. Huxley, J. Žunić*, The number of n-point digital discs, IEEE Trans. Pattern Analysis and Machine Intelligence, **29** (2007), 159-161.

[8] *M.N. Huxley, J. Žunić*, The number of configurations in lattice point counting I, Forum Mathematicum, to appear.

[9] *M.N. Huxley, J. Žunić*, The number of configurations in lattice point counting II, submitted.

[10] *M.N. Huxley, M. Kolountzakis, J. Žunić*, The number of configurations in lattice point counting III,

[11] *D.G. Kendall*, On the number of lattice points inside a random oval, Quarterly J. Maths. (Oxford) **19** (1948), 1-26.

Hybrid moments of the zeta-function on the critical line

Aleksandar Ivić

Power moments on the "critical line" $\sigma = \Re\mathrm{e}\, s = \frac{1}{2}$ represent one of the most important parts of the theory of the Riemann zeta-function $\zeta(s)$ (see [2], [3]). The aim here is to discuss the so-called "hybrid" moments and some related topics. These are integrals of the type

$$\int_T^{2T} |\zeta(\tfrac{1}{2}+it)|^k \left(\int_{t-G}^{t+G} |\zeta(\tfrac{1}{2}+ix)|^\ell \,\mathrm{d}x\right)^m \mathrm{d}t \qquad (k,\ell,m \in \mathbb{N}), \tag{1}$$

where k,ℓ,m are assumed to be fixed, and $1 \ll G \ll T$. The expected bound for the expression in (1) (this is consistent with the hitherto unproved Lindelöf

hypothesis that $\zeta(\frac{1}{2}+it) \ll_\varepsilon |t|^\varepsilon$) is clearly

$$O_\varepsilon(T^{1+\varepsilon}G^m), \tag{2}$$

where here and later ε (>0) denotes arbitrarily small constants, not necessarily the same ones at each occurrence. The problem is to find, for given k, ℓ, m, the range of

$$G = G(T; k, \ell, m)$$

for which (1) is bounded by (2). From general results (see [12]) it is known that the expression in (1) is, for $\log\log T \ll G \ll T$,

$$\gg G^m(\log T)^{\ell^2 m/4}\int_T^{2T} |\zeta(\tfrac{1}{2}+it)|^k\,\mathrm{d}t \gg TG^m(\log T)^{(\ell^2 m+k^2)/4}.$$

This shows that, up to 'ε', the bound in (2) is indeed best possible. The (less difficult) case $k=0$ in (1) was investigated in [5] and [6]. In view of the bound (see [3])

$$|\zeta(\tfrac{1}{2}+it)|^k \ll \log t\int_{t-1}^{t+1} |\zeta(\tfrac{1}{2}+ix)|^k\,\mathrm{d}x + 1, \qquad (k\in\mathbb{N}\ \text{ fixed})$$

it is clear that hybrid moments can be used to bound $I_k(T) := \int_0^T |\zeta(\frac{1}{2}+it)|^{2k}\,\mathrm{d}t$, although this approach is somewhat wasteful, but on the other hand one gains flexibility by choosing G appropriately. For example, one of our bounds is

$$\int_T^{2T} |\zeta(\tfrac{1}{2}+it)|^4 \int_{t-G}^{t+G} |\zeta(\tfrac{1}{2}+ix)|^4\,\mathrm{d}x\,\mathrm{d}t \ll \log^C T\Big(TG + \min(T^{5/3}, T^2G^{-1})\Big) \tag{3}$$

for $1 \ll G = G(T) \ll T$, and from (3) one easily deduces ($C>0$ is a generic constant) the hitherto sharpest bound $I_4(T) \ll T^{3/2}\log^C T$. We have obtained results on (1) for several values of m when k, ℓ equal 2 or 4, which is logical, since it is in these cases that we have good information on $I_k(T)$. Namely we have F.V. Atkinson's formula [1] (for $k=1$) and Y. Motohashi's formula [11] (for $k=2$), although it is more convenient to use formulas for the smoothed integrals

$$J_k(T,G) := \frac{1}{\sqrt{\pi}G}\int_{-\infty}^{\infty} |\zeta(\tfrac{1}{2}+iT+iy)|^{2k}\mathrm{e}^{-(y/G)^2}\,\mathrm{d}y \quad (k\in\mathbb{N}, 1\ll G\ll T).$$

To avoid excessive length, we mention here only one more explicit result, namely

$$\int_T^{2T} |\zeta(\tfrac{1}{2}+it)|^2\left(\int_{t-G}^{t+G} |\zeta(\tfrac{1}{2}+ix)|^2\,\mathrm{d}x\right)^3\,\mathrm{d}t \ll_\varepsilon T^{1+\varepsilon}G^3 \tag{4}$$

for $T^{\frac{1}{5}} \ll G = G(T) \ll T$. In bounds like (4), it is the lower bound for G which is of importance, while for $G \geq T^{1/3}$ the bound is trivial, since (see [2], [3]) one shows without difficulty that

$$\int_{t-G}^{t+G} |\zeta(\tfrac{1}{2}+ix)|^2\,\mathrm{d}x \ll G\log t \qquad (t^{1/3}\ll G\leq t).$$

In the course of the proofs, besides the explicit formulas for $J_k(T,G)$ we use the bound

$$\int_0^T E_2^2(t)\,\mathrm{d}t \;\ll\; T^2\log^C T,$$

due to Y. Motohashi and the author (see [8], [9]), where $E_2(T)$ is the error term in the asymptotic formula for $I_2(T)$. The chief arithmetical tool is the recent result of [13] that, for any given $\varepsilon>0$, $k\ge 2$ a fixed integer and given $\delta>0$, the number of integers n_1,n_2,n_3,n_4 such that $N<n_1,n_2,n_3,n_4\le 2N$ and

$$|n_1^{1/k}+n_2^{1/k}-n_3^{1/k}-n_4^{1/k}|<\delta N^{1/k}$$

is $\ll_\varepsilon N^\varepsilon(N^4\delta+N^2)$. To deal with bounds like the one in (4), we also need results on the moments of the function

$$E^*(t)\;:=\;E(t)-2\pi\Delta^*\bigl(\frac{t}{2\pi}\bigr),$$

where

$$\Delta^*(x):=-\Delta(x)+2\Delta(2x)-\tfrac12\Delta(4x)=\tfrac12\sum_{n\le 4x}(-1)^n d(n)-x(\log x+2\gamma-1).$$

Here as usual $d(n)$ is the number of divisors of n, γ is Euler's constant and

$$\Delta(x)\;=\;\sum_{n\le x}d(n)-x(\log x+2\gamma-1)$$

is the error term in the classical Dirichlet divisor problem. The function $E^*(t)$ gives an insight into the analogy between the Dirichlet divisor problem and the mean square of $|\zeta(\frac12+it)|$. It was investigated by several authors, including M. Jutila [10], who introduced the function $E^*(t)$, and the author [4]–[6]. Among other things, the author (op. cit.) proved that

$$\int_0^T (E^*(t))^2\,\mathrm{d}t\;=\;T^{4/3}P_3(\log T)+O_\varepsilon(T^{7/6+\varepsilon}),$$

where P_3 is a polynomial of degree three in $\log T$ with positive leading coefficient,

$$\int_0^T |E^*(t)|^5\,\mathrm{d}t\;\ll_\varepsilon\;T^{2+\varepsilon},\quad \int_0^T |E^*(t)|^3\,\mathrm{d}t\;\ll_\varepsilon\;T^{3/2+\varepsilon},$$

and none of these three results implies any one of the other two. The connection of $E^*(t)$ to the mean square of $|\zeta(\frac12+it)|$ in short intervals is given by the formula

$$J_1(t,G)=\frac{2}{\sqrt{\pi}G^3}\int_{-G\log T}^{G\log T} xE^*(t+x)\mathrm{e}^{-(x/G)^2}\,\mathrm{d}x+O(\log^2 T)$$

for $T^\varepsilon\le G=G(T)\le T^{1/3}$, $T/2\le t\le 5T/2$. Thus the moments of $E^*(t)$ can be used for hybrid moments (1) when $\ell=2$. Complete results with detailed proofs will appear in due time.

One can also use moments of $E(t+G)-E(t-G)$ to bound moments of $|\zeta(\frac{1}{2}+it)|$. Results of this type are given in [7]. In particular it was proved there that, for $1 \ll U = U(T) \le \frac{1}{2}\sqrt{T}$, we have ($c_3 = 8\pi^{-2}$)

$$\begin{aligned}\int_T^{2T} \left(E(x+U)-E(x)\right)^2 \,\mathrm{d}x &= TU\sum_{j=0}^{3} c_j \log^j\Big(\frac{\sqrt{T}}{U}\Big) \\ &\quad + O_\varepsilon(T^{1/2+\varepsilon}U^2) + O_\varepsilon(T^{1+\varepsilon}U^{1/2}),\end{aligned}$$

and an analogous result holds true if $E(x+U)-E(x)$ is replaced by $\Delta(x+U)-\Delta(x)$.

References

[1] F.V. Atkinson, The mean value of the Riemann zeta-function, Acta Math. **81**(1949), 353-376.

[2] A. Ivić, The Riemann zeta-function, John Wiley & Sons, New York, 1985 (2nd ed., Dover, Mineola, N.Y., 2003).

[3] A. Ivić, The mean values of the Riemann zeta-function, LNs **82**, Tata Inst. of Fundamental Research, Bombay (distr. by Springer Verlag, Berlin etc.), 1991.

[4] A. Ivić, On the Riemann zeta function and the divisor problem, Central European Journal of Mathematics 2(**4**) (2004), 1-15; II ibid. 3(**2**) (2005), 203-214, III, subm. to Ann. Univ. Budapest, Sectio Computatorica, and IV, Uniform Distribution Theory **1**(2006), 125-135.

[5] A. Ivić, Some remarks on the moments of $|\zeta(\frac{1}{2}+it)|$ in short intervals, to appear in Acta Mathematica Hungarica. `math.NT/0611427`

[6] A. Ivić, On moments of $|\zeta(\frac{1}{2}+it)|$ in short intervals, Ramanujan Math. Soc. LNS**2**, The Riemann zeta function and related themes: Papers in honour of Professor K. Ramachandra, 2006, 81-97.

[7] A. Ivić, On the divisor function and the Riemann zeta-function in short intervals, to appear. `arXiv:0707.1756`

[8] A. Ivić and Y. Motohashi, The mean square of the error term for the fourth moment of the zeta-function, Proc. London Math. Soc. (3)**66**(1994), 309-329.

[9] A. Ivić and Y. Motohashi, The fourth moment of the Riemann zeta-function, J. Number Theory **51**(1995), 16-45.

[10] M. Jutila, Riemann's zeta-function and the divisor problem, Arkiv Mat. **21**(1983), 75-96 and II, ibid. **31**(1993), 61-70.

[11] Y. Motohashi, Spectral theory of the Riemann zeta-function, Cambridge University Press, Cambridge, 1997.

[12] K. Ramachandra, On the mean-value and omega-theorems for the Riemann zeta-function, Tata Institute of Fundamental Research, Bombay, distr. by Springer Verlag, 1995.

[13] O. Robert and P. Sargos, Three-dimensional exponential sums with monomials, J. reine angew. Math. **591**(2006), 1-20.

Atkinson's formula for Hardy's function

Matti Jutila

By definition, *Hardy's function* is

$$Z(t) = \chi^{-1/2}(\tfrac{1}{2}+it)\zeta(\tfrac{1}{2}+it),$$

where

$$\chi(s) = 2^s\pi^{s-1}\sin(\tfrac{1}{2}\pi s)\Gamma(1-s)$$

as in the functional equation $\zeta(s) = \chi(s)\zeta(1-s)$ for Riemann's zeta-function. For real t, $Z(t)$ is real and $|Z(t)| = |\zeta(\frac{1}{2}+it)|$, whence the real zeros of $Z(t)$ are related to the zeros of the zeta-function on the critical line.

The famous formula of Atkinson [1] (see also [2], Chapter 15) gives an expression for the mean square of $Z^2(t)$. As an analogue, we have a formula of similar structure for the integral

$$F(T) = \int_0^T Z(t)\,dt.$$

We state it using the notation of [2]. Let T be a large positive number, $N \asymp T$, and

$$N' = T/2\pi + N/2 - \sqrt{N^2/4 + NT/2\pi}.$$

Then

$$F(T) = \Sigma_1(T) + \Sigma_2(T) + O\left(\log^2 T\right),$$

where

$$\Sigma_1(T) = 2\sqrt{2}(T/2\pi)^{1/4} \sum_{0\le n\le\sqrt{N}} (-1)^{n(n+1)/2} e\left(T, \left(n+\tfrac{1}{2}\right)^2\right)\left(n+\tfrac{1}{2}\right)^{-1}$$
$$\times \cos\left(\tfrac{1}{2} f\left(T, \left(n+\tfrac{1}{2}\right)^2\right) - 3\pi/8\right)$$

and

$$\Sigma_2(T) = -4 \sum_{1\le n\le\sqrt{N'}} n^{-1/2}\left(\log(T/2\pi n^2)\right)^{-1} \cos\left(\tfrac{1}{2} g\left(T, n^2\right) + \pi/4\right)$$

with

$$e(T,n) = (1+\pi n/2T)^{-1/4}\left\{\sqrt{2T/\pi n}\,\text{ar sinh}\left(\sqrt{\pi n/2T}\right)\right\}^{-1} = 1 + O(nT^{-1}),$$

$$f(T,n) = 2T\,\text{ar sinh}\left(\sqrt{\pi n/2T}\right) + \left(2\pi nT + \pi^2 n^2\right)^{1/2} - \pi/4$$
$$= -\pi/4 + 2\sqrt{2\pi nT} + \frac{1}{6}\sqrt{2\pi^3} n^{3/2} T^{-1/2} + \ldots,$$

and

$$g(T,n) = T\log(T/2\pi n) - T + \pi/4.$$

The proof is based on a formula for the Laplace transformation of $Z(t)$ and the argument follows [4], where we derived the original Atkinson formula together with its analogue for cusp form L-functions by a unified method.

It was shown by A. Ivić [3] that $F(T) \ll T^{1/4+\varepsilon}$ for any fixed $\varepsilon > 0$, and he conjectured that this estimate is close to being best possible. Indeed, it was recently proved by M. A. Korolev [6] that $F(T) = \Omega_{\pm}(T^{1/4})$. Also, he proved that $F(T) = O(T^{1/4})$, and hence the amplitude of the oscillations of $F(T)$ is fully understood. These conclusions can be drawn also from the above formula; Ivić and Korolev used variants of the approximate functional equation for $Z(t)$ which we dispense with.

As another application, we may estimate gaps between consecutive zeros of $Z(t)$, that is gaps between consecutive zeros of the zeta-function on the critical line, in terms of exponential sums related to the sum $\Sigma_1(T)$. These exponential sums turn out to be of similar structure as in the work of A. A. Karatsuba [5].

References

[1] F. V. Atkinson, The mean value of the Riemann zeta-function, Acta Math. 81 (1949), 353–376.

[2] A. Ivić, The Riemann Zeta-Function, John Wiley & Sons, Inc., New York, 1985 (2nd ed., Dover, Mineola, New York, 2003).

[3] A. Ivić, On the integral of Hardy's function, Arch. Math. 83 (2004), 41–47.

[4] M. Jutila, Atkinson's formula revisited, Voronoi's impact on modern science, Book 1, Institute of Mathematics, National Academy of Sciences of Ukraine, Kyiv, 1998, pp. 137–154.

[5] A. A. Karatsuba, On the distances between consecutive zeros of Riemann's zeta-function on the critical line (Russian), Trudy Mat. Inst. Akad. Nauk USSR 157 (1981), 49–63.

[6] M. A. Korolev, On the Primitive of the Hardy Function $Z(t)$, Dokl. Math. 75 (2007), 295–298.

Nonexistence of L-functions of degree $1 < d < 2$

Jerzy Kaczorowski

(joint work with Alberto Perelli)

The extended Selberg class $S^\sharp$ consists of Dirichlet series $F(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$ ($s = \sigma + it$) which converge absolutely for $\sigma > 1$, admit meromorphic continuation to $\mathbb{C}$ such that $(s-1)^m F(s)$ is entire of finite order ($m = m(F) \in \mathbb{N} \cup \{0\}$), and satisfies a general functional equation of the Riemann type

$$\Phi(s) = \omega\overline{\Phi(1-\overline{s})},$$

where

$$\Phi(s) = Q^s \prod_{j=21}^{r} \Gamma(\lambda_j s + \mu_j) F(s)$$

with $Q, \lambda_j > 0$, $\Re(\mu_j) \geq 0$ and $|\omega| = 1$. The Selberg class S (see [12]) is the set of $F \in S^\sharp$ satisfying in addition the Ramanujan condition ($a(n) \ll n^\varepsilon$ for every $\varepsilon > 0$) and having an Euler product expansion. The Selberg class may be regarded as an axiomatic model for L-functions in number theory, and the main problem, apart from classical open problems such as the Riemann Hypothesis, is classifying its elements. We expect that the degree of every $F \in S^\sharp$ is a non-negative integer (the *Degree Conjecture*), and that the functions in S with integer degree d coincide with the automorphic L-functions of degree d (a kind of analytic version of the Langlands program). We refer to survey papers [3] [5], [9], [10] for more information about S and $S^\sharp$.

The focus of the research reported here is on the degree conjecture for functions of small degrees, and the main result reads as follows.

Theorem. *Degree Conjecture holds true for $d \leq 2$.*

Due to classical work by Bochner [1], Richert [11] (see also [2] and [8]), and a more recent results by Kaczorowski-Perelli [4], [6], it is enough to show that there are no entire L-functions in $S^\sharp$ of degree $5/3 \le d < 2$. The main idea is to work not directly with an L-function F but with a closely related family of Dirichlet series $\tilde{F}$, called the *shadows* of F, and to prove that one of them has a pole in the region of holomorphy getting in this way a contradiction. A general new method is developed to this purpose which gives a uniform solution in the whole range $0 < d < 2$, $d \neq 1$. In the range $0 < d < 1$ a construction of the proper shadow was given in [7]. The case of $1 < d < 2$ is much more involved and leads to the study of the multidimensional twists of the form

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} \exp\left(-2\pi i \sum_{\nu=1}^{N} \alpha_\nu n^{\kappa_\nu}\right),$$

where $\kappa_1 > \kappa_2 > \ldots > \kappa_N > 0$, $d\kappa_1 > 1$, are fixed.

References

[1] S. Bochner, *On Riemann's functional equation with multiple gamma factors*, Ann. of Math. **67** (1958), 29–41.

[2] J.B. Conrey, A. Ghosh, *On the Selberg class of Dirichlet series: small degrees*, Duke Math. J. **72** (1993), 673–693.

[3] J. Kaczorowski, *Axiomatic theory of L-functions: the Selberg class*, In *Analytic Number Theory*, C.I.M.E. Summer School, Cetraro (Italy) 2002, ed. by A. Perelli and C. Viola, 133–209, Springer L.N. 1891, 2006.

[4] J. Kaczorowski, A. Perelli, *On the structure of the Selberg class, I:* $0 \le d \le 1$, Acta Math. **182** (1999), 207–241.

[5] 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.

[6] J. Kaczorowski, A. Perelli, *On the structure of the Selberg class, V:* $1 < d < 5/3$, Invent. Math. **150** (2002), 485–516.

[7] J. Kaczorowski, A. Perelli, *On the structure of the Selberg class, VI: non-linear twists*, Acta Arith. **116** (2005), 315–341.

[8] G. Molteni, *A note on a result of Bochner and Conrey-Ghosh about the Selberg class*, Arch. Math. **72** (1999), 219–222.

[9] A. Perelli, *A survey of the Selberg class, part I*, Milan J. Math. **73** (2005), 19–52.

[10] A. Perelli, *A survey of the Selberg class, part II*, Riv. Inst. Mat. Univ. Parma (7) **3*** (2004), 83–118.

[11] H.-E. Richert, *Über Dirichletreihen mit Funktionalgleichung*, Publ. Inst. Math. Acad. Serbe Sci. **11** (1957), 73–124.

[12] A. Selberg, *Old and new conjectures and results about a class of Dirichlet series*, In *Proc. Amalfi Conf. Analytic Number Theory*, ed. by E. Bombieri *et al., 367–385, Università di Salerno 1992; Collected Papers, vol. II, 47–63, Springer Verlag 1991.*

Prime or almost-prime solutions to quadratic equations

Jianya Liu
(joint work with Peter Sarnak)

In the introductory part of the talk, various results for the Waring-Goldbach problem [3] are revisited in the spirit of recent general conjectures of Sarnak [7], and of Bourgain, Gamburd, and Sarnak [1]. Special attention is paid to the quadratic Waring-Goldbach problem, i.e. prime solutions to quadratic equations. In the main part of the talk, a new result of Sarnak and the speaker [6], on the almost-prime solutions to quadratic equations in three variables, is reported. Roughly speaking, this new result states that, if $g(x_1, x_2, x_3)$ is an indefinite anisotropic quadratic form with determinant $d(g)$, and t a non-zero integer such that $d(g)t$ is square-free, then there are infinitely many solutions to the equation $g(x_1, x_2, x_3) = t$ such that the product $x_1x_2x_3$ has at most 26 prime divisors. The above 26 can be reduced to 22 under Selberg's eigenvalue conjecture. This result is obtained via a three dimensional combinatorial sieve [2] and a key level equidistribution theorem; the latter is established by the theory of quadratic forms [10], the Jacquet-Langlands theory [4] on automorphic representations, the Kim-Sarnak bound [5] toward Selberg's eigenvalue conjecture, and ideas in harmonic analysis [9] [8].

References

[1] J. Bourgain, A. Gamburd, and P. Sarnak, *Sieving and expanders*, C. R. Math. Acad. Sci. Paris **343** (2006), 155–159; *An affine linear sieve, expanders and sum product* , in preparation.

[2] H. Diamond and H. Halberstam, *Some applications of sieves of dimension exceeding 1*, in *Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995)*, 101-107, London Math. Soc. Lecture Notes Ser., 237, Cambridge Univ. Press, Cambridge, 1997.

[3] L. K. Hua, *Some results in the additive prime number theory*, Quart. J. Math. (Oxford) **9** (1938), 68–80.

[4] H. Jacquet and R. P. Langlands, *Automorphic forms on* GL(2), Lecture Notes in Mathematics, Vol. 114, Springer-Verlag, Berlin-New York, 1970.

[5] H. Kim and P. Sarnak, *Refined estimates towards the Ramanujan and Selberg conjectures, J. Amer. Math. Soc.* **16** (2003), 175–181.

[6] J. Y. Liu and P. Sarnak, *Integral points on quadrics in three variables whose coordinates have few prime factors*, to appear.

[7] P. Sarnak, *Equidistribution and primes*, Pacific Institute of Mathematics 10th Anniversary Lecture, September 2007.

[8] P. Sarnak and X. Xue, Bounds for multiplicities of automorphic representations, Duke Math. J. 64 (1991), 207-227.

[9] A. Selberg, *Harmonic analysis on weakly symmetric Riemannian spaces with applications to Dirichlet series*, J. Indian Math. Soc. **20** (1956), 47–87.

[10] C. L. Siegel, *Lectures on the analytic theory of quadratic forms*, third edition, Robert Peppermuller, Göttingen 1963.

Intervals on the critical line, in which the Riemann zeta function assumes only small values

Helmut Maier
(joint work with Ulirike Vorhauer)

Assuming the Riemann Hypothesis we establish the existence of long intervals on the critial line, whose endpoints have arbitrarily large imaginary parts, in which the Riemann zeta function assumes only small values.

Theorem. *Assume RH. Then there is a constant $c > 0$ and arbitrarily large values T, such that*

$$|\zeta(\frac{1}{2} + it)| \le \frac{1}{2} \quad \textit{for} \quad t \in [T, T + c(\log_4 T)^{-1}]$$

(for $k \ge 2$ we denote as usual by $\log_k(x) = \log(\log_{k-1}(x))$ the k-fold iterated logarithm).

We shortly describe the basic ideas of the proof: From a well-known approximate formula of Selberg we deduce the inequality

$$\log|\zeta(\frac{1}{2} + it)| \ \le \ \mathrm{Re} \sum_{n<x^2} \frac{\Lambda_x(n)}{(\log n)^{\sigma_1+it}} + O\left(\frac{\log T}{\log x}\right) \ + \ O\left(\frac{1}{\log x}\left|\sum_{n<x^2} \frac{\Lambda_x(n)}{n^{\sigma_1+it}}\right|\right) \tag{1}$$

where $T \le t \le 2T$, $\Lambda_x(n) = \Lambda(n) w_x(n)$ with

$$w_x(n) \ = \ \begin{cases} 1 & \text{if} \quad 1 \le n < x \\ \frac{\log(\frac{x^2}{n})}{\log(x)} & \text{if} \quad x \le n \le x^2 \\ 0 & \text{o.w.} \end{cases} , \ \log(x) = \frac{\log T}{\log\log T} \ , \ \sigma_1 = \frac{1}{2} + \frac{1}{\log x} \ .$$

For a suitably chosen function ϱ and a partition $u_0 < u_1 < \cdots < u_m$ of the support of ϱ we impose the conditions

$$\sum_{u_j < \log p \le u_{j+1}} p^{-(\frac{1}{2}+it)} \ = \ \varrho(u_j)\Delta u_j \ + \ \mathrm{err}(j) \ , \ \Delta u_j \ = \ u_{j+1} - u_j \ , \tag{2}$$

$\mathrm{err}(j)$ a suitable error-term. Then we obtain the approximation

$$\sum_{u_0 < \log p \le u_m} p^{-(\frac{1}{2}+i(t+\tau))} \ = \ \int_{-\infty}^{\infty} \varrho(u) e^{-i\tau u} du \ + \ \mathrm{error} \, ,$$

which together with (1) implies the Theorem, if the values p^{-it} satisfy some additional - less restrictive - conditions.

The existence of values t, such that p^{-it} satisfy the conditions (2) and these additional conditions are established by harmonic analysis.

The Combinatorics of moment calculations

Hugh L. Montgomery

In work that was first announced at Oberwolfach in 1998, the author and Soundararajan constructed a heuristic argument that suggests that

$$\int_0^X (\psi(x+h)-\psi(x)-h)^K\,dx = (\mu_K+o(1))X(h\log X/h)^{K/2}$$

where $\mu_{2k} = 1\cdot 3\cdots(2k-1)$ and $\mu_{2k+1}=0$ are the moments of a normal random variable. It was initially envisaged that the argument would begin by an application of the binomial theorem, so that

$$\sum_{n=1}^N \Big(\sum_{m=1}^h \Lambda(m+n)-h\Big)^K = \sum_{k=0}^K \binom{K}{k}(-h)^{K-k}\sum_{n=1}^N\Big(\sum_{m=1}^h\Lambda(m+n)\Big)^k.$$

After some simplifications, it is found that the sum over n on the right hand side is approximately

$$\sum_{r=1}^k S(k,r)r!\sum_{\mathcal{D}\subseteq\{1,\dots,h\}\mathrm{card}\mathcal{D}=r}\sum_{n=1}^N(\log n)^{k-r}\prod_{i=1}^r\Lambda(n+d_i)$$

where the $S(k,r)$ are the Stirling numbers of the second kind. Hardy and Littlewood conjectured that

$$\sum_{n=1}^N\prod_{i=1}^r\Lambda(n+d_i) = (\mathfrak{S}(\mathcal{D})+o(1))N$$

where $\mathfrak{S}(\mathcal{D})$ is a singular series. We take the main term and ignore any effect that the error terms might have, and are led to the conclusion that the original moment should be approximately

$$\sum_{s=0}^K R_s(h)\sum_{j=0}^{K-s} I_j(N)P_{K,s,j}(h)$$

where $R_s(h)$ is an average of singular series whose asymptotics can be determined, $I_j(N)$ is a simple singular integral, and the $P_{K,s,j}(h)$ are the polynomials

$$P_{K,s,j}(h) = \sum_{i=s}^{K-j}\binom{K}{i+j}S(i+j,i)\frac{i!}{s!}(-h)^{K-i-j}\binom{h-s}{i-s}.$$

In order to complete the argument along these lines, it is necessary to know more about these polynomials—specifically that $\deg P_{K,s,j}\le K-s-j$, that $\deg P_{K,s,j}\le[(K-s)/2]$, that for $0\le j\le k-s$ the leading term of $P_{2k,2s,j}(h)$ is

$$(-1)^{k-s-j}\binom{k-s}{j}\binom{k}{s}\frac{1\cdot 3\cdots(2k-1)}{1\cdot 3\cdots(2s-1)}h^{k-s},$$

and that the leading term of $P_{2k+1,2s+1,j}(h)$ is

$$(-1)^{k-s+j}\binom{k-s}{j}\binom{k}{s}\frac{1\cdot 3\cdots(2k+1)}{1\cdot 3\cdots(2s+1)}h^{k-s}\,.$$

The Montgomery–Soundararajan argument was completed in a way that avoided these polynomials, but the above properties can be established by showing that each $P_{K+1,s,j}(h)$ is a linear combination of five earlier polynomials of the same sort. Precisely,

$$\begin{aligned} P_{K+1,s,j}(h) \;=\; & (j-s-K)P_{K,s,j}(h)+P_{K,s-1,j}(h)+(K-j+1)P_{K,s,j-1}(h)\\ & -hKP_{K-1,s,j}(h)+hKP_{K-1,s,j-1}(h)\,. \end{aligned}$$

Complete Spectral Decomposition of the Mean Value of any Automorphic *L*-function — A unified approach

Yoichi Motohashi

We report on our recent resolution of the longstanding problem of constructing a unified theory for the complete spectral expansion of the mean value

$$\mathcal{M}(L_\psi,g)=\int_{-\infty}^{\infty}\left|L_\psi(\tfrac12+it)\right|^2 g(t)dt,$$

where L_ψ is the L-function associated with an arbitrary automorphic form ψ of one complex variable, under the normalization given below; the weight g is assumed, for the sake of simplicity, to be even, entire, real-valued on $\mathbb{R}$, and of rapid decay in any horizontal strip.

We consider the pair $G=\mathrm{PSL}(2,\mathbb{R})$, $\Gamma=\mathrm{PSL}(2,\mathbb{Z})$, which is not too restrictive; in fact our argument extends considerably. Then, there are three types of automorphic forms ψ: (1) holomorphic cusp forms of even integral weights $2k\ge 12$, (2) real analytic cusp forms, and (3) Eisenstein series. The Fourier expansions for (1) and (2) are, respectively,

$$\textstyle\sum_{n=0}^{\infty}a_\psi(n)n^{k-\frac12}\exp(2\pi inz) \text{ and } \sqrt{y}\sum_{n=-\infty}^{\infty}a_\psi(n)K_\nu(2\pi|n|y)\exp(2\pi inx),$$

with $a_\psi(0)=0$, and that of (3) is analogous to the latter save for a term constant with respect to x. Here $z=x+iy$, $x\in\mathbb{R}$, $y>0$; $y^2\left(\partial_x^2+\partial_y^2\right)\psi=\left(\nu^2-\frac14\right)\psi$ with a certain constant ν, and K_ν is the K-Bessel function of order ν. With the Fourier coefficients $\{a_\psi(n)\}$ we form the L-function: $L_\psi(s)=\sum_{n=1}^{\infty}a_\psi(n)n^{-s}$, $\mathrm{Re}\,s>1$.

A. Good treated, in early 1980's, the case (1), and we dealt in [3] with $\mathcal{M}(\zeta^2,g)$ the fourth moment of the Riemann zeta-function which corresponds to the case (3). Complete spectral expansions for the respective mean values were obtained. However, the case (2) has had a slow development. To make explicit the reason for this, we begin with the expression

$$\mathcal{M}(L_\psi,g)=\lim_{(u,v)\to(\frac12,\frac12)}\int_{-\infty}^{\infty}L_\psi(u+it)\overline{L_\psi(\bar v+it)}g(t)dt,$$

for the cases (1), (2); and in (3) the same holds with a residual contribution added. In the region of absolute convergence, the off-diagonal part of the last integral is an (extended) additive divisor sum:

$$\mathcal{D}_f(\psi, W) = \sum_{n=1}^{\infty} a_\psi(n)\overline{a_\psi(n+f)}W(n/f), \quad f > 0,$$

where W, entire in (u, v), is derived from g in a natural way; note that the Mellin transform of W decays rapidly but much slower than exponentially. We then encounter a very basic problem: how to capture $\mathcal{D}_f(\psi, W)$ in the context of the Γ-automorphy structure. To this end, Good and we exploited, respectively, the facts: in the case (1) exp is an 'additive' character and in (3) $a_\psi = \sigma_c$, sum of powers of divisors, has an 'inner' structure. However, any analogous argument does not work in the case (2), for K_ν is not an additive character and a_ψ does not have anything like the inner structure of σ_c.

To this difficulty one may approach with the following naïve idea: *Try to modify ψ so that the result is almost like a holomorphic function on the upper half plane, while retaining the automorphy.* In [4, Part XIV] we showed that this is indeed possible, if ψ is regarded as a function not on the upper half plane but on G or more precisely on G/K, $K = \left\{ \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \right\}$. The key is the L^2-structure of the irreducible subspace $V \subset L^2(\Gamma\backslash G)$ that contains ψ as its vector of weight zero; that is, representations of G in $L^2(\Gamma\backslash G)$ comes into our view. Then we have the Jacquet normalization and the Kirillov model: namely, the universal rôle of $\{a_\psi(n)\}$ as to be the Fourier coefficients of all vectors in V as well as the existence of the isometry $V \simeq L^2(\mathbb{R}^\times, d^\times)$ with $d^\times x = dx/\pi|x|$. That is, for any $\xi \in L^2(\mathbb{R}^\times, d^\times)$, there exists a $\Psi(\cdot, \xi) \in V$ such that $\Psi\left(\mathrm{n}[x]\mathrm{a}[y], \xi\right) = \sum_{n=1}^{\infty} a_\psi(n)\xi(2\pi ny)\exp(2\pi inx)$, where $\mathrm{n}[x] = \left(\begin{smallmatrix} 1 & x \\ & 1 \end{smallmatrix}\right)$, $\mathrm{a}[y] = \begin{pmatrix} \sqrt{y} & \\ & 1/\sqrt{y} \end{pmatrix}$, $x \in \mathbb{R}$, $y > 0$. Then, the function $\Psi\left(\mathrm{n}[x]\mathrm{a}[y], \xi_\sigma\right)$ with $\xi_\delta(y) = y^\delta \exp(-y)$, $\delta > 0$, should look like a holomorphic function on the upper half plane.

With this, we have, for $\mathrm{Re}\, s > 1$,

$$\begin{aligned} &\frac{2^{2\delta}(2\pi)^s}{\Gamma(s+2\delta)} \int_0^\infty \left\{ \int_0^1 \left|\Psi(\mathrm{n}[x]\mathrm{a}[y], \xi_\delta)\right|^2 \exp(2\pi ifx)dx \right\} y^{s-1}dy \\ &= \sum_{n=1}^{\infty} \frac{a_\psi(n)\overline{a_\psi(n+f)}}{(2n+f)^s} \left(1 - \left(\frac{f}{2n+f}\right)^2\right)^\delta. \end{aligned}$$

The right side is essentially the (extended) additive-divisor zeta-function associated with ψ. Spectrally decompose $|\Psi(\cdot, \xi_\delta)|^2$ in $L^2(\Gamma\backslash G)$ and insert the result into the left side. A full spectral decomposition of our additive divisor zeta-function follows. Then, multiply both sides of the decomposition by a modification of the Mellin transform of W and integrate. This procedure should give rise to a full spectral decomposition of $\mathcal{D}_f(\psi, W)$ and consequently that of $\mathcal{M}(L_\psi, g)$,... but

only formally. To make the matter rigorous, we have to prove that the spectral decomposition of our additive divisor zeta-function is absolutely and uniformly convergent at least in the half-plane $\operatorname{Re} s > \frac{1}{2}$ and that each spectral contribution of the result of the continuation is of polynomial growth; the former is necessary because of the above limiting procedure with $(u, v) \to (\frac{1}{2}, \frac{1}{2})$ and the latter because of the nature of the Mellin transform of W mentioned above. (Here Jutila's unified but approximative treatment [2] should be referred to, with which he proved the analytic continuation and the polynomial growth of the additive-divisor zeta-function, though leaving the full spectral decomposition open. See also [5].)

This issue was recently settled in [1] and [4, Part XV] independently. Our argument in the latter is simpler than that in the former, and similar to Ju.V. Linnik's on his derivation of the uniform approximate functional equation for Dirichlet L-functions: We only replace $\xi_\delta(y)$ by $\xi_\delta(y, s) = y^\delta \exp(-sy)$ with $\operatorname{Re} s > 0$, and $|\Psi(\cdot, \xi_\sigma)|^2$ by $\Psi(\cdot, \xi_\delta(\cdot, s))\overline{\Psi(\cdot, \xi_\delta(\cdot, \bar{s}))}$. This kills the exponential growth of the annoying factor $1/\Gamma(s + 2\delta)$. The absolute and uniform convergence for $\operatorname{Re} > \frac{1}{2}$ of the spectral decomposition of $\Psi(\cdot, \xi_\delta(\cdot, s))\overline{\Psi(\cdot, \xi_\delta(\cdot, \bar{s}))}$ can be derived from a uniform bound for Whittaker functions with variable orders and weights, such as given in Section 2 of [4, Part XV].

In this way we obtain, after a careful handling of the limiting procedure,

Theorem ([4, Part XV]). *With the above specifications, we have, for any automorphic form ψ, the spectral decomposition*

$$\mathcal{M}(L_\psi, g) = \text{Main term} + \sum_V + \int .$$

Here V runs over all irreducible cuspidal representations and the integral stands for the contribution of the continuous spectrum, which occur in $L^2(\Gamma\backslash G)$. All terms are explicit with respect to the weight g and the spectral data.

Concluding remark. The first paragraph of Section 4 of [4, Part XV] should be augmented: Harcos kindly sent us a copy of [1] in March 2007. Our exploitation of the Kirillov model was adopted there, and the authors devised their own argument for the analytic continuation and the polynomial growth in question. Shortly afterward we realized that our investigations subsequent to [4, Part XIV] as well had in fact yielded the same already, even in a simpler and more direct way as rendered above.

References

[1] V. Blomer and G. Harcos. The spectral decomposition of shifted convolution sums. arXiv: math/0703246.

[2] M. Jutila. The additive divisor problem and its analogs for Fourier coefficients of cusp forms. I. Math. Z. **223** (1996), 435–461; II. ibid, **225** (1997), 625–637.

[3] Y. Motohashi. *Spectral Theory of the Riemann Zeta-Function*. Cambridge Univ. Press, Cambridge 1997.

[4] Y. Motohashi. A note on the mean value of the zeta and L-functions. XIV. Proc. Japan Acad., **80A** (2004), 28–33; XV. ibid, **83A** (2007), 73–78.
[5] P. Sarnak. Integrals of products of eigenfunctions. Int. Math. Res. Notes, **6** (1994), 251–260.

New estimates for multidimensional Weyl sums

Scott T. Parsell

Let k and d be positive integers, and write $\ell = \binom{k+d-1}{k}$. Further let P be a positive real number, and consider the exponential sum

$$f(\boldsymbol{\alpha}) = \sum_{\mathbf{x} \in [1,P]^d} e\left(\sum_{|\mathbf{i}|=k} \alpha_{\mathbf{i}} \mathbf{x}^{\mathbf{i}} \right),$$

where $\mathbf{x}^{\mathbf{i}} = x_1^{i_1} \cdots x_d^{i_d}$ and $|\mathbf{i}| = i_1 + \cdots + i_d$. We observe that the mean value

$$I_{s,k,d}(P) = \int_{[0,1]^\ell} |f(\boldsymbol{\alpha})|^{2s} d\boldsymbol{\alpha}$$

counts solutions of the system of diophantine equations

$$\mathbf{x}_1^{\mathbf{i}} + \cdots + \mathbf{x}_s^{\mathbf{i}} = \mathbf{y}_1^{\mathbf{i}} + \cdots + \mathbf{y}_s^{\mathbf{i}} \qquad (|\mathbf{i}| = k)$$

with $\mathbf{x}_j, \mathbf{y}_j \in [1,P]^d \cap \mathbb{Z}^d$ for $1 \le j \le s$. By applying estimates of the author [3] for the number of solutions of the corresponding complete system, which includes each $\mathbf{i}$ with $1 \le |\mathbf{i}| \le k$, and adapting the method of Ford [2], we obtain estimates of the shape

$$I_{t,k,d}(P) \ll P^{2td - k\ell + \Delta(t,k,d)},$$

where $\Delta(t,k,d)$ becomes small when $t \gg k^{d+1} \log k$. Next we use the large sieve to generalize a result of Bombieri [1], which provides an upper bound for $|f(\boldsymbol{\alpha})|$ when some $\alpha_{\mathbf{i}}$ is well-approximated by a rational number with moderately large denominator. Combining this with the argument of Wooley [4] yields new estimates of the shape

$$\sup_{\boldsymbol{\alpha} \in \mathfrak{m}} |f(\boldsymbol{\alpha})| \ll P^{d - \sigma(k,d) + \varepsilon},$$

where $\mathfrak{m}$ is a suitably defined set of minor arcs. It follows that the contribution to $I_{t+u,k,d}(P)$ arising from $\mathfrak{m}$ is negligible whenever $\Delta(t,k,d) < 2u\sigma(k,d)$. After making optimal choices for t and u, we obtain the asymptotic formula

$$I_{s,k,d}(P) = c(s,k,d) P^{2sd - k\ell}(1 + O(P^{-\delta})),$$

where $c(s,k,d) > 0$ is the usual product of local densities, provided that

$$s \ge \tfrac{4d-1}{6d!} k^{d+1}(\log k + O(\log\log k)).$$

References

[1] E. Bombieri, *On Vinogradov's mean value theorem and Weyl sums*, Proceedings of the conference on automorphic forms and analytic number theory, Univ. Montreal, 1990, pp. 7–24.
[2] K. B. Ford, *New estimates for mean values of Weyl sums*, Internat. Math. Res. Notices (1995), 155–171.
[3] S. T. Parsell, *A generalization of Vinogradov's mean value theorem*, Proc. London Math. Soc. (3) **91** (2005), 1–32.
[4] T. D. Wooley, *New estimates for Weyl sums*, Quart. J. Math. Oxford (2) **46** (1995), 119–127.

A converse theorem for Dirichlet L-functions

Alberto Perelli
(joint work with J.Kaczorowski and G.Molteni)

A well known theorem by Hamburger states that the Riemann zeta function $\zeta(s)$ is determined by its functional equation in the following sense. Let $f(s)$ be a Dirichlet series, absolutely convergent for $\sigma > 1$ and such that $(s-1)f(s)$ is entire of finite order, and let $f(s)$ satisfy the functional equation

$$\pi^{-s/2}\Gamma\big(\frac{s}{2}\big)f(s) = \pi^{-(1-s)/2}\Gamma\big(\frac{1-s}{2}\big)f(1-s).$$

Then $f(s) = c\zeta(s)$ for some $c \in \mathbb{C}$. In fact, the same conclusion holds under somewhat weaker conditions; we refer to Piatetski-Shapiro and Raghunathan [2], and to the literature quoted there, for an interesting discussion of the above theorem, especially in connection with uniqueness properties of the Poisson summation formula.

In general, the analogue of Hamburger's theorem does not hold for Dirichlet L-functions, and it is natural to address the following question: under what conditions a functional equation has only one solution in the set of Dirichlet L-functions ? As we shall see in Theorem 1 below, the question essentially asks for an analog of Hamburger's theorem where the Euler product is added to the standard analytic properties. We characterize the moduli q such that all the functional equations (mod q) have only one solution in the set of Dirichlet L-functions.

We recall that [1] contains a general converse theorem for degree 1 L-functions in the Selberg class $\mathcal{S}$, namely that $\zeta(s)$ and $L(s+i\theta,\chi)$ with χ primitive and $\theta \in \mathbb{R}$ are the only L-functions of degree 1 in $\mathcal{S}$. Using this result and Theorem 2 below we can prove the following general version of Hamburger's theorem for Dirichlet L-functions. For a primitive character χ (mod q), let $W(\chi)$ be the set of Dirichlet series $F(s)$ satisfying the following three conditions:

(i) the coefficients $a(n)$ of $F(s)$ satisfy $a(n) \ll n^{\varepsilon}$ for every $\varepsilon > 0$ and $(s-1)^m F(s)$ is an entire function of finite order for some integer m;

(ii) $\log F(s)$ is a Dirichlet series with coefficients $b(n)$ satisfying $b(n) = 0$ unless n is a prime-power, and $b(n) \ll n^{\vartheta}$ for some $\vartheta < 1/2$;

(iii) $F(s)$ satisfies the functional equation

$$(1) \qquad \Big(\frac{q}{\pi}\Big)^{s/2}\Gamma\Big(\frac{s+a(\chi)}{2}\Big)F(s) = \omega_\chi\Big(\frac{q}{\pi}\Big)^{(1-s)/2}\Gamma\Big(\frac{1-s+a(\chi)}{2}\Big)\overline{F(1-\overline{s})}.$$

Note that clearly $L(s,\chi)$ belongs to $W(\chi)$, and that condition *(ii)* means that $F(s)$ is a rather general Euler product. We also denote by $\mathbb{Q}$ the set of non-negative integers $q \not\equiv 2 \pmod 4$ of the form $q = 2^a 3^b m$, with m square-free and $(m,6) = 1$, and satisfying at least one of the following two conditions:

(a) $a \in \{0,2,3,4,5\}$ and $b \in \{0,1\}$;
(b) $a \in \{0,2,3\}$ and $b = 2$.

Theorem 1. *If $q \in \mathbb{Q}$ then $W(\chi) = \{L(s,\chi)\}$ for every primitive character $\chi \pmod q$, while if $q \notin \mathbb{Q}$, $q \not\equiv 2 \pmod 4$, there exists a primitive character $\chi \pmod q$ such that $W(\chi)$ contains $L(s,\chi)$ and at least another $L(s,\psi)$ with primitive $\psi \pmod q$.*

As remarked in [1], the above conditions defining $W(\chi)$ can be weakened, and still the same result follows. For example, the Ramanujan conjecture $a(n) \ll n^{\varepsilon}$ in *(i)* is not necessary, the weaker assumption that $F(s)$ is absolutely convergent for $\sigma > 1$ being sufficient. Hence Theorem 1 may be expressed by saying that for $q \in \mathbb{Q}$, every primitive Dirichlet L-function $(\mathrm{mod}\ q)$ is characterized by the functional equation and the multiplicativity of the coefficients.

The following result is crucial for Theorem 1 and also of independent interest. Given $q \not\equiv 2 \pmod 4$, let s_q be the map sending each primitive character $\chi \pmod q$ into its signature $s(\chi) = (a(\chi), \tau(\chi))$ (parity and Gauss sum). We have

Theorem 2. *The map s_q is injective if and only if $q \in \mathbb{Q}$.*

Corollary. *The functional equations of the $L(s,\chi)$'s with χ primitive $\pmod q$ are all distinct if and only if $q \in \mathbb{Q}$.*

Theorem 1 follows at once from the Corollary and the results in [1]. Theorem 2 is based on elementary Galois theory and a certain decomposition of primitive characters modulo prime-powers.

References

[1] J.Kaczorowski, A.Perelli - *On the structure of the Selberg class, I: $0 \le d \le 1$* - Acta Math. **182** (1999), 207–241.

[2] I.Piatetski-Shapiro, R.Raghunathan - *On Hamburger's theorem* - Amer. Math. Soc. Translations (2) **169** (1995), 109–120.

Gaps between primes and Goldbach numbers

János Pintz

There are many famous conjectures about gaps between primes and Goldbach numbers. We list some of them below (p_n denotes the n^{th} prime; $g_1 = 4$, $g_2 = 6$, $\dots g_n$ denotes the n^{th} Goldbach number, that is, the n^{th} even natural number which can be expressed as a sum of two primes).

Twin Prime Conjecture. $p_{n+1} - p_n = 2$ *infinitely often.*

Bounded Gap Conjecture. *There exists an absolute constant C, such that $p_{n+1} - p_n \le C$ infinitely often.*

Large Gap Conjecture for Primes. *We have for every $\varepsilon > 0$*

$$p_{n+1} - p_n \ll_\varepsilon p_n^\varepsilon \quad \text{for every } n.$$

Statistical Large Gap Conjecture for Primes. *For every $\varepsilon > 0$ and for all $x > x_0(\varepsilon)$ we have at least one prime number in the interval $[y, y + y^\varepsilon]$ for almost all $y \in [x, 2x]$.*

Large Gap Conjecture for Goldbach numbers.

$$g_{n+1} - g_n \ll_\varepsilon g_n^\varepsilon \quad \text{for every } \varepsilon > 0.$$

It is well known that the Statistical Large Gap Conjecture for Primes implies the Large Gap Conjecture for Goldbach numbers. This can be interpreted in the way that if large gaps between primes are rare then there are no large gaps between Goldbach numbers. In the lecture a proof of the following surprising fact is sketched: if bounded gaps between primes are rare then there are no large gaps between Goldbach numbers. We have to remark, however, that 'rare' means in this context a much lower density than the expected one, which is $C(\log x)^{-2}$. To formulate the phenomenon more simply, we state the following result.

Theorem. *At least one of the following two conjectures is true:*

(i) *The Bounded Gap Conjecture.*

(ii) *The Large Gap Conjecture for Goldbach numbers.*

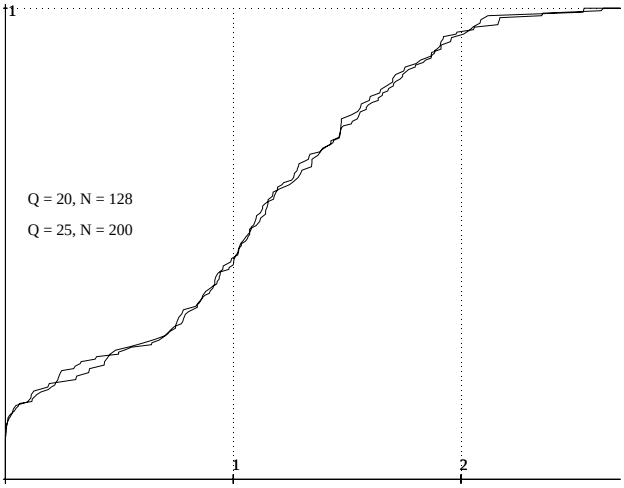
Eigenvalues in the large sieve inequality

Olivier Ramaré

The large sieve inequality applied to the Farey sequence [2], [4] reads

$$\sum_{q\le Q}\sum_{a \bmod {}^*q}\Big|\sum_{n\le N}\varphi_n e(na/q)\Big|^2 \le \sum_{n\le N}|\varphi_n|^2(N+Q^2)$$

where $e(\alpha)=\exp(2i\pi\alpha)$. Notice that there are $\Phi(Q)=\sum_{q\le Q}\phi(q)\sim 3Q^2/\pi^2$ fractions a/q. We are mainly concerned with the behaviour of the left-hand side hermitian form when Q is of order $\sqrt{N}$. Let us denote by $\lambda_1,\lambda_2,\cdots,\lambda_N$ its eigenvalues. The simplest guess would be to claim that they are all close to N, as happens when $Q=o(\sqrt{N})$, see [1]. In case $N=\Phi(Q)$, $Q=20$ or $Q=25$, we plotted the distribution function $\mathscr{D}(N,Q,\lambda)=\#\{i/\lambda_i\le\lambda N\}/N$ and obtained



A strong asymptotic behaviour appears which is not the simplest one we mentioned. We further numerically show that this behaviour is *not* the one arising when replacing the a/q's by randomly chosen points, even if we force them to be at least $1/Q^2$ apart. In order to confirm the existence of an asymptotic distribution, we evaluate the moment of order 2. When $\Phi(Q)=N$, our result states that

$$N^{-1}\sum_i(N^{-1}\lambda_i-1)^2=0.4477\ldots$$

In general, the corresponding dispersion equals $\mathfrak{f}(N/Q^2)$ for a fairly mysterious function $\mathfrak{f}$. Most of the material presented comes from [3].

References

[1] I. Kobayashi. A note on the Selberg sieve and the large sieve. *Proc. Japan Acad.*, 49(1):1–5, 1973.
[2] H.L. Montgomery and R.C. Vaughan. The large sieve. *Mathematika*, 20(2):119–133, 1973.
[3] O. Ramaré. Eigenvalues in the large sieve inequality. *Funct. Approximatio, Comment. Math.*, 37:7–35, 2007.

[4] A. Selberg. Collected papers. *Springer-Verlag*, II:251pp, 1991.

The sum of digits of primes and squares

Joël Rivat
(joint work with Christian Mauduit)

1. The sum of digits function

Let q be an integer with $q \geqslant 2$. Every integer $n \geqslant 0$ can be written uniquely in basis q:

$$n = \sum_{k \geqslant 0} n_k q^k \quad \text{where } n_k \in \{0, \dots, q-1\}$$

and the sum of digits function is defined by:

$$\sigma(n) = \sum_{k \geqslant 0} n_k.$$

This function has many aspects that have been studied, for instance ergodicity, finite automata, dynamical systems, number theory.

The origin of our work is the following result of Gelfond:

Theorem A (Gelfond [6], 1968)**.** *Let $m \geqslant 2$, $(m, q-1) = 1$. Then there exists $\lambda < 1$ such that for all $d \geqslant 1$, $a,\ r \in \mathbb{Z}$, we have*

$$\sum_{\substack{n<N \\ n \equiv r \bmod d \\ \sigma(n) \equiv a \bmod m}} 1 = \frac{N}{md} + O(N^\lambda).$$

In the same paper Gelfond pose the following two problems:

1 Evaluate the number of prime numbers $p \leqslant x$ such that $\sigma(p) \equiv a \bmod m$.
2 Evaluate the number of integers $n \leqslant x$ such that $\sigma(P(n)) \equiv a \bmod m$, where P is a suitable polynomial *[for example $P(n) = n^2$]*.

2. Digits and primes – Historical background

Until recently, very little was known concerning the digits of prime numbers. We can mention a result of Sierpiński [11] (1959), recently generalized by Wolke [12] (2005) and then by Harman [7] (2006), on prime numbers with some prescribed digits.

Concerning Gelfond's question, no progress was made in its original form. Let us mention the two following variants:

Theorem B (Fouvry–Mauduit [4, 5], 1996)**.** *For $m \geqslant 2$ such that $(m, q-1) = 1$, there exists $C(q,m) > 0$ such that for all $a \in \mathbb{Z}$ and $x > 0$, we have*

$$\sum_{\substack{n\leqslant x\\ n=p \text{ or } n=p_1p_2\\ \sigma(n)\equiv a \bmod m}} 1 \geqslant \frac{C(q,m)}{\log\log x} \sum_{\substack{n\leqslant x\\ n=p \text{ or } n=p_1p_2}} 1.$$

Theorem C (Dartyge–Tenenbaum [1], 2005)**.** *For $m \geqslant 2$ with $(m, q-1) = 1$ and $r \geqslant 2$, there exists $C(q,m,r) > 0$ such that for all $a \in \mathbb{Z}$ and $x > 0$, we have*

$$\sum_{\substack{n\leqslant x\\ n=p_1\dots p_r\\ \sigma(n)\equiv a \bmod m}} 1 \geqslant \frac{C(q,m,r)}{\log\log x \log\log\log x} \sum_{\substack{n\leqslant x\\ n=p_1\dots p_r}} 1.$$

3. Digits and primes – Results

Theorem 1 (Mauduit-Rivat [8])**.** *For $\alpha \in \mathfrak{Re}$ such that $(q-1)\alpha \in \mathfrak{Re} \setminus \mathbb{Z}$, there exists $C(q,\alpha) > 0$ and $\sigma_q(\alpha) > 0$, with*

$$\left|\sum_{p\leqslant x} \exp(2i\pi\alpha\sigma(p))\right| \leqslant C(q,\alpha)\ x^{1-\sigma_q(\alpha)}.$$

Corollary 1. *The sequence $(\alpha\sigma(p_n))_{n\geqslant 1}$ is equidistributed modulo 1 if and only if $\alpha \in \mathfrak{Re} \setminus \mathbb{Q}$ (here $(p_n)_{n\geqslant 1}$ denotes the sequence of prime numbers).*

Corollary 2. *For $m \geqslant 2$ such that $(m, q-1) = 1$ and $a \in \mathbb{Z}$, we have*

$$\sum_{\substack{p\leqslant x\\ \sigma(p)\equiv a \bmod m}} 1 \ \sim\ \frac{1}{m}\sum_{p\leqslant x} 1 \quad (x \to +\infty).$$

4. Digits and squares – Historical background

Until recently, very little was known concerning the digits of squares. We can mention a result of Davenport and Erdös (1952), later improved by Peter (2002) [10].

Theorem D (Consequence of Davenport-Erdös [3], , 1952)**.**

$$\sum_{n\leqslant x} \sigma(n^2) \sim (q-1)\ x\ \frac{\log x}{\log q} \quad (x \to +\infty).$$

Erdös considered that passing from such a mean result to a local result like the question of Gelfond *"hopelessly difficult"*. However, Dartyge and Tenenbaum succeeded to obtain a positive density:

Theorem E (Dartyge-Tenenbaum [2], 2005)**.** *For $m \geqslant 2$ such that $(m, q-1) = 1$, there exists $C(q,m) > 0$ and $x_0(q,m) \geqslant 1$ such that for all $a \in \mathbb{Z}$ and $x \geqslant x_0(q,m)$, we have*

$$\sum_{\substack{n \leqslant x \\ \sigma(n^2) \equiv a \bmod m}} 1 \geqslant C(q,m)\ x.$$

5. Digits and squares – Results

Theorem 2 (Mauduit-Rivat [9])**.** *For $\alpha \in \Re\mathrm{e}$ such that $(q-1)\alpha \in \Re\mathrm{e} \setminus \mathbb{Z}$, there exist $C(q,\alpha) > 0$ and $\sigma_q(\alpha) > 0$, with*

$$\left| \sum_{n \leqslant x} \exp(2i\pi\alpha\sigma(n^2)) \right| \leqslant C(q,\alpha)\ x^{1-\sigma_q(\alpha)}.$$

Corollary 3. *The sequence $(\alpha\sigma(n^2))_{n\geqslant 1}$ is equidistributed modulo 1 if and only if $\alpha \in \Re\mathrm{e} \setminus \mathbb{Q}$.*

Corollary 4. *For $m \geqslant 2$ such that $(m, q-1) = 1$ and $a \in \mathbb{Z}$, we have*

$$\sum_{\substack{n \leqslant x \\ \sigma(n^2) \equiv a \bmod m}} 1 \ \sim\ \frac{x}{m} \quad (x \to +\infty).$$

6. Methods

For $s(p)$, the key argument is the control of carry propagation using the van der Corput inequality, which permits to remove almost the half of the digits. Concerning $s(n^2)$, this idea is applied twice with a variant of the van der Corput inequality, making possible to keep only a few digits. The rest of the proof involve elementary but complicated analytic number theory, together with very precise estimates of the quantities $\max_{h\in\mathbb{Z}} |F_\lambda(h,\alpha)|$ and $\sum_{0\leqslant h<q^\lambda} |F_\lambda(h,\alpha)|$ where

$$F_\lambda(h,\alpha) = q^{-\lambda} \sum_{0\leqslant u<q^\lambda} \exp\left(2i\pi\left(\alpha\sigma(u) - \frac{hu}{q^\lambda}\right)\right).$$

References

[1] C. Dartyge and G. Tenenbaum, *Sommes des chiffres de multiples d'entiers*, Ann. Inst. Fourier (Grenoble), **55** (2005), pp. 2423–2474.

[2] C. Dartyge and G. Tenenbaum, *Congruences de sommes de chiffres de valeurs polynomiales*, Bull. London Math. Soc. **38**,1 (2006), 61–69.

[3] H. Davenport and P. Erdös, *Note on normal decimals*, Canadian J. Math. **4** (1952), 58–63.

[4] E. Fouvry and C. Mauduit, *Sommes des chiffres et nombres presques premiers*, Mathematische Annalen, **305** (1996), pp. 571–599.

[5] E. Fouvry and C. Mauduit, *Méthodes de crible et fonctions sommes des chiffres*, Acta Arithmetica, **77** (1996), pp. 339–351.

[6] A. O. Gelfond, *Sur les nombres qui ont des propriétés additives et multiplicatives données*, Acta Arith., **13** (1968), pp. 259–265.

[7] G. Harman, *Primes with preassigned digits*, Acta Arith., **125** (2006), pp. 179–185.
[8] C. Mauduit and J. Rivat, *Sur un problème de Gelfond: la somme des chiffres des nombres premiers*, Annals of Mathematics, to appear.
[9] C. Mauduit and J. Rivat, *La somme des chiffres des carrés*, Acta Mathematica, to appear.
[10] M. Peter, *The summatory function of the sum-of-digits function on polynomial sequences*, Acta Arith. **104**,1 (2002), 85–96.
[11] W. Sierpiński, *Sur les nombres premiers ayant des chiffres initiaux et finals donnés*, Acta Arith., **5** (1959), pp. 265–266.
[12] D. Wolke, *Primes with preassigned digits*, Acta Arith., **119** (2005), pp. 201–209.

Statistics of zeros for families of zeta functions of curves over a finite field

Zeév Rudnick
(joint work with Dmitry Faifman)

Let C be a smooth, projective curve of genus $g \geqslant 1$ defined over a finite field $\mathcal{F}_q$ of cardinality q. The zeta function of the curve is defined as

$$Z_C(u) := \exp \sum_{n=1}^{\infty} N_n \frac{u^n}{n}, \quad |u| < 1/q$$

where N_n is the number of points on C with coefficients in an extension $\mathcal{F}_{q^n}$ of $\mathcal{F}_q$ of degree n. The zeta function is a rational function of the form

$$Z_C(u) = \frac{P_C(u)}{(1-u)(1-qu)}$$

where $P_C(u) \in \mathbb{Z}[u]$ is a polynomial of degree $2g$, with $P(0) = 1$, satisfies the functional equation

$$P_C(u) = (qu^2)^g P_C(\frac{1}{qu})$$

and has all its zeros on the circle $|u| = 1/\sqrt{q}$ (this is the Riemann Hypothesis for curves - Weil's theorem [5]). Moreover there is some unitary symplectic matrix $\Theta_C \in USp(2g)$, defined up to conjugacy, so that

$$P_C(u) = \det(I - u\sqrt{q}\Theta_C)$$

The eigenvalues of Θ_C are of the form $e^{2\pi i \theta_{C,j}}$, $j = 1, \ldots, 2g$.

Our goal is to study the statistics of the set of angles $\{\theta_{j,C}\}$ as we draw C at random from a family of hyperelliptic curves of genus g defined over $\mathcal{F}_q$ where q is assumed to be odd. The family, denoted by $\mathcal{H}_{2g+2,q}$, is that of curves having an affine equation of the form $y^2 = Q(x)$, with $Q \in \mathcal{F}_q[x]$ a monic, square-free polynomial of degree $2g+2$. The measure on $\mathcal{H}_{2g+2,q}$ is simply the uniform probability measure on the set of such polynomials Q.

Katz and Sarnak [1] showed that for fixed genus, as C varies in $\mathcal{H}_{2g+2,q}$, the conjugacy classes Θ_C become uniformly distributed in $USp(2g)$ in the limit of large constant field size and fixed genus. Thus in that limit, various statistics of

the conjugacy classes Θ_C coincide with the corresponding ones in $USp(2g)$. Our results aim for the opposite case, of constant field size and large genus.

A fundamental statistic is the counting function of the angles. Thus for an interval $\mathcal{I}$ let

$$N_{\mathcal{I}}(C) = \#\{j : \theta_{j,C} \in \mathcal{I}\}$$

Asymptotically as $g \to \infty$, the angles are uniformly distributed: For fixed $\mathcal{I}$,

$$N_{\mathcal{I}}(C) \sim 2g|\mathcal{I}| \, .$$

In joint work with D. Faifman, we study the fluctuations of $N_{\mathcal{I}}$ as we vary C in $\mathcal{H}_{2g+2,q}$. This is in analogy to the work of Selberg [2, 3, 4], who studied the fluctuations in the number $N(t)$ of zeros of the Riemann zeta function up to height t.

We find that for a fixed constant field, in the limit of large genus, for both the global regime ($|\mathcal{I}|$ fixed) and the mesoscopic regime ($|\mathcal{I}| \to 0$ while $2g|\mathcal{I}| \to \infty$), the variance of $N_{\mathcal{I}}$ is asymptotically $\frac{2}{\pi^2}\log(2g|\mathcal{I}|)$ and that the fluctuations are Gaussian, that is for fixed $a < b$,

$$\lim_{g\to\infty} \mathrm{Prob}_{\mathcal{H}_{2g+2,q}}\left(a < \frac{N_{\mathcal{I}} - 2g|\mathcal{I}|}{\sqrt{\frac{2}{\pi^2}\log(2g|\mathcal{I}|)}} < b\right) = \frac{1}{\sqrt{2\pi}}\int_a^b e^{-x^2/2}dx$$

An important and open challenge is the local regime, when the length of the interval is of order $1/2g$ as $g \to \infty$.

References

[1] N.M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*. American Mathematical Society Colloquium Publications, **45**. American Mathematical Society, Providence, RI, 1999.

[2] A. Selberg *On the remainder in the formula for $N(T)$, the number of zeros of $\zeta(s)$ in the strip $0 < t < T$*. Avh. Norske Vid. Akad. Oslo. I. 1944, (1944). no. 1, 1–27.

[3] A. Selberg *Contributions to the theory of the Riemann zeta-function*. Arch. Math. Naturvid. **48**, (1946). no. 5, 89–155.

[4] A. Selberg *Contributions to the theory of Dirichlet's L-functions*. Skr. Norske Vid. Akad. Oslo. I. 1946, (1946). no. 3, 1–62.

[5] A. Weil *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Hermann, Paris (1948).

An improved version of the inductive method for zero-sum problems

Jan-Christoph Schlage-Puchta

(joint work with Gautami Bhowmik, Immanuel Halupczok)

Let G be a finite abelian group. Define $D(G)$, the Davenport constant of G, to be the least integer k such that every sequence $g_1, \dots, g_k$ of elements in G contains a non-empty subsequence $g_{i_1}, \dots, g_{i_\ell}$, $1 \leqslant i_1 < \dots < i_\ell \leqslant k$ adding up to 0. Writing $G \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \dots \oplus \mathbb{Z}_{n_k}$ with $n_1|n_2|\dots|n_k$, we have the obvious lower bound

$D(G) \geqslant M(G) := \sum_{i=1}^{k}(n_i - 1) + 1$. While $D(G) = M(G)$ for groups of rank $\leqslant 2$ and for p-groups, in general this equality fails to hold, and at present there is no conjecture concerning the exact value of $D(G)$ for groups of rank $\geqslant 4$.

One way of proving upper bounds for $D(G)$ is the inductive method: Decompose $G = H \oplus K$. Suppose that every sequence of N elements in H contains a disjoint system consisting of $D(K)$ non-empty zero-sums. Then $D(G) \leqslant N$. In fact, if $g_1, \ldots, g_N$ is a sequence of elements in G, write $g_i = (h_i, k_i)$ with $h_i \in H$, $k_i \in K$. If $h_{i_1} + \cdots + h_{i_\ell} = 0$ in H, then $g_{i_1} + \cdots + g_{i_\ell}$ defines an element in K, and among sufficiently many such elements we can choose a non-empty zero-sum. Unfortunatelly, in general this method does not give optimal bounds, which is caused by the fact that the system of disjoint zero-sums in H can be chosen in a variety of ways, and only one choice is actually used.

If we understand large zero-sum free subsets of K sufficiently well, this problem can be solved. For example, let H be a fixed group, n an integer coprime to $|H|$, and set $G = H \oplus \mathbb{Z}_n$. Suppose that among N elements in H we can always find a system of $n-1$ disjoint zero-sums, and that there are no sequences $h_1, \ldots, h_N \in H$, $x_1, \ldots, x_N \in \mathbb{Z}_n$, such that for any system of $n-1$ disjoint zero-sums $Z_1, \ldots, Z_{n-1}$ among the h_i we have for every $i \leqslant n-1$ the equation$\sum_{j:h_j \in Z_i} x_j = 1$, then $D(G) \leqslant N$.

To consider all pairs of sequences of length N in H and $\mathbb{Z}_n$ is no easier then considering all sequences of length N in G, however, we can choose zero-sums of length $\leqslant \exp(H)$ whithout considering the corresponding elements in $\mathbb{Z}_n$, in this way turning the problem for arbitrary n into a finite problem of size only depending on the structure of H. We applied this to $H = \mathbb{Z}_3^3$ and showed that $D(G) = M(G)$ holds true for $G = \mathbb{Z}_3^2 \oplus \mathbb{Z}_{3n}$. More generally, if H is a fixed finite group, and $G = H \oplus \mathbb{Z}_n$, we showed that $D(G) - M(G)$ is a computable ultimately periodic function of n.

If K is not cyclic, the structure of zero-sum free sets of maximal size is hardly understood at all. Gao and Geroldinger conjectured, that every zero-sum free subsequece A of $\mathbb{Z}_n^2$ of length $2n-2$ contains one element with multiplicity at least $n-2$. We proved this conjecture for $n \leqslant 19$, and showed that if this conjecture holds true for n, then $D(G) = M(G)$ holds true for $G = \mathbb{Z}_3 \oplus \mathbb{Z}_{3n}$.

Fermat Quotients

Igor E. Shparlinski
(joint work with Jean Bourgain, Kevin Ford and Sergei V. Konyagin)

For a prime p and an integer a the *Fermat quotient* is defined as

$$q_p(a) = \frac{a^{p-1} - 1}{p}.$$

It is well known that divisibility of Fermat quotients $q_p(a)$ by p has numerous applications which include the Fermat Last Theorem and squarefreeness testing, see [4, 5, 6, 11].

In particular, the smallest value ℓ_p of a for which $q_p(a) \not\equiv 0 \pmod p$ plays a prominent role in these applications. In this direction, H. W. Lenstra [11, Theorem 3] has shown that

$$\ell_p \leqslant \begin{cases} 4(\log p)^2, & \text{if } p \geqslant 3, \\ (4e^{-2} + o(1))(\log p)^2, & \text{if } p \to \infty, \end{cases} \tag{1}$$

see also [5]. A. Granville [7, Theorem 5] has shown that in fact

$$\ell_p \leqslant (\log p)^2 \tag{2}$$

for $p \geqslant 5$.

A very different proof of a slightly weaker bound $\ell_p \leqslant (4 + o(1))(\log p)^2$ has recently been obtained by Y. Ihara [9] as a by-product of the estimate

$$\sum_{\substack{\ell^k < p \\ \ell \in \mathcal{W}(p)}} \frac{\log \ell}{\ell^k} \leqslant 2 \log\log p + 2 + o(1), \tag{3}$$

as $p \to \infty$, where the summation is take over all prime powers up to p of primes ℓ from the set

$$\mathcal{W}(p) = \{\ell \text{ prime } : \ \ell < p, \ q_p(\ell) \equiv 0 \pmod p\}.$$

However, the proof of (3), given in [9], is conditional under the Extended Riemann Hypothesis.

It has been conjectured by A. Granville [6, Conjecture 10] that

$$\ell_p = o((\log p)^{1/4}). \tag{4}$$

It is quite reasonable to expect a much stronger bound on ℓ_p. For example, H. W. Lenstra [11] conjectures that in fact $\ell_p \leqslant 3$; this has been supported by extensive computation, see [3, 10]. The motivation to the conjecture (4) comes from the fact, as it is shown in [6], that this is the weakest assumption which has some interesting applications to the Fermat Last Theorem. Although this motivation relating ℓ_p to the Fermat Last Theorem does not exist anymore, improving the bounds (1) and (2) is still of interest and may have some other applications.

Theorem. *We have*

$$\ell_p \leqslant (\log p)^{463/252+o(1)}$$

as $p \to \infty$.

We note that

$$\frac{463}{252} = 1.8373\ldots .$$

Following the arguments of [11], we derive the following improvement of [11, Theorem 2].

Corollary. *For every* $\varepsilon > 0$ *and a sufficiently large integer* n, *if* $a^{n-1} \equiv 1 \pmod n$ *for every positive integer* $a \leqslant (\log p)^{463/252+\varepsilon}$ *then* n *is squarefree.*

The proof of Theorem is based on the original idea of H. W. Lenstra [11], which relates ℓ_p to the distribution of smooth numbers, which we also supplement by some recent results on the distribution of elements of multiplicative subgroups of residue rings of J. Bourgain, S. V. Konyagin and I. E. Shparlinski [2] combined with a bound of D. R. Heath-Brown and S. V. Konyagin [8] for Heilbronn exponential sums.

Theorem. *For every* $\varepsilon > 0$, *there is* $\delta > 0$ *such that for all but* $O(Q^{1-\delta})$ *primes* $p \leqslant Q$, *we have* $\ell_p \leqslant (\log p)^{5/3+\varepsilon}$.

The proof of this result is based on a large sieve inequality with square moduli which is due to S. Baier and L. Zhao [1].

References

[1] S. Baier and L. Zhao, 'An improvement for the large sieve for square moduli', *J. Number Theory*, **128** (2008), 154–174.

[2] 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', *Preprint*, 2008.

[3] R. Crandall, K. Dilcher and C. Pomerance, 'A search for Wieferich and Wilson primes', *Math. Comp.*, **66** (1997), 433–449.

[4] R. Ernvall and T. Metsänkylä, 'On the p-divisibility of Fermat quotients', *Math. Comp.*, **66** (1997), 1353–1365.

[5] W. L. Fouché, 'On the Kummer-Mirimanoff congruences', *Quart. J. Math. Oxford Ser.*, **37** (1986), 257–261.

[6] A. Granville, 'Some conjectures related to Fermat's Last Theorem', *Number Theory*, W. de Gruyter, NY, 1990, 177–192.

[7] A. Granville, 'On pairs of coprime integers with no large prime factors', *Expos. Math.*, **9** (1991), 335–350.

[8] D. R. Heath-Brown and S. V. Konyagin, 'New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum', *Ouart. J. Math.*, **51** (2000), 221–235.

[9] Y. Ihara, 'On the Euler-Kronecker constants of global fields and primes with small norms', *Algebraic Geometry and Number Theory*, Progress in Math., Vol. 850, Birkhäuser, Boston, Cambridge, MA, 2006, 407–451.

[10] J. Knauerand and J. Richstein, 'The continuing search for Wieferich primes', *Math. Comp.*, **74** (2004), 1559–1563.

[11] H. W. Lenstra, 'Miller's primality test', *Inform. Process. Lett.*, **8** (1979), 86–88.

Diophantine inequalities in function fields

Craig V. Spencer

Over 60 years ago, the Davenport-Heilbronn method (see [2]) was introduced to study non-trivial integral solutions of Diophantine inequalities. Let k and s be positive integers with $k > 1$, and let τ be some fixed positive real number. Suppose that $\lambda_1, \dots, \lambda_s$ are non-zero real numbers, not all in rational ratio. Let $N_0(P, \boldsymbol{\lambda})$ denote the number of solutions $\mathbf{x} \in [-P, P]^s \cap \mathbb{Z}^s$ that satisfy

$$|\lambda_1 x_1^k + \cdots + \lambda_s x_s^k| < \tau.$$

Plainly, in the case that k is an even number, we must impose the restriction that the numbers λ_i do not all share the same sign in order to guarantee the existence of a non-trivial solution of $\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0$ in $\mathbb{R}^s$. In [2], Davenport and Heilbronn proved that if $s > 2^k$, then $N_0(P_n, \boldsymbol{\lambda}) \gg P_n^{s-k}$ for a sequence $(P_n)_{n=1}^{\infty}$ which increases to infinity. This sequence is determined from the convergents of the continued fraction expansion for an irrational number of the form λ_i/λ_j, and as a result, the sequence $(P_n)_{n=1}^{\infty}$ may be arbitrarily sparse. In the last decade, the Bentkus-Götze-Freeman version of the Davenport-Heilbronn method (see [1], [3], [4], and [6]) has been used to establish an asymptotic formula for $N_0(P, \boldsymbol{\lambda})$, valid for all large enough values of P, provided that

$$s \geqslant k^2(\log k + \log\log k + O(1)),$$

and an asymptotic lower bound for $N_0(P, \boldsymbol{\lambda})$, valid for all large enough values of P, provided that

$$s \geqslant k(\log k + \log\log k + 2 + o(1)).$$

In this talk, we use the Bentkus-Götze-Freeman version of the Davenport-Heilbronn method to study the analogous problem in function fields.

In order to state our main result, it is first necessary to record some notation. Let $\mathbb{F}_q[t]$ denote the ring of polynomials over $\mathbb{F}_q$, the finite field of q elements. Let $\mathbb{K}_\infty = \mathbb{F}_q((1/t))$ be the completion of $\mathbb{K} = \mathbb{F}_q(t)$ at the infinite place. Each non-zero element α in $\mathbb{K}_\infty$ can be written as $\alpha = \sum_{i \leqslant n} a_i t^i$, where each a_i is an element in $\mathbb{F}_q$ and $a_n \neq 0$. We define $\operatorname{ord}\alpha$ to be n in this situation, and we adopt the convention that $\operatorname{ord} 0 = -\infty$. There exists a natural non-Archimedean valuation $\langle x \rangle = q^{\operatorname{ord} x}$ on $\mathbb{K}_\infty$. For any real number u, we will let $\widehat{u}$ denote q^u. For a positive number x, we let $\operatorname{Log} x = \max(1, \log x)$. When k has a base-p expansion $k = a_0 + a_1 p + \cdots + a_n p^n$ with $0 \leqslant a_i \leqslant p-1$ $(0 \leqslant i \leqslant n)$, we define $\gamma(k) = \gamma_q(k)$ by

$$\gamma(k) = a_0 + a_1 + \cdots + a_n.$$

Define the constant $B = B_q(k)$ by

$$B_q(k) = \begin{cases} 1, & \text{when } k \leqslant 2^{\gamma-2}, \\ (1 - 2^{-\gamma(k)})^{-1}, & \text{when } k > 2^{\gamma-2}. \end{cases}$$

Let

$$s_{q,k} = Bk(\operatorname{Log} k + \operatorname{Log}\operatorname{Log} k + 2 + B \operatorname{Log}\operatorname{Log} k/ \operatorname{Log} k).$$

We are now in a position to state the main result of [5].

Theorem 1. *There exists a positive absolute constant C with the following property. Suppose that k and s are natural numbers with $k > 1$,*

$$s \geqslant s_{q,k} + Ck\sqrt{\operatorname{Log}\operatorname{Log} k}/ \operatorname{Log} k,$$

and $\operatorname{char}(\mathbb{F}_q) \nmid k$. *Let τ be some fixed integer, and let $\lambda_1, \dots, \lambda_s$ be fixed non-zero elements of $\mathbb{K}_\infty$, not all in $\mathbb{F}_q(t)$-rational ratio. Suppose also that the equation $\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0$ has a non-trivial solution $\mathbf{z}$ in $\mathbb{K}_\infty^s$. Then, for all sufficiently large positive real numbers P, the number of $\mathbb{F}_q[t]$-solutions $N(P; \boldsymbol{\lambda})$ of*

$$\langle \lambda_1 x_1^k + \cdots + \lambda_s x_s^k \rangle < \widehat{\tau},$$

with $\langle x_i \rangle < \widehat{P}$ $(1 \leqslant i \leqslant s)$, satisfies $N(P, \boldsymbol{\lambda}) \gg \widehat{P}^{s-k}$.

References

[1] V. Bentkus and F. Götze, *Lattice point problems and distribution of values of quadratic forms,* Ann. Math. **150** (1999), 977–1027.

[2] H. Davenport and H. Heilbronn, *On indefinite quadratic forms in five variables,* J. London Math. Soc. **21** (1946), 185–193.

[3] D. E. Freeman, *Asymptotic lower bounds and formulas for Diophantine inequalities,* Number Theory for the Millennium, Vol. 2 (Urbana, IL, 2000), A. K. Peters, Natick, MA, 2002, 57–74.

[4] D. E. Freeman, *Asymptotic lower bounds for Diophantine inequalities,* Mathematika **47** (2000), 127–159.

[5] C. V. Spencer, *Diophantine inequalities in function fields* (submitted).

[6] T. D. Wooley, *On Diophantine inequalities: Freeman's asymptotic formula,* Bonner Math. Schriften **360** (2003), Article 30, 32pp.

Higher order terms in Waring's problem

R. C. Vaughan
(joint work with T. D. Wooley)

As usual in Waring's problem, when $k > 1$, we let

$$R(n) = R(n; s, k)$$

denote the number of solutions to the equation

$$m_1^k + \cdots + m_s^k = n$$

in positive integers m_j. Then, as first discovered by Hardy and Littlewood [1922], provided that s is sufficiently large in terms of k there is an asymptotic formula for $R(n)$,

$$R(n) \sim \tfrac{\Gamma(1+1/k)^s}{\Gamma(s/k)} n^{s/k-1} \mathfrak{S}_s(n) \quad \text{as } n \to \infty$$

where $\mathfrak{S}_s(n)$ denotes the singular series, defined by

$$\mathfrak{S}_s(n) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} q^{-s} S(q,a)^s e(-an/q)$$

with

$$S(q,a) = \sum_{r=1}^{q} e(ar^k/q).$$

In particular various values of s_0 have been given for which this holds whenever $s \geqslant s_0$, namely

$$s_0 = 2^k \quad (k = 3, 4, 5),$$

$$s_0 = 7.2^{k-3} \quad (k = 6, 7, 8),$$

$$s_0 = k^2(\log k + \log\log k + O(1)) \quad (k \geqslant 9),$$

by Vaughan [1986a,b], Boklan [1994], Ford [1995], repsectively.

It is known that there is some limitation on the quality of the error term which can be obtained in the above asymptotic formula. See Loh [1996].

In this memoir we show that there are second order terms which have a similar appearance to the main term, and which explain rather precisely the phenomenon discovered by Loh. In principle the method described here could also be adapted to obtain third, and higher, order terms, but the conclusions are not so illuminating and and do not merit inclusion, especially in view of the extra complexity of the arguments.

Theorem 1. *Suppose that $s \geqslant s_1$ and $s \geqslant 2k+3$. Then*

$$R(n) = \tfrac{\Gamma(1+1/k)^s}{\Gamma(s/k)} n^{s/k-1}\mathfrak{S}_s(n) + \tfrac{\Gamma(1+1/k)^{s-1}}{\Gamma((s-1)/k)} n^{(s-1-k)/k}\mathfrak{S}_s(n;1) + O\left(n^{(s-1-k)/k-\delta}\right)$$

where

$$\mathfrak{S}_s(n;1) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} q^{-s} S(q,a)^{s-1} T(q,a) e(-an/q)$$

and

$$T(q,a) = \sum_{r=1}^{q} \left(\frac{r}{q} - \frac{1}{2}\right) e(ar^k/q).$$

When k is even, $T(q,a) = \frac{1}{2}$ and so $\mathfrak{S}_s(n;1)$ takes on a simpler form. For convenience we define

$$\mathfrak{T}_s(n;w) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} q^{w-s} S(q,a)^{s-1} e(-an/q).$$

When k is odd there is apparently no such simple relationship with an Euler product. Indeed it is not clear that the series is always non-zero, although this seems rather likely when s is sufficiently large. However it is quite possible that for large s it is close to the value of its first term, $\frac{1}{2}$, and so is always positive. We are able to show that it is bounded away from zero a substantial proportion of the time. We are also able to demonstrate a close connection with $\mathfrak{T}_s(n;w)$.

Theorem 2. *(i) Suppose that k is even and $s \geqslant 5$. Then $\mathfrak{S}_s(n:1)$ converges*

$$\mathfrak{S}_s(n;1) = \tfrac{1}{2}\mathfrak{T}_s(n;0)$$

and $\mathfrak{T}_s(n;0) \gg 1$ uniformly in n. (ii) Suppose that $s \geqslant 2k+3$. Then $\mathfrak{S}_s(n:1)$ converges and there is a positive constant c such that for all sufficiently large x the number $N(x)$ of $n \leqslant x$ with $|\mathfrak{S}_s(n;1)| \geqslant c$ satisfies $N(x) \geqslant cx$.

Theorem 3. *There is an $s_2 = s_2(k)$ such that whenever $s > s_2$ there is a $u_0(s) > 1$ such that the function $G(w)$ defined by*

$$G(w) = \sum_{m=1}^{\infty} \frac{1}{m^w} \mathfrak{T}_s(n-m^k;w)$$

is analytic for w in the strip $1 < \Re w < u_0(s)$. Moreover $G(w)$ has an analytic continuation to the half–plane $\Re w < u_0(s)$, and is analytic at every point of that half–plane except $w = 1$ where it has a simple pole with residue $\mathfrak{S}_s(n)$. Finally

$$G(0) = -\mathfrak{S}_s(n;1).$$

References

[1] K. D. Boklan [1994], *The asymptotic formula in Waring's problem*, Mathematika **41**, 147-161.

[2] K. B. Ford [1995], *New estimates for mean values of Weyl sums*, Internat. Math. Res. Notices, 155–171.

[3] G. H. Hardy and J. E. Littlewood [1922], *Some problems of "Partitio Numerorum": IV. The singular series in Waring's Problem and the value of the number $G(k)$*, Math. Z., **12**, 161–188.

[4] W. K. A. Loh [1996], *Limitation to the asymptotic formula in Waring's problem*, Acta Arithmetica, **74**, 1–15.

[5] E. C. Titchmarsh [1986], The Theory of the Riemann Zeta-Function, 2nd edition, revised by D. R. Heath-Brown, Oxford University Press, Oxford.

[6] R. C. Vaughan [1986a], *On Waring's problem for cubes*, J. Reine Angew. Math., **365**, 122–170.

[7] R. C. Vaughan [1986b], *On Waring's problem for smaller exponents. II*, Mathematika, **33**, 6–22.

[8] R. C. Vaughan [1997], The Hardy-Littlewood Method, 2nd edition, Cambridge University Press, Cambridge.

Uniform distribution of $(cx)^{3/2} \pmod 1$ for $c \in \mathbf{Q}$

Mark Watkins

We describe a decade-old result of Elkies involving the equidistribution of $x^{3/2}$ modulo 1, and in particular its relation to small nonzero values of $x^3 - y^2$ and Hall's conjecture. This is part of a more general idea of Elkies involving finding points near varieties using lattice reduction.

Elkies shows that the inequality $|x^3 - y^2| \leqslant X$ has no more than $\ll \sqrt{X} \log X$ solutions with $X/2 \leqslant x \leqslant X$. Following Hall, we first transform the problem by writing $x = 3a^2 + b$ with a, b integral, and $b \in (3a, 3a]$. Then we expand

$$\left(\frac{4x^3}{3}\right)^{1/2} = 6a^3 + 3ab + \frac{1}{4}\frac{b^2}{a} - \frac{1}{72}\frac{b^3}{a^3} + O\left(\frac{1}{\sqrt{X}}\right).$$

Writing

$$y = 6a^2 + 3ab + \frac{1}{4}\frac{b^2}{a} + c,$$

we have that $|4x^3 - 3y^2| \ll x$ if and only if

$$c = \frac{b^2}{4a} - \frac{1}{72}\left(\frac{b}{a}\right)^3 + O\left(\frac{1}{\sqrt{X}}\right). \tag{1}$$

Elkies now approximates b/a within $1/\sqrt{X}$ by one of $O(\sqrt{X})$ points β on the interval $(-3, 3]$, and for each β will attempt to bound the number of (a, b, c) that satisfy (1). We start by linearising $b^2/4a$ via

$$\frac{b^2}{4a} - \frac{a}{4}\big(\beta - b/a\big)^2 = -\frac{\beta^2}{4}a + \frac{\beta}{2}b,$$

where the second term on the left is $O\big(1/\sqrt{X}\big)$ by the β-approximation.

We are then left with the three conditions:

$$a \ll \sqrt{X}, \quad b - a\alpha \ll 1, \quad c + \frac{\beta^2}{4}a - \frac{\beta}{2}b + \frac{\beta^3}{72} \ll 1/\sqrt{X},$$

which form an off-center box of volume $O(1)$. If such lattices were uniformly distributed in the 5-dimensional moduli space, we would obtain an upper bound of $O(\sqrt{X})$ such (a, b, c) triples as we varied β. However, the lattices lie in the 2-dimensional symmetric square subspace that preserves $4ac - b^2$ (over the algebraic closure), as might be inferred already from the principal contribution in (1).

So instead of getting a 3-dimensional lattice problem, we can reduce to one in only 2 dimensions, which allows the use of continued fractions. This allows Elkies to prove theorems, whereas in most of his other contexts, only heuristic estimates could be made. Indeed, writing

$$M_\beta = \begin{pmatrix} 0 & 0 & 1/\sqrt{X} \\ 0 & 1 & -\beta \\ \sqrt{X} & -\frac{\beta}{2}\sqrt{X} & \frac{\beta^2}{4}\sqrt{X} \end{pmatrix}, \quad \vec{\delta}_\beta = \big(0, 0, -\beta^3/72\big),$$

we want $\vec{v} = (c, b, a)$ to satisfy $\|M_\beta \vec{v} - \vec{\delta}_\beta\| \ll 1$, and we have that $M_\beta = \mathrm{Sym}^2 N_\beta$ for

$$N_\beta = \begin{pmatrix} 0 & 1/X^{1/4} \\ X^{1/4} & -X^{1/4}\frac{\beta}{2} \end{pmatrix}.$$

We can use continued fractions to find T_β such that $N_\beta T_\beta$ is as small as possible, and then $M'_\beta = M_\beta \mathrm{Sym}^2 T_\beta$ will similarly be small. We can then find a box containing all $\vec{w}$ with $\|M'_\beta \vec{w} - \vec{\delta}_\beta\| \ll 1$, and the number of such $\vec{w}$ (summed over all β) gives an upper bound for the number of x, y that satisfy $|4x^3 - 3y^2| \leqslant X$.

A computation shows that we get a box of approximate size

$$\frac{X^{1/4}}{q} \times 1 \times \frac{q}{X^{1/4}}$$

when $\left|\frac{\beta}{2} - \frac{p}{q}\right| \leqslant \frac{1}{qX^{1/4}}$, and so a denominator of q leads to a contribution of no more than $O\big(X^{1/4}/q\big)$ integral triples. Furthermore, the equi-spacing of the β implies that each p/q appears no more than $X^{1/4}/q$ times, so by summing q up to $X^{1/4}$ and p coprime to q with $p/q \in (-3, 3]$, we get a total bound of

$$\ll \sum_{q \ll X^{1/4}} \frac{X^{1/4}}{q} \cdot \sum_{\substack{p=1 \\ (p,q)=1}}^{q} \frac{X^{1/4}}{q} \ll \sum_{q \ll X^{1/4}} \frac{X^{1/4}}{q} \cdot \frac{X^{1/4}}{q} \cdot \phi(q) \ll \sqrt{X} \log X.$$

A fuller exposition appears in §4.2 of [1], and a function field analogue in §3.3.2 of the preprint [2].

References

[1] N. D. Elkies, *Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction.* In *Algorithmic number theory,* Proceedings of the 4th International Symposium (ANTS-IV) held at the Universiteit Leiden, Leiden, July 2–7, 2000, edited by W. Bosma, Lecture Notes in Computer Science **1838**, Springer-Verlag, Berlin (2000), 33–63. Preprint available online at
http://arxiv.org/math.NT/0005139 and possibly the paper from `springerlink.com` via http://dx.doi.org/10.1007/10722028_2

[2] N. D. Elkies, M. Watkins, *Polynomial Families and the Davenport-Mason bound.* Preprint (2008), available from
http://magma.maths.usyd.edu.au/~watkins/papers/hall.ps

The circle method in function fields

Trevor D. Wooley
(joint work with Yu-Ru Liu)

We report on recent work joint with Yu-Ru Liu centred on the circle method in function fields, illustrating our ideas with a consideration of Waring's problem in polynomial rings with coefficients from a finite field. Let $\mathbb{F}_q[t]$ denote the ring of polynomials over the finite field $\mathbb{F}_q$ of characteristic p, and write $\mathbb{J}_q^k[t]$ for the additive closure of the set of kth powers of polynomials in $\mathbb{F}_q[t]$. Define $G_q(k)$ to be the least integer s satisfying the property that every polynomial in $\mathbb{J}_q^k[t]$ of sufficiently large degree admits a strict representation as a sum of s kth powers. We employ a version of the Hardy-Littlewood method involving the use of smooth polynomials in order to establish a bound of the shape $G_q(k) \leqslant Ck \log k + O(k \log\log k)$. Here, the coefficient C is equal to 1 when $k < p$, and C is given explicitly in terms of k and p when $k > p$, but in any case satisfies $C \leqslant 4/3$. There are associated conclusions for the solubility of diagonal equations over $\mathbb{F}_q[t]$.

In order to be more precise, we require some notation. First, to each exponent k and finite field $\mathbb{F}_q$ we associate an integer $\gamma = \gamma_q(k)$ defined in terms of $p = \mathrm{ch}(\mathbb{F}_q)$ as follows. We write k in base p, say $k = a_0 + a_1 p + \cdots + a_n p^n$, where $0 \leqslant a_i \leqslant p-1$ $(0 \leqslant i \leqslant n)$, and then put $\gamma_q(k) = a_0 + a_1 + \cdots + a_n$. It is apparent that for each q and k one has $\gamma_q(k) \leqslant k$, and also that when $k \geqslant 2$ and $\mathrm{ch}(\mathbb{F}_q) \nmid k$, then $\gamma_q(k) \geqslant 2$. In addition, we define $A = A_q(k)$ by putting

$$A_q(k) = \begin{cases} 1, & \text{when } \mathrm{ch}(\mathbb{F}_q) > k, \\ (1 - 2^{-\gamma_q(k)})^{-1}, & \text{when } \mathrm{ch}(\mathbb{F}_q) < k. \end{cases}$$

Finally, when x is a positive real number, we write $\mathrm{Log}\, x$ for $\max\{1, \log x\}$, and put

$$\widehat{G}_q(k) = Ak(\mathrm{Log}\, k + \mathrm{Log}\,\mathrm{Log}\, k + 2 + A\mathrm{Log}\,\mathrm{Log}\, k/\mathrm{Log}\, k).$$

Theorem 1. *There is a positive absolute constant C_1 with the property that whenever k and q are natural numbers with $ch(\mathbb{F}_q) \nmid k$, then*

$$G_q(k) \leqslant \widehat{G}_q(k) + C_1 k\sqrt{\operatorname{Log}\operatorname{Log} k}/\operatorname{Log} k.$$

Meanwhile, when $ch(\mathbb{F}_q)|k$, one has $G_q(k) = G_q(k/ch(\mathbb{F}_q))$.

Almost all work concerning $G_q(k)$ hitherto has been restricted to those situations wherein $\mathrm{ch}(\mathbb{F}_q) > k$. Under this condition, Kubota [3, 4] established that $G_q(k) \leqslant 2^k + 1$, and Car [1, 2] obtained the upper bound $G_q(k) \leqslant 2k(k-1)\log 2 + 2k + 3$.

We also discuss the density of solutions of diagonal equations in $\mathbb{F}_q[t]$. Given $s, k \in \mathbb{N}$, and fixed coefficients $a_i \in \mathbb{F}_q[t]$ $(1 \leqslant i \leqslant s)$, denote by $N_s(B; \mathbf{a})$ the number of solutions of the equation

$$a_1 x_1^k + \cdots + a_s x_s^k = 0, \tag{1}$$

with $\mathbf{x} \in \mathbb{F}_q[t]^s$ and $\operatorname{ord} x_i \leqslant B$ $(1 \leqslant i \leqslant s)$.

Theorem 2. *Let k and q be natural numbers with $ch(\mathbb{F}_q) \nmid k$. There is a positive absolute constant C_2 with the property that whenever s is a natural number with*

$$s \geqslant \widehat{G}_q(k) + C_2 k\sqrt{\operatorname{Log}\operatorname{Log} k}/\operatorname{Log} k,$$

then the equation (1) *satisfies the following quantitative local-to-global principle. Let $\mathbf{a} \in (\mathbb{F}_q[t] \setminus \{0\})^s$, and suppose that the equation* (1) *has non-trivial solutions in all completions $\mathbb{F}_q(t)_\varpi$ of $\mathbb{F}_q(t)$. Then one has $N_s(B; \mathbf{a}) \gg (q^B)^{s-k}$.*

The Lang-Tsen theory of C_i-fields shows that the equation (1) possesses a solution $\mathbf{x} \in \mathbb{F}_q[t]^s \setminus \{\mathbf{0}\}$ whenever $s > k^2$. The local solubility hypothesis of Theorem 2 is consequently satisfied automatically under the same condition. Rather than merely establishing the existence of non-trivial solutions of equation (1), we instead supply a Hasse principle with good control of the associated density of solutions.

Our methods are based on an $\mathbb{F}_q[t]-$analogue of the repeated efficient differencing process introduced in [5], and as such make use of the set of smooth polynomials

$$\mathcal{A}(P, R) = \{x \in \mathbb{F}_q[t] \,:\, \deg x \leqslant P \text{ and } \varpi \text{ irreducible}, \varpi | x \Rightarrow \deg \varpi \leqslant R\}.$$

We also discuss analogues of Vinogradov's mean value theorem, again obtaining conclusions essentially free of hypotheses concerning the characteristic of the ambient function field.

References

[1] M. Car, Arithmétique additive dans l'anneau des polynômes á une indéterminée sur un corps fini. Thèse soutenue á l'Université de Provence 1972.

[2] M. Car, Le problème de Waring pour l'anneau des polynômes sur un corps fini. Séminaire de Théorie des Nombres, 1972-1973 (Univ. Bordeaux I, Talence), Exp. No. 6, 13pp. Lab. Théorie des Nombres, Centre Nat. Recherche Sci., Talence 1973.

[3] R. M. Kubota, Waring's problem for $\mathbb{F}_q[x]$. Ph. D. Thesis, University of Michigan, Ann Arbor 1971.
[4] R. M. Kubota, Waring's problem for $\mathbb{F}_q[x]$. Dissertationes Math. (Rozprawy Mat.) 117 (1974), 60pp.
[5] T. D. Wooley, Large improvements in Waring's problem. Ann. of Math. (2) 135 (1992) 131–164.

Some observations on the zeros of the Riemann zeta-function

Cem Yalçın Yildirim
(joint work with Moubariz Z. Garaev)

1. Relations between zeros of $\zeta(s)$ and of $\zeta'(s)$

We studied the relationships between the zeros of $\zeta(s)$ whose imaginary parts in the upper half-plane will be denoted by γ_n (ordered according to the increasing size of the ordinates), and the zeros $\beta' + i\gamma'$ of $\zeta'(s)$.

Soundararajan [4] conjectured that under the Riemann Hypothesis (RH) the statements (i) $\liminf_{\gamma'\to\infty}(\beta' - \frac{1}{2})(\log\gamma') = 0$ and (ii) $\liminf_{\gamma\to\infty}(\gamma^+ - \gamma)\log\gamma = 0$ are equivalent. (Here γ^+ is the least ordinate of a zero of $\zeta(s)$ with $\gamma^+ > \gamma$). Zhang [5] proved that (ii) implies (i).

We obtained the following results pertaining to this conjecture: For any $\beta'+i\gamma'$, let of all ordinates of zeros of $\zeta(s)$, γ_c be the one for which $|\gamma_c - \gamma'|$ is smallest. For large γ', there exists γ_n such that $\gamma' - 1 \leqslant \gamma_n \leqslant \gamma_{n+2} \leqslant \gamma' + 1$ and

$$\min\{|\gamma_c - \gamma'|\log\gamma',\ |\gamma_{n+2} - \gamma_n|\log\gamma_n\} \ll (|\beta' - \frac{1}{2}|\log\gamma')^{\frac{1}{2}}.$$

For any $\beta' + i\gamma'$ we have

$$|\gamma_c - \gamma'| \ll |\beta' - \frac{1}{2}|^{\frac{1}{2}}.$$

Assuming RH and $\liminf_{\gamma'\to\infty}(\beta' - \frac{1}{2})\log\gamma' = 0$, we have $\liminf_{\gamma'\to\infty}|\gamma_c - \gamma'|\log\gamma' = 0$. Assuming RH and

$$\liminf_{\gamma'\to\infty}(\beta' - \frac{1}{2})(\log\gamma')(\log\log\gamma')^2 = 0,$$

we have $\liminf_{n\to\infty}(\gamma_{n+1} - \gamma_n)(\log\gamma_n) = 0$.

These results and their proofs recently appeared in [1], but they have not been announced in an international meeting prior to the March 2008 Oberwolfach workshop on Analytic Number Theory.

2. A modified approach to the pair correlation of zeta zeros

In deriving his original estimates for the pair correlation function for the zeros of the Riemann zeta-function, Montgomery [3] went through the following steps.

First, assuming RH, he obtained the explicit formula

$$(2\sigma-1)\sum_{\gamma}\frac{x^{i\gamma}}{(\sigma-\frac{1}{2})^2+(t-\gamma)^2} = \\ -x^{-\frac{1}{2}}\big(\sum_{n\leqslant x}\Lambda(n)(\frac{x}{n})^{1-\sigma+it}\sum_{n>x}\Lambda(n)(\frac{x}{n})^{\sigma+it}\big) \\ -\frac{\zeta'}{\zeta}(1-\sigma+it)x^{\frac{1}{2}-\sigma+it}+\frac{x^{\frac{1}{2}}(2\sigma-1)}{(\sigma-1+it)(\sigma-it)} \\ -x^{-\frac{1}{2}}\sum_{n=1}^{\infty}\frac{(2\sigma-1)x^{-2n}}{(\sigma-1-it-2n)(\sigma+it+2n)},$$

valid for $\sigma>1$, and all $x\geqslant 1$. In this formula $\frac{\zeta'}{\zeta}(1-\sigma+it)$ is replaced by $-\frac{\zeta'}{\zeta}(\sigma-it)-\log(|t|+2)+O(1)$ (for s in a fixed strip to the right of $\sigma>1$), and the last two terms are easily replaced by upper-bound estimates. Montgomery took $\sigma=\frac{3}{2}$, squared the modulus of both sides, and then integrated both sides over t from 0 to T. To carry out the integration of the square of the series involving $\Lambda(n)$, Montgomery had recourse to the Parseval identity for Dirichlet series, which he had proved together with Vaughan. The end result of this calculation was

$$(\frac{T\log T}{2\pi})^{-1}\sum_{0<\gamma,\tilde{\gamma}\leqslant T}T^{i\alpha(\gamma-\tilde{\gamma})}\frac{4}{4+(\gamma-\tilde{\gamma})^2}=(1+o(1))T^{-2\alpha}\log T+\alpha+o(1),$$

as $T\to\infty$, uniformly for $0\leqslant\alpha\leqslant 1-\varepsilon$. (Here γ and $\tilde{\gamma}$ run through the ordinates of the nontrivial zeros of $\zeta(s)$). Montgomery then went on to deduce results on the gaps between zeta zeros and the proportion of simple zeros, and also formulated his pair correlation conjecture along with connections to random matrix theory.

In our approach we take Montgomery's explicit formula with $\sigma=\frac{5}{2}$, and sum both sides over $t=\tilde{\gamma}\in[0,T]$. Evaluating the sums involving $\Lambda(n)$ using the Landau-Gonek formula [2]

$$\sum_{0<\gamma\leqslant T}x^{\rho} = -\frac{T}{2\pi}\Lambda(x)+O(x\log 2xT\log\log 3x) \\ +O(\log x\min(T,\frac{x}{\langle x\rangle}))+O(\log 2T\min(T,\frac{1}{\log x}))$$

which holds uniformly for x, $T>1$, we obtain the same estimate as Montgomery for $x=o(T/\log\log T)$. One possible advantage in this approach is that it allows us to let t run through any sequence of numbers, so that we may hope to obtain the correlation of zeta zeros with the sequence elements. For example, we can take t to run through fractional powers of integers. Taking $t=m^{\frac{3}{2}}$, and using the

simplest van der Corput estimates for exponential sums, we found that

$$\sum_{0<\gamma\leqslant T}\sum_{m\leqslant T^{\frac{2}{3}}}\frac{4x^{i(\gamma-m^{\frac{3}{2}})}}{4+(\gamma-m^{\frac{3}{2}})^2} = x^{-2}T^{\frac{2}{3}}(\log T+O(1))+O((x\log x)^{\frac{1}{2}}\log T) +O(\log^3 T),$$

which gives an asymptotic when $x \ll T^{\frac{1}{15}}/(\log T)^4$. This research is still in a very preliminary stage, and we are currently working on results involving t running through various sequences. We hope to complete these calculations soon, and provide explanations or interpretations for the results.

References

[1] M. Z. Garaev and C. Y. Yıldırım, On small distances between ordinates of zeros of $\zeta(s)$ and $\zeta'(s)$, *Int. Math. Res. Not. IMRN* **2007**, no. 21, Art. ID rnm091, (2007), 14 pp.

[2] S. M. Gonek, An explicit formula of Landau and its applications to the theory of the zeta-function, in *A tribute to Emil Grosswald: Number Theory and related analysis* (edited by M. Knopp and M. Sheingorn), *Contemporary Math.* **143**, 395–413, Amer. Math. Soc., Providence, R.I., 1993.

[3] H. L. Montgomery, The pair correlation of zeros of the Riemann zeta-function, in *Analytic Number Theory (St. Louis, Mo., 1972), Proc. Sympos. Pure Math.* **24**, 181–193, Amer. Math. Soc., Providence, R.I., 1973.

[4] K. Soundararajan, The horizontal distribution of zeros of $\zeta(s)$, *Duke Math. J.* **91**, No. 1, (1998), 33–59.

[5] Y. Zhang, On the zeros of $\zeta'(s)$ near the critical line, *Duke Math. J.* **110**, No. 3, (2001), 555–572.

Reporter: Jörg Brüdern

Participants

Prof. Dr. Michel Balazard
Institut de Mathematiques
de Luminy
Case 907
163 Avenue de Luminy
F-13288 Marseille Cedex 9

Prof. Dr. Antal Balog
Alfred Renyi Institute of
Mathematics
Hungarian Academy of Sciences
P.O.Box 127
H-1364 Budapest

Prof. Dr. William D. Banks
Dept. of Mathematics
University of Missouri-Columbia
202 Mathematical Science Bldg.
Columbia , MO 65211
USA

Dr. Valentin Blomer
Department of Mathematics
University of Toronto
40 St.George Street
Toronto , Ont. M5S 2E4
CANADA

Dr. Tim D. Browning
Department of Mathematics
University of Bristol
University Walk
GB-Bristol BS8 1TW

Prof. Dr. Jörg Brüdern
Institut für Algebra und
Zahlentheorie
Universität Stuttgart
Pfaffenwaldring 57
70569 Stuttgart

Dr. Regis de la Breteche
U.F.R. de Mathematiques
Case 7012
Universite de Paris VII
2, Place Jussieu
F-75251 Paris Cedex 05

Dr. Anne de Roton
Departement de Mathematiques
Universite de Nancy I
Boite Postale 239
F-54506 Vandoeuvre les Nancy Cedex

Prof. Dr. Jean-Marc Deshouillers
Institut Mathematique de Bordeaux
Universite de Bordeaux I
F-33405 Talence Cedex

Dr. Rainer Dietmann
Institut für Algebra und
Zahlentheorie
Universität Stuttgart
Pfaffenwaldring 57
70569 Stuttgart

Dr. Christian Elsholtz
Department of Mathematics
Royal Holloway
University of London
GB-Egham Surrey TW20 OEX

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
USA

Prof. Dr. Etienne Fouvry
Laboratoire de Mathematiques
Universite Paris Sud (Paris XI)
Batiment 425
F-91405 Orsay Cedex

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

Prof. Dr. Friedrich Götze
Fakultät für Mathematik
Universität Bielefeld
Universitätsstr. 25
33615 Bielefeld

Prof. Dr. Daniel A. Goldston
Department of Mathematics
San Jose State University
San Jose CA 95192-0103
USA

Prof. Dr. Sidney W. Graham
Dept. of Mathematics
Central Michigan University
Mt Pleasant , MI 48859
USA

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

Dr. Harald Helfgott
Department of Mathematics
University of Bristol
University Walk
GB-Bristol BS8 1TW

Dr. Christopher Hughes
Dept. of Mathematics
University of York
GB-Heslington, York Y010 5DD

Prof. Dr. Martin N. Huxley
School of Mathematics
Cardiff University
23, Senghennydd Road
GB-Cardiff CF24 4AG

Prof. Dr. Aleksandar Ivic
Katedra Matematike RGF-a
Universiteta u Beogradu
Djusina 7
11000 Beograd
SERBIA

Prof. Dr. Matti Jutila
Department of Mathematics
University of Turku
FIN-20014 Turku

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

Prof. Dr. Jianya Liu
Department of Mathematics
Shandong University
27 Shanda Nanlu
Jinan
Shandong 250100
CHINA

Prof. Dr. Helmut Maier
Abteilung Zahlentheorie und Wahrscheinlichkeitstheorie
Universität Ulm
Helmholtzstrasse 18
89069 Ulm

Prof. Dr. Hugh L. Montgomery
Dept. of Mathematics
The University of Michigan
4066 East Hall
Ann Arbor MI 48109-1109
USA

Prof. Dr. Yoichi Motohashi
Dept. of Mathematics
Nihon University
Surugadai
Tokyo 101-8308
JAPAN

Prof. Dr. Scott T. Parsell
Butler University
4600 Sunset Ave.
Indianapolis , IN 46208
USA

Prof. Alberto Perelli
Dipartimento di Matematica
Universita di Genova
Via Dodecaneso 35
I-16146 Genova

Prof. Dr. Janos Pintz
Alfred Renyi Mathematical Institute
of the Hungarian Academy of Science
Realtanoda u. 13-15
H-1053 Budapest

Prof. Dr. Olivier Ramare
Mathematiques
UMR 8524 CNRS
Universite de Lille 1
F-59655 Villeneuve d'Ascq.

Prof. Dr. Joel Rivat
IML
CNRS
Case 907 - Luminy
F-13288 Marseille Cedex 9

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

Dr. Jan-Christoph Schlage-Puchta
Mathematisches Institut
Universität Freiburg
Eckerstr. 1
79104 Freiburg

Prof. Dr. Igor E. Shparlinski
Department of Computing
Macquarie University
Sydney NSW 2109
Australia

Craig Spencer
Department of Mathematics
University of Michigan
2074 East Hall
530 Church Street
Ann Arbor , MI 48109-1043
USA

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

Mark J. Watkins
MAGMA Computer Algebra Group
School of Mathematics & Statistics
F07
University of Sydney
Sydney NSW 2006
Australia

Trevor D. Wooley
Department of Mathematics
University of Bristol
University Walk
GB-Bristol BS8 1TW

Prof. Dr. Cem Yalcin Yildirim
Department of Mathematics
Bogazici University
Bebek
Istanbul 34342
Turkey