Mathematisches Forschungsinstitut Oberwolfach

Report No. 50/2022

DOI: 10.4171/OWR/2022/50

Analytic Number Theory (hybrid meeting)

Organized by
Kaisa Matomäki, Turku
Kannan Soundararajan, Stanford
Robert C. Vaughan, State College
Trevor D. Wooley, West Lafayette

6 November – 12 November 2022

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

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

Introduction by the Organizers

The workshop *Analytic Number Theory*, organised by Kaisa Matomäki (Turku), Kannan Soundararajan (Stanford), Robert Vaughan (State College) and Trevor Wooley (West Lafayette) was well attended with 53 participants from a broad geographic spectrum, all either distinguished and leading workers in the field or very promising younger researchers, and notable on this occasion for the diversity of this participant group.

The workshop was most opportune as there has been quite a number of recent significant developments in cognate areas by Bhargava, Alpöge and Shnidman, by Brüdern and Wooley, by Green, and in several directions by Maynard and his collaborators. There were also very substantial contributions by Bloom, Lichtman, Peluse, Pratt and Smith who are all extremely young and doing work of the very highest quality.

Bhargava presented joint work with Alpöge and Shnidman on the density of integers which are the sum of two rational cubes. There is a long standing belief that such numbers have positive density in the integers. They show that a positive proportion of integers do have such a representation and a positive proportion do not. Their methods are connected with investigations into the average size of the 2-Selmer group of elliptic curve and they have numerous applications.

Brüdern described for us joint work with Wooley which is the first movement on the upper bound for $G(k)$ in Waring's problem for over a quarter of a century, and Green presented startling progress on a quantitative version of Sárközy's theorem for shifted primes.

In a sensational piece of work, Lichtman presented a proof of a famous open conjecture of Erdős on primitive sets. A set of integers $n > 1$ is *primitive* when no member divides any other. Erdős's conjecture gives a quantitative expression to the belief that the primes are the extremal primitive set.

Smith's talk resolved an old problem on traces of totally real algebraic integers that goes back to the work of Schur and Siegel. Surprisingly he shows that a long standing conjecture on these traces is in fact false.

One of the major sources of advances in our area is Maynard, who this summer was awarded a Fields medal. The myriad impacts of his ideas is illustrated not only by his own talk but by major presentations by three of his collaborators.

Merikoski showcased joint work with Maynard on a well known open question of Gordon from 1962 which asks if it is possible to walk to infinity in the complex plane with bounded steps by using Gaussian primes as stepping stones. The answer is likely to be no, but then the question arises as to how small can we make each successive step in terms of the average size of the current stone $|\mathfrak{p}|$. Surprisingly they are able to break the square root barrier, namely that the step size can be $\ll |\mathfrak{p}|^{\frac{1}{2}-\delta}$ for some small fixed δ.

Dietmann presented joint work with Elsholtz, Kalmynin, Konyagin and Maynard on long gaps between values of a given binary quadratic form. Previous work in the area dated from more than forty years ago. Significant progress was made on this. Moreover a result was obtained for forms of arbitrary discriminant D which has only a mild dependence on D.

Dartyge described her impressive work with Maynard on the largest prime factor of quartic polynomials with cyclic and dihedral Galois groups.

In addition Maynard gave a talk on joint work with Heath-Brown and Pratt which suggests that it might be possible to make highly significant progress on the distribution of primes without a major breakthrough in our knowledge of the distribution of zeros of the Riemann zeta function. The idea would be to deal with various special distributions of zeros which collectively might cover the worst cases. He then showed how it is possible to proceed with one of these distributions.

Several other presentations were made on topics connected with the Riemann zeta-function and it generalizations. Florea described joint work with Hung Bui on new bounds for negative moments of the Riemann zeta function, and Devin

spoke on work with Fiorilli and Södergren on extending the unconditional support for the one-level density of zeros in an Iwaniec-Luo-Sarnak family.

There was an intriguing presentation by Harper on the typical size of character sums which, based on probabilistic arguments, made some thought provoking suggestions which could mould future work in the area. Kowalski and Mangerel also presented interesting results on character and exponential sums. In a different direction Peluse presented joint work with Soundararajan on the divisibility of elements in the character table for the symmetric group, which resolved a recent conjecture of Miller. In yet another direction Pratt made interesting progress on an irrationality question of Erdős and Kac.

In addition significant progress was reported by Blomer, Bloom, Browning and Hochfilzer on questions related to special cases of the local to global principal or applications of the circle method. There were also reports on a spectrum of other questions across the field by Chow (joint with Chapman), Gun (joint with Bilu and Naik), Matomäki (joint with Teräväinen), Rodgers (joint with Gorodetsky and Mangerel), Salberger, and Swaenepoel.

On Tuesday evening participants were invited to give 10 minute presentations in an informal session made particularly energetic by the contributions of the promising younger researchers. This led to some interesting and lively reactions. On Thursday evening Montgomery led a problem session where a large number of interesting unsolved questions were presented and stimulated further lively discussions.

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

Workshop (hybrid meeting): Analytic Number Theory

Table of Contents

Abstracts

Integers expressible as the sum of two rational cubes

Manjul Bhargava
(joint work with Levent Alpöge, Ari Shnidman)

It has long been known which numbers can be expressed as the sum of two rational squares. As was first observed by Girard in 1625 and Fermat in 1638, and finally proven by Euler in 1749 [5, pp. 227–231], they are those positive integers whose prime factorizations have all primes $p \equiv 3 \pmod 4$ occurring with even exponent. Using this precise description, we see that a density of 0% of integers are the sum of two rational squares. Moreover, an integer is the sum of two rational squares if and only if it is the sum of two integer squares.

In contrast, the integers that are the sum of two rational cubes do not seem to follow any simple pattern:

$$1, 2, 6, 7, 8, 9, 12, 13, 15, 16, 17, 19, 20, 22, 26, 27, 28, 30, 31, 33, 34, 35, \ldots$$

It is conjectured that these integers have positive density; indeed, based on predictions of Goldfeld [6], Katz and Sarnak [10], and Bektemirov, Mazur, Stein and Watkins [3], it is natural to conjecture that the integers that can be expressed as the sum of two rational cubes should have natural density exactly 1/2. However, it has not previously been known whether this density is even greater than 0 or even less than 1.

We prove that a positive proportion of integers are expressible as the sum of two rational cubes, and a positive proportion are not so expressible. More generally, we prove that a positive proportion (in fact, at least one sixth) of elliptic curves in any cubic twist family have rank 0, and a positive proportion (in fact, at least one sixth) of elliptic curves with good reduction at 2 in any cubic twist family have rank 1.

Our method involves proving that the average size of the 2-Selmer group of elliptic curves in any cubic twist family, having any given root number, is 3. We accomplish this by generalizing a parametrization, due to the second author and Ho, of elliptic curves with extra structure by pairs of binary cubic forms. We then count integer points satisfying suitable congruence conditions on a quadric hypersurface in the space of real pairs of binary cubic forms in a fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$, using a combination of geometry-of-numbers methods and the circle method, building on earlier work of Ruth and the first author. We give a new interpretation of the singular integral and singular series arising in the circle method in terms of real and p-adic integrals with respect to a natural $(\mathrm{SL}_2 \times \mathrm{SL}_2)$-invariant measure. A uniformity estimate and sieve then shows that the average size of the 2-Selmer group over the full cubic twist family is 3.

After suitably partitioning the subset of curves in the family with given root number, we execute a further sieve to show that the root number is equidistributed

and that the same average, now taken over only those curves of given root number, is also 3. Finally, we apply the p-parity theorem of Dokchitser–Dokchitser [4] and a p-converse theorem of Burungale–Skinner to conclude.

We prove the following theorems

Theorem 1. *When ordered by their absolute values, a positive proportion of integers are the sum of two rational cubes, and a positive proportion are not.*

More precisely, we prove that

$$\liminf_{X\to\infty} \frac{\#\{n\in\mathbb{Z} : |n|<X \text{ and } n \text{ is the sum of two rational cubes}\}}{\#\{n\in\mathbb{Z}\colon |n|<X\}} \geq \frac{2}{21} \tag{1}$$

and

$$\liminf_{X\to\infty} \frac{\#\{n\in\mathbb{Z} : |n|<X \text{ and } n \text{ is not the sum of two rational cubes}\}}{\#\{n\in\mathbb{Z}\colon |n|<X\}} \geq \frac{1}{6}. \tag{2}$$

In fact we will prove the stronger claim that among the cubic twists $x^3+y^3=nz^3$ of the Fermat cubic, at least $1/6$ of twists have rank 0 and at least $2/21$ have rank 1. More generally, we consider general families of cubic twists of elliptic curves.

Theorem 2. *Fix $d\neq 0$. Then, when n varies ordered by $|n|$, at least $1/6$ of the elliptic curves in the cubic twist family $E_{d,n} : y^2 = x^3 + dn^2$ have rank 0, and at least $1/6$ of the elliptic curves $E_{d,n}$ with good reduction at 2 have rank 1. In particular, if the squarefree part of d is congruent to 1 (mod 4), then a proportion of at least $\frac{1}{21}2^{r-1}$ of the curves $E_{d,n}$ have rank 1, where r is the least residue of $v_2(d)/2$ modulo 3.*

We prove Theorem 2 via a determination of the average size of the 2-Selmer group of elliptic curves satisfying any finite—or any acceptable infinite—set of congruence conditions in a cubic twist family.

This bound on the average rank can be improved via an analysis of root numbers. Indeed, for any fixed $d\neq 0$, we prove that the set of n such that the elliptic curve $E_{d,n}$ has a given root number is a countable union of acceptable sets. Moreover, a density of $1/2$ of elliptic curves $E_{d,n}$ have root number $+1$ and $1/2$ have root number -1.

Theorem 3. *Fix $d\neq 0$. The density of elliptic curves in the cubic twist family $E_{d,n}$ that have root number $+1$ (resp. -1) is $1/2$. The average size of the 2-Selmer group of just those elliptic curves $E_{d,n}$ having root number $+1$ (resp. -1) is 3.*

Theorems 1 and 2 are deduced from Theorem 3, using the p-parity theorem of Dokchitser–Dokchitser [4][1] and the p-converse theorem of Burungale–Skinner established in an Appendix.

Theorem 3 also implies the following bounds on (the limsup and the liminf of) the average rank of elliptic curves in cubic twist families:

[1]Many important cases of the p-parity theorem were proved by Kim [11] and by Nekovář [14]; in fact, we only use the case $p=2$ which was proved by Monsky [13].

Theorem 4. *Fix $d \neq 0$, and let $\Sigma \subset \mathbb{Z}$ be any acceptable subset. The average rank in the cubic twist family of elliptic curves $E_{d,n}$ $(n \in \Sigma)$ is at most $4/3$. Furthermore, if the squarefree part of d is congruent to $1 \pmod{*}4$, then the average rank in the cubic twist family of elliptic curves $E_{d,n}$ $(n \in \mathbb{Z})$ is at least $\frac{1}{21}2^{r-1}$, where r is the least residue of $v_2(d)/2$ modulo 3.*

Theorem 4 shows, for the first time, the boundedness (and, in many cases, the positivity) of the average rank in cubic twist families. The question of the boundedness of the average rank in twist families of elliptic curves has been studied extensively. The unique sextic twist family was handled by Elkies and the second and third authors [1]. The quadratic case has been studied by many authors (see, e.g., [7, 15, 17, 2, 16, 8, 12]), and most recently by Smith [18], whose work covers most quadratic twist families. Meanwhile, significant progress on the unique quartic twist family was made by Kane and Thorne [9].

One may also ask which positive integers can be expressed as the sum of two *positive* rational cubes.

Theorem 5. *A positive proportion of positive integers are expressible as the sum of two positive rational cubes, and a positive proportion are not.*

Indeed, the same lower bounds on the proportions as in (1) and (2) hold for Theorem 5

Our methods also imply the following result about integers that are the product of three rational numbers in arithmetic progression:

Theorem 6. *A positive proportion of integers are expressible as the product of three rational numbers in arithmetic progression, and a positive proportion are not.*

Again, by the same arguments, the same lower bounds on the proportions in Theorem 6 hold as in (1) and (2); and the same lower bounds on the proportions hold for the set of positive integers that are the product of three *positive* rational numbers in arithmetic progression.

More generally, our results imply that a positive proportion of integers cannot be represented by any given reducible binary cubic form over $\amalg$.

Theorem 7. *Let $f(x, y)$ be any binary cubic form over $\amalg$ with a linear factor. Then, when ordered by absolute value, a positive proportion of integers cannot be expressed as $f(x, y)$ with $x, y \in \mathbb{Q}$. Furthermore, if the squarefree part of* $\mathrm{Disc}(f)$ *is* $1 \pmod 4$, *then a positive proportion of integers can be expressed as $f(x, y)$ with $x, y \in \mathbb{Q}$.*

Theorems 1 and 6 are the special cases of Theorem 7 where we set $f(x, y) = x^3+y^3$ and $f(x, y) = x(x + y)(x + 2y)$, respectively. Theorem 7 follows from Theorem 2, since the elliptic curve $f(x, y) = n$ is isomorphic to the curve $E_{d,n}$ where $d = 16\,\mathrm{Disc}(f)$.

When $f(x, y)$ is irreducible, the curve $f(x, y) = nz^3$ is not necessarily an elliptic curve, as it then often fails to even have local points. Indeed, in the irreducible

case, the density of integers n, such that $f(x,y) = n$ has points everywhere locally, is 0. More precisely:

Theorem 8. *Let $f(x,y)$ be an irreducible binary cubic form over $\mathbb{Q}$. The number of integers n with $|n| < X$ such that the curve $f(x,y) = n$ has points everywhere locally is on the order of either $X/\log^{1/3} X$ or $X/\log^{2/3} X$, depending on whether $\mathrm{Disc}(f)$ is or is not a square.*

References

[1] M. Bhargava, N. Elkies, and A. Shnidman, *The average size of the 3-isogeny Selmer groups of elliptic curves $y^2 = x^3 + k$*, J. Lond. Math. Soc. (2), 101(2020), 299–327.

[2] M. Bhargava, Z. Klagsbrun, R. J. Lemke Oliver, and A. Shnidman, *3-isogeny Selmer groups and ranks of abelian varieties in quadratic twist families over a number field*, Duke Math. J. 168(2019), 2951–2989.

[3] B. Bektemirov, B. Mazur, W. Stein, and M. Watkins, *Average ranks of elliptic curves: tension between data and conjecture*, Bull. Amer. Math. Soc. (N.S.), 44(2007), 233–254.

[4] T. Dokchitser and V. Dokchitser, *Regulator constants and the parity conjecture*, Invent. Math., 178(2009), 23–71.

[5] L. E. Dickson, *History of the theory of numbers. Vol. II: Diophantine analysis*, Chelsea Publishing Co., New York, 1966.

[6] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, In *Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979)*, volume 751 of *Lecture Notes in Math.*, pages 108-118. Springer, Berlin, 1979.

[7] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem. II*, Invent. Math., 118(1994), 331–370, with an appendix by P. Monsky.

[8] D. Kane, *On the ranks of the 2-Selmer groups of twists of a given elliptic curve*, Algebra Number Theory, 7(2013), 1253–1279.

[9] D. M. Kane and J. A. Thorne, *On the ϕ-Selmer groups of the elliptic curves $y^2 = x^3 - Dx$*, Math. Proc. Cambridge Philos. Soc., 163(2017), 71–93.

[10] N. M. Katz and P. Sarnak, *Zeroes of zeta functions and symmetry*, *Bull. Amer. Math. Soc. (N.S.)*, 36(1999), 1–26.

[11] B. D. Kim, *The parity conjecture for elliptic curves at supersingular reduction primes*, Compos. Math., 143(2007), 47-72.

[12] Z. Klagsbrun, B. Mazur, and K. Rubin, *A Markov model for Selmer ranks in families of twists*, Compos. Math., 150(2014), 1077–1106.

[13] P. Monsky, *Generalizing the Birch-Stephens theorem. I. Modular curves*, Math. Z., 221(1996), 415–420.

[14] J. Nekovář, *On the parity of ranks of Selmer groups. IV*, Compos. Math., 145(2009), 1351–1359, with an appendix by Jean-Pierre Wintenberger.

[15] K. Rubin and A. Silverberg, *Ranks of elliptic curves in families of quadratic twists*, Experiment. Math., 9(2000), 583–590.

[16] H. P. F. Swinnerton-Dyer, *The effect of twisting on the 2-Selmer group*, Math. Proc. Cambridge Philos. Soc., 145(2008), 513–526.

[17] A. Silverberg, *The distribution of ranks in families of quadratic twists of elliptic curves*, In *Ranks of elliptic curves and random matrix theory*, London Math. Soc. Lecture Note Ser., vol. 341, pages 171–176, Cambridge Univ. Press, Cambridge, 2007.

[18] A. Smith, *ℓ^∞-Selmer Groups in Degree ℓ Twist Families*, PhD thesis, Harvard University, Graduate School of Arts & Sciences, 2020.
`https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37365902`

Additive problems with almost prime squares

Valentin Blomer
(joint work with Lasse Grimmelt, Junxian Li, Simon Rydin Myerson)

In an influential paper [4], Hardy and Littlewood stated that a formal application of the circle method predicts that the number of representations of a large integer n in the form

$$n = p + x_1^2 + x_2^2 \tag{1}$$

with p prime, $x_1, x_2 \in \mathbb{Z}$ is $\pi \mathfrak{S}(n)\mathrm{Li}(n)$ for the singular series

$$\mathfrak{S}(n) = \prod_p \Big(1 + \frac{\chi_{-4}(p)}{p(p-1)}\Big) \prod_{p|n} \frac{(p-1)(p-\chi_{-4}(p))}{p^2 - p + \chi_{-4}(p)}$$

associated with this problem. Hooley [5] gave the first proof conditional on GRH, while Linnik [7] a few years later provided the first unconditional proof. A simpler and more modern treatment based on the Bombieri-Vinogradov theorem can be found in [6, Chapter V]. The best error term, saving an arbitrary power of $\log n$, has been obtained recently in [1], using the full force of the spectral theory of automorphic forms as well as estimates for multi-dimensional exponential sums.

Here we reconsider the problem with multiplicative restrictions on x_1, x_2 and require that they are almost primes, cf. [2].

Theorem 1. *There exists a constant $C > 0$ such that every sufficiently large integer $n \equiv 1, 3 \bmod 6$ can be represented in the form (1), where p is a prime and x_1, x_2 are integers all of whose prime factors are greater than $n^{1/C}$. The number of such representations is $\gg \mathfrak{S}(n) n (\log n)^{-3}$.*

The congruence condition on n is necessary to guarantee solutions to (1) with $(x_1 x_2, 6) = 1$ and p a prime greater than 3. At the cost of slightly more work it is possible to remove the condition modulo 6 if x_1, x_2 are permitted to have the small primes 2 and 3 as factors. A similar analysis leads to

Theorem 2. *There exists a constant $C > 0$ such that the number of solutions to the equation*

$$p = x_1^2 + x_2^2 + 1 \tag{2}$$

in primes $p \le x$ and x_1, x_2 all of whose prime factors are greater than $p^{1/C}$ is $\gg x(\log x)^{-3}$. In particular, there are infinitely many primes shifted by one that can be written as two squares of almost primes.

This should be compared with a beautiful recent result of Friedlander-Iwaniec [3] who considered (2) for a prime x_1 and an almost prime x_2, but without the additive shift.

It will come as no surprise that the first step in the proof of Theorem 1 consists in implementing a lower bound sieve in order to detect almost primes. There are two obvious difficulties to overcome:

a) the sieve requires an analysis of representations of integers by the form

$$d_1^2x_1^2 + d_2^2x_2^2 \tag{3}$$

which will typically not have class number one (and not even genus number one);

b) even if a good understanding of the previous problem was available, the sieve weights are supported on $d_1, d_2 \ll n^\kappa$ for some small $\kappa > 0$, but the best error term in the asymptotic formula for (1) is only on a logarithmic scale.

To understand the numbers $m \in \mathbb{N}$ represented by the quadratic form (3), we use the arithmetic of the non-maximal order $\mathbb{Z} + d_1d_2\mathbb{Z}[i]$ and in particular linear combinations of class group characters to identify the relevant numbers m. If the class group character is non-real, i.e. has order > 2, this amounts to summing Hecke eigenvalues over shifted primes:

$$\sum_{p<n} \lambda(n-p),$$

which is reminiscent of work of Pitt [8]. If the class group character is real, then it factors through the norm, and one obtains a familar convolution formula that can be used to extract the desired main term. Here it is important to carry the sieve weights directly through the Bombieri-Vinogradov type estimate in order to deal with problem b) mentioned above.

In some sense dual to prime numbers are smooth numbers, and we also discuss the equation

$$n = m + x_1^2 + x_2^2 \tag{4}$$

where m satisfies $P^+(m) \le g(n)$ for some function $g(n)$ and x_1, x_2 are almost primes. In this respect we prove [2]:

Theorem 3. *There exist constants $C, D > 0$ such that for any function g with $(\log n)^D \le g(n) \le n$, every sufficiently large integer n can be represented in the form (4) with $P^+(m) \le g(n)$ and integers x_1, x_2 all of whose prime factors are greater than $n^{1/C}$. The number of such representations is*

$$\gg \mathcal{F}(n, g(n))\Psi(n, g(n))(\log n)^{-2}.$$

Here $\Psi(n,y) = \#\{m \le n \mid P^+(m) \le y\}$ and

$$\mathcal{F}(n,y) = \prod_{p|n} \Big(1 - \frac{\chi_{-4}(p)}{p}\Big) \prod_{\substack{p|n \\ p\le y}} \Big(1 + \frac{\chi_{-4}(p)}{p^\alpha}\Big)$$

where $\alpha = \alpha(n,y)$ is the unique positive solution to the equation

$$\sum_{p\le y} \frac{\log p}{p^\alpha - 1} = \log n.$$

For the proof we replace Vaughan type identities with Buchstab's identity. An extra complication arises from the fact that the number of representations of n as $m + d_1^2x_1^2 + d_2^2x_2^2$ with m smooth is not multiplicative in d_1, d_2, which makes the application of a sieve problematic. Again we have to carry the sieve weights

explicitly through the computation and postpone the sum over m to the very last moment.

References

[1] E. Assing, V. Blomer, J. Li, *Uniform Titchmarsh divisor problems*, Adv. Math. **393** (2021), 108076.

[2] V. Blomer, L. Grimmelt, J. Li, S. Rydin Myerson, *Additive problems with almost prime squares*, `arXiv:2111.01601`

[3] J. B. Friedlander, H. Iwaniec, *Coordinate distribution of Gaussian primes*, J. Eur. Math. Soc. **24** (2022), 737–772.

[4] G. H. Hardy, J. E. Littlewood, *Some problems of partitio numerorum; III: on the expression of a number as a sum of primes*, Acta Math. **44** (1922), 1–70.

[5] C. Hooley, *On the representation of a number as the sum of two squares and a prime*, Acta Math. **97** (1957), 189–210.

[6] C. Hooley, *Applications of sieve methods to the theory of numbers* Cambridge Tracts in Mathematics **70** (1976), Cambridge University Press

[7] Ju. V. Linnik, *An asymptotic formula in an additive problem of Hardy-Littlewood*, Izv. Akad. Nauk SSSR Ser. Mat. **24** (1960), 629–706.

[8] N. Pitt, *On an analogue of Titchmarsh's divisor problem for holomorphic cusp forms*, J. Amer. Math. Soc. **26** (2013), 735–776

Unit fractions with unit summation

Thomas F. Bloom

An Egyptian fraction decomposition of 1 is a solution to

$$1 = \frac{1}{n_1} + \cdots + \frac{1}{n_k} \tag{1}$$

with $1 < n_1 < n_2 < \cdots < n_k$ distinct positive integers. (We stress that there is no restriction on k.) The study of such solutions is an old topic in number theory, and we are in particular concerned with the question of whether solutions can be found with the denominators n_i taken from a prescribed set $A \subset \mathbb{N}$.

There are no congruence restrictions (i.e. solutions can be found in any infinite arithmetic progression, as first shown by van Albada and van Lint [1]). There is an obvious trivial size requirement: if $\sum_{n\in A} \frac{1}{n} < 1$ then A cannot contain any solutions. For example, there are no solutions in $[N, 2N]$ for large N. Nonetheless, Croot [3] has shown that for large intervals this is the only constraint, so that for any $\varepsilon > 0$ and $N = N(\varepsilon)$ large enough $A = [N, (e + \varepsilon)N]$ contains a solution.

Given the absence of any non-trivial obvious arithmetic obstructions, it is natural to conjecture that (1) has a Ramsey-type property, in that any finite colouring of the integers contains a non-trivial solution to (1). This was conjectured many times by Erdős and Graham (see for example [5]) and was finally proved in a breakthrough paper of Croot [4].

Given this colouring statement, it is also natural to speculate whether in fact the largest colouring class always suffices, and that any $A \subset \mathbb{N}$ with positive density contains a solution to (1). This stronger statement was also conjectured by Erdős and Graham [5].

In this talk we discuss a proof of this conjecture, contained in the preprint [2], in a strong form: any $A \subset \mathbb{N}$ with positive upper density contains a solution to (1). Our methods also yield a quantitative form of a logarithmic density version: there exists a constant $C > 0$ such that if $A \subset [1, N]$ is a set of integers with

$$\sum_{n \in A} \frac{1}{n} \geq C \frac{\log\log\log N}{\log\log N} \log N$$

then A contains a solution to (1).

We build upon the methods of Croot, who used a variant of the circle method to count solutions to (1). In brief, if $A \subset [N, 2N]$ is a finite set of positive integers with $\sum_{n \in A} \frac{1}{n} < 2$ then a simple application of orthogonality shows that the number of solutions to (1) with $n_i \in A$ is

$$\frac{1}{P} \sum_{-P/2 < h \leq P/2} \prod_{n \in A} (1 + e(h/n)) - 1.$$

Provided all $n \in A$ have no very large prime divisors ($> N/\log N$, say) the term $h = 0$ contributes $2^{(1-o(1))|A|}$. The contribution from small h (say $|h| \leq N$) can be shown to be non-negative. To prove the existence of solutions to (1) it suffices, therefore, to show that the contribution from h with $N < |h| \leq P/2$ is small. Croot proves such a bound via an elegant, yet elaborate, combinatorial procedure concerning the distribution of multiples in intervals, that is too involved to summarise here.

Croot's original method in [4] in fact delivers a density result for sets A with a sufficiently strong 'smoothness' property, essentially that any $n \in A$ is not divisible by any prime power $q \geq n^{1/4-o(1)}$. This suffices to deduce the colouring result, since of course any finite colouring of all integers must produce a monochromatic set of such smooth integers with positive density.

For the new unrestricted density result Croot's smoothness exponent must be raised from $1/4 - o(1)$ to $1 - o(1)$. In brief, this is accomplished by replacing an L^∞ estimate for the 'minor arcs' with an L^1 estimate. This L^1 estimate is established by a modification of Croot's combinatorial procedure, allowing local information from large prime divisors to be carried throughout the argument. This allows for the requisite milder smoothness assumption, and the resulting L^1 estimate is still strong enough for the 'major arc' contribution to dominate.

References

[1] P. J. van Albada and J. H. van Lint, *Reciprocal bases for the integers*, Amer. Math. Monthly 70(1963), 170–174.

[2] T. F. Bloom, *On a density conjecture about unit fractions*, arXiv:2112.03726 (2021).

[3] E. S. Croot, *On unit fractions with denominators in short intervals*, Acta Arith. 99(2001), 99–114.

[4] E. S. Croot, *On a coloring conjecture about unit fractions*, Ann. of Math. 157(2003), 545-556.

[5] P. Erdős and R. L. Graham, *Old and new problems and results in combinatorial number theory*, Monographies de L'Enseignement Mathématique, 28. Université de Genève, Geneva, 1980.

Bateman-Horn, Chowla and the integral Hasse principle for random polynomials

Tim Browning
(joint work with Efthymios Sofos, Joni Teräväinen)

The average behaviour of arithmetic functions evaluated at polynomials $f \in \mathbb{Z}[t]$ has long been a central pursuit in analytic number theory. For the von Mangoldt function Λ, this encodes the fundamental question of when polynomials capture their primes. Here, Dirichlet's theorem allows us to handle linear polynomials, but polynomials such as $f(t) = t^2 + 1$ remain out of reach.

For the Liouville function λ, cancellation is predicted by the Chowla conjecture precisely when the polynomial is not proportional to the square of a polynomial. This also seems out of reach for irreducible polynomials of degree at least two. For the arithmetic function r that counts representations of an integer as a sum of two squares, this relates to deep questions about the solubility of the equation $u^2 + v^2 = f(t)$ in integers. Current techniques prevent us from treating such equations when $\deg(f) \geq 3$.

Inspired by recent work of Skorobogatov and Sofos [2], the purpose of this paper is to resolve all of these questions by introducing averaging over the coefficients of polynomials of a given degree.

Define the set of coefficient vectors

$$S_d(H) = \left\{ \mathbf{c} = (c_0, \dots, c_d) \in \mathbb{Z}^{d+1} : \max_{0 \leq i \leq d} |c_i| \leq H, c_0 > 0 \right\},$$

parameterising polynomials $f_{\mathbf{c}}(t) = c_0 t^d + \cdots + c_d \in \mathbb{Z}[t]$ with positive leading coefficient. Our first result shows that we typically obtain a polynomial lower bound on the number of prime values that a polynomial takes.

Theorem 1. *Let $d \geq 1$ and $\varepsilon > 0$ be fixed. Then, for 100% of degree d polynomials $f \in \mathbb{Z}[t]$ with coefficients in $S_d(H)$ and no fixed prime divisor, we have*

$$\#\{n \in \mathbb{N} : f(n) \text{ is prime}\} \geq H^{5/(19d)-\varepsilon}.$$

We are also able to treat Chowla's conjecture on average. Let λ be the Liouville function, which we extend to $\mathbb{Z}$ in the obvious way. The polynomial Chowla conjecture [1] states that, for any $f \in \mathbb{Z}[t]$ that is not of the form $cg(t)^2$ with $c \in \mathbb{R}$ and $g \in \mathbb{R}[t]$, we have

$$\sum_{n \leq x} \lambda(f(n)) = o(x).$$

Despite recent progress due to Tao and Teräväinen [3, 4, 5], concerning the case of polynomials that factor into linear factors, this conjecture remains wide open for any f that is irreducible and of degree at least 2. However, we can treat if on average, as in the following result.

Theorem 2. *Let $d \geq 1$ and let $x = H^{\frac{1}{100d}}$. Then, for 100% of degree d polynomials $f \in \mathbb{Z}[t]$ with coefficients in $S_d(H)$, we have*

$$\sum_{n \leq x} \lambda(f_{\mathbf{c}}(n)) \ll \frac{x}{(\log x)^{100}}.$$

Finally we are also able to study the Hasse principle on average for a certain Diophantine equation defined using norms. Let $K/\mathbb{Q}$ be a finite extension of number fields of degree $e \geq 2$ and fix a $\mathbb{Z}$-basis $\{\omega_1, \dots, \omega_e\}$ for the ring of integers of K. We will denote the corresponding *norm form* by $\mathrm{N}_K(\mathbf{x}) = N_{K/\mathbb{Q}}(x_1\omega_1 + \cdots + x_e\omega_e)$, where $\mathbf{x} = (x_1, \dots, x_e)$ and $N_{K/\mathbb{Q}}$ is the field norm.

Our final result concerns the probability that the equation

$$\mathrm{N}_K(\mathbf{x}) = f(t)$$

is soluble over $\mathbb{Z}$, for a randomly chosen degree d polynomial $f \in \mathbb{Z}[t]$. These surfaces are sometimes called *generalised Châtelet surfaces*. Put $S_d^{\mathrm{loc}}(H)$ for the set of $\mathbf{c} \in S_d(H)$ such that $\mathrm{N}_K(\mathbf{x}) = f_{\mathbf{c}}(t)$ is soluble over $\mathbb{Z}_p$ for all primes p. Then we prove the following result.

Theorem 3. *Let $d \geq 1$ and let $K/\mathbb{Q}$ be any number field of degree e. Then*

$$\frac{\#\left\{\mathbf{c} \in S_d^{\mathrm{loc}}(H) : \mathrm{N}_K(\mathbf{x}) = f_{\mathbf{c}}(t) \text{ is soluble over } \mathbb{Z}\right\}}{\#S_d^{\mathrm{loc}}(H)} = 1 + O_{d,K}\left(\frac{1}{(\log H)^{100}}\right),$$

where the implied constant depends only on d and K.

In other words, as degree d polynomials are ordered by height, the integral Hasse principle holds for 100% of generalised Châtelet surfaces.

References

[1] S. Chowla, *The Riemann hypothesis and Hilbert's tenth problem*, Mathematics and Its Applications, Vol. 4, Gordon and Breach Science Publishers, New York–London–Paris, 1965.

[2] A.N. Skorobogatov and E. Sofos, *Schinzel Hypothesis with probability 1 and rational points*, Inventiones Math., to appear.

[3] T. Tao, *The logarithmically averaged Chowla and Elliott conjectures for two-point correlations*, Forum Math. Pi **4** (2016), e8, 36pp.

[4] T. Tao and J. Teräväinen, *The structure of correlations of multiplicative functions at almost all scales, with applications to the Chowla and Elliott conjectures*, Algebra & Number Theory **13** (2019), 2103–2150.

[5] T. Tao and J. Teräväinen, *The structure of logarithmically averaged correlations of multiplicative functions, with applications to the Chowla and Elliott conjectures*, Duke Math. J. **168** (2019), 1977–2027.

Major arc moments of smooth Weyl sums

Jörg Brüdern
(joint work with Trevor D. Wooley)

Since the arrival of Hardy and Littlewood's circle method a century ago, progress on Waring's problem was considered the benchmark test for new devices added to their toolbox. Hardy and Littlewood themselves obtained $G(k) \le (k-2)2^{k-1}+5$ where $G(k)$, as usual, is the smallest number s such that all large natural numbers are the sum of s k-th powers of natural numbers. This was improved rapidly over the next decades, culminating in 1959 with Vinogradov's bound

$$G(k) \le 2k(\log k + 2\log\log k + O(\log\log\log k))$$

(see [7]). In 1989 Vaughan [4] introduced smooth numbers to the subject. This made it possible to preserve homogenenity to a larger extent than was possible by older routines. In this way, Vinogradov's bound was refined to

$$G(k) \le 2k(\log k + 2\log\log k + O(\log\log\log k))$$

Soon afterwards Wooley's efficient differencing enhanced the smooth numbers approach considerably. His bound is roughly half that of Vinogradov, showing that

$$G(k) \le k(\log k + \log\log k + 2 + O(\log\log k/\log k))$$

(see [8] and [10, Theorem 1.4]). This bound remained unimproved ever since.

Theorem 1. *For all $k \in \mathbb{N}$, one has $G(k) \le \lceil k(\log k + 4.20032)\rceil$.*

For very large k one can do slightly better. Let ω be the unique real solution, with $\omega \ge 1$, of the transcendental equation

$$\omega - 2 - 1/\omega = \log\omega.$$

Then put

$$C_1 = 2 + \log(\omega^2 - 3 - 2/\omega) \quad \text{and} \quad C_2 = \frac{\omega^2+3\omega-2}{\omega^2-\omega-2}.$$

The decimal representations of these numbers are

$$\omega = 3.548292\ldots, \quad C_1 = 4.200189\ldots \quad \text{and} \quad C_2 = 3.015478\ldots.$$

Theorem 2. *For all $k \in \mathbb{N}$, one has $G(k) < k(\log k + C_1) + C_2$.*

For smaller values of k, this may be refined further, and then our method improves on existing bounds for $G(k)$ for all $k \ge 14$.

In part III of their famous series Partitio Numerorum, Hardy and Littlewood made a number of conjectures concerning representations of intergers as the sum of a prime and a number of k-th powers. In this direction, let $H(k)$ denote the smallest number s such that all large natural numbers are the sum of a prime and s k-th powers of natural numbers. One easily proves that in this problem one needs no more than about half as many k-th powers as are required in Waring's problem when studied by the methods underlying the results in Theorems 1 and

2. The next theorem shows that much more is true. Let $r = 4$ or 5, and let c_r be the unique solution of the transcendental equation

$$2c_r = 2 + \log(rc_r - 1)$$

in the interval $[1, \infty)$. The decimal representations are $c_5 = 2.134693\ldots$ and $c_4 = 1.961969\ldots$.

Theorem 3. *One has $H(k) \le c_5 k + 4$. If the Riemann hypothesis is true for all Dirichlet L-functions, then $H(k) \le c_4 k + 4$.*

This is the first unconditional proof that $H(k)/k$ remains bounded. Again, refinements are possible for smaller k, and our method performs better than existing technology for all $k \ge 6$, under the Riemann hypothesis for Dirichlet l-functions also for $k = 5$.

The proofs of these results all depend on a new method for bounding major arc moments of smooth Weyl sums. When $1 \le R \le P$, let $\mathcal{A}(P, R)$ denote the set of integers $n \in [1, P]$, all of whose prime divisors are at most R. Let

$$f(\alpha; P, R) = \sum_{x \in \mathcal{A}(P,R)} e(\alpha x^k),$$

where, as usual, we write $e(z)$ to denote $\mathrm{e}^{2\pi i z}$. The work of Wooley [9] and Vaughan and Wooley [5, 6] supplies, for every real $t \ge 2$, relative small numbers Δ_t with the property that for any fixed positive real number ε there exists a positive real number η such that, whenever $1 \le R \le P^\eta$, one has

$$\int_0^1 |f(\alpha; P, R)|^t \, \mathrm{d}\alpha \ll P^{t-k+\Delta_t+\varepsilon}.$$

Now let Q be a real number with $1 \le Q \le P^{k/2}$, and let $\mathfrak{M} = \mathfrak{M}(Q)$ denote the union of the intervals $\{\alpha \in [0,1] : |q\alpha - a| \le QP^{-k}\}$ with $0 \le a \le q \le Q$ and $(a, q) = 1$. In this notation, and under the same conditions, one has

$$\int_{\mathfrak{M}(Q)} |f(\alpha; P, R)|^t \, \mathrm{d}\alpha \ll P^{t-k+\varepsilon} Q^{2\Delta_t/k}.$$

This bound is a versatile pruning device of great utility in various problems in additive number theory, well beyond those discussed here. A related bound appears in recent work of Liu and Zhao [3], but they work with a set of smooth numbers consisting solely of products of primes in a dyadic range, they have major arcs that are much narrower than ours, and their estimate is valid only when $t \ge k+1$ is an even integers. These restrictions rule out some applications, and make it difficult to combine their method with breaking convexity devices.

When combined with a new slicing method for minor arcs that is too technical to be described here in detail, the above major arc moment estimate suffices to arrive at Theorem 3. The results on Waring's problem depend on a further development where the t-th moment is restricted to localized major arcs $\mathfrak{M}(2Q) \setminus \mathfrak{M}(Q)$ in order to extract the most of Weyl type bounds for smooth numbers.

References

[1] J. Brüdern and T. D. Wooley, *Partitio Numerorum: sums of a prime and a number of k-th powers*, submitted, 26pp; arXiv:2211.10387.

[2] J. Brüdern and T. D. Wooley, *On Waring's problem for larger powers*, submitted, 28pp; arXiv:2211.10380.

[3] J. Liu and L. Zhao, *Representation by sums of unlike powers*, J. Reine Angew. Math. **781** (2021), 19–55.

[4] R. C. Vaughan, *A new iterative method in Waring's problem*, Acta Math. **162** (1989), no. 1-2, 1–71.

[5] R. C. Vaughan and T. D. Wooley, *Further improvements in Waring's problem*, Acta Math. **174** (1995), no. 2, 147–240.

[6] R. C. Vaughan and T. D. Wooley, *Further improvements in Waring's problem, IV: higher powers*, Acta Arith. **94** (2000), no. 3, 203–285.

[7] I. M. Vinogradov, *On an upper bound for $G(n)$*, Izv. Akad. Nauk SSSR Ser. Mat. **23** (1959), 637–642.

[8] T. D. Wooley, *Large improvements in Waring's problem*, Ann. of Math. (2) **135** (1992), no. 1, 131–164.

[9] T. D. Wooley, *The application of a new mean value theorem to the fractional parts of polynomials*, Acta Arith. **65** (1993), no. 2, 163–179.

[10] T. D. Wooley, *New estimates for smooth Weyl sums*, J. London Math. Soc. (2) **51** (1995), no. 1, 1–13.

[11] T. D. Wooley, *On Waring's problem for intermediate powers*, Acta Arith. **176** (2016), no. 3, 241–247.

Generalised Rado and Roth criteria

Sam Chow

(joint work with Jonathan Chapman)

Roth [11] showed that $x+y=2z$ is *density regular*, i.e. if $A \subseteq \mathbb{N}$ has positive upper density then there exist $x, y, z \in A$ distinct solving the equation. The equation $x + y = z$ is not density regular, for it has no solution in odd numbers. However, Schur (1916, see [4]) showed that it has the weaker property of being *partition regular*, i.e. if $\mathbb{N} = C_1 \cup \cdots \cup C_r$ then there exist $j \in [r]$ and $x, y, z \in C_j$ solving the equation.

Let $d \geq 2$ be an integer, and define

$$s_1(d) = \begin{cases} 5, & \text{if } d = 2, \\ 9, & \text{if } d = 3, \\ d^2 - d + 2\lfloor \sqrt{2d+2} \rfloor + 1, & \text{if } d \geq 4. \end{cases}$$

This is essentially the number of variables currently needed for the asymptotic formula in Waring's problem [13].

Theorem 1. *Let $s \geq s_1(d)$, let $a_1, \dots, a_s \in \mathbb{Z} \setminus \{0\}$, and let $P(x) \in \mathbb{Z}[x]$ have degree d. Then the diophantine equation*

$$\sum_{i \leq s} a_i P(x_i) = 0$$

is

- *DR iff* $\sum_i a_i = 0$*;*
- *PR iff*
  - $\sum_i a_i = 0$ ***or***
  - ∗ *there exists non-empty* $I \subseteq [s]$ *such that* $\sum_{i\in I} a_i = 0$ ***and***
    ∗ P *is intersective (has a root modulo any* $q \in \mathbb{N}$*).*

We further generalise to $\sum_i a_i P(x_i) = b$, and show that there are at least a positive constant times X^{s-d} dense/monochromatic solutions up to height X. Note that if $\sum_i a_i = 0$ then we can replace $P(x)$ by the intersective polynomial $P(x) - P(0)$. Thus, intersectivity characterises partition regularity of these equations, much like with the Furstenberg–Sárköy problem [7].

Previously:

- Rado [10] characterised PR in the case $P(x) = x$.
- Roth [12] characterised DR in the case $P(x) = x$.
- Green [5] established Roth's theorem over the primes.
- Browning and Prendiville [1] characterised DR for $P(x) = x^2$, when $s \geq 5$.
- C. [2] characterised DR for $P(x) = x^d$, including over the primes, when $s \geq (1 + o(1))s_1(d)$.
- C., Lindqvist and Prendiville [3] characterised PR for $P(x) = x^d$, when $s \geq (1 + o(1))d \log d$, using smooth numbers.

We use the Fourier-analytic transference principle [9] to linearise some of the variables. This requires Fourier decay, which is ensured by the W-trick. However, a naive application of the W-trick falsifies the other key input required for transference to succeed, namely Fourier restriction (tight estimates for mean values of weighted exponential sums). To solve this, we deploy a two-step W-trick in tandem with Lucier's auxiliary intersective polynomials [8].

A further difficulty arises in the colouring problem. In the case of homogeneous equations, this aspect was solved in [3] using *homogeneous sets*. The equations dealt with in the present work are, in general, inhomogeneous. We resolve the issue by choosing the colour class which has the largest intersection with a certain polynomial Bohr set that arises from an application of the arithmetic regularity lemma [6].

References

[1] T. Browning and S. Prendiville, *A transference approach to a Roth-type theorem in the squares*, Int. Math. Res. Not. **2017,** 2219–2248.

[2] S. Chow, *Roth–Waring–Goldbach*, Int. Math. Res. Not. **2018,** 2341–2374.

[3] S. Chow, S. Lindqvist and S. Prendiville, *Rado's criterion over squares and higher powers*, J. Eur. Math. Soc. **23** (2021), 1925–1997.

[4] R. L. Graham, B. L. Rothschild and J. H. Spencer, *Ramsey theory*, Second edition, John Wiley & Sons, Inc., New York, 1990.

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

[6] B. Green and T. Tao, *An arithmetic regularity lemma, associated counting lemma, and applications*, 2020 update, arXiv:1002.2028v3.

[7] T. H. Lê, *Problems and results on intersective sets.* In: Combinatorial and Additive Number Theory (pp. 115–128), Springer, New York, 2014.

[8] J. Lucier, *Intersective sets given by a polynomial*, Acta Arith. **123** (2006), 57–95.

[9] S. Prendiville, *Counting monochromatic solutions to diagonal Diophantine equations*, Discrete Anal. (2021), Paper No. 14, 47 pp.
[10] R. Rado, *Studien zur Kombinatorik*, Math. Z. **36** (1933), 242–280.
[11] K. F. Roth, *On certain sets of integers*, J. London Math. Soc. **28** (1953), 104–109.
[12] K. F. Roth, *On certain sets of integers (II)*, J. London Math. Soc. **29** (1954), 20–26.
[13] T. D. Wooley, *Nested efficient congruencing and relatives of Vinogradov's mean value theorem*, Proc. London Math. Soc. (3) **118** (2019), 942–1016.

On the largest prime factor of quartic polynomial values: the cyclic and dihedral cases

Cécile Dartyge
(joint work with James Maynard)

Let $P \in \mathbb{Z}[X]$ be an irreducible polynomial with no fixed divisor. Are there infinitely many integers n such that $P(n)$ is a prime number? Schinzel and Sierpiński [5] have formulated a general and quantitative conjecture associated to this question.

When $P(X)$ has degree one, Dirichlet's Theorem on prime numbers in arithmetic progressions, provides a positive answer but this problem is still open for polynomials of degree ≥ 2. A natural approach is to try to find polynomial values with a large prime factor.

Let $P^+(n)$ denote the largest prime factor of the integer n. Chebyshev proved that

$$\lim_{x\to\infty} \frac{1}{x} P^+\Big(\prod_{n\leq x}(n^2+1)\Big) = +\infty.$$

The best general result was obtained by Tenenbaum [6] who proved that if $f(X) \in \mathbb{Z}[X]$ is irreducible with degree ≥ 2 then for $\alpha \in]0, 2-\log 4[$,

$$P^+\Big(\prod_{n\leq x} f(n)\Big) \geq x \exp((\log x)^\alpha), \qquad (x \geq x_0(\alpha, f)).$$

When the degree of f is small it is possible to have better lower bound. In this talk we focus on quartic polynomials. Dartyge [2] has handled the case of the twelfth cyclotomic polynomial $\Phi_{12}(X) = X^4 - X^2 + 1$. Her result has been generalised by La Bretèche [1] to monic, even, irreducible quartic polynomials with Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In this talk we present the following Theorem:

Theorem 1 (C. Dartyge and J. Maynard). *Let $P \in \mathbb{Z}[X]$ be monic, irreducible, quartic, with Galois group isomorphic to $C_4 := \mathbb{Z}/4\mathbb{Z}$ or $D_4 := \mathbb{Z}/4\mathbb{Z} \propto \mathbb{Z}/2\mathbb{Z}$. Then there exists $c_P > 0$ such that for $x > x_0(P)$, we have:*

$$\sharp\{x < n \leq 2x : P^+(P(n)) \geq x^{1+c_P}\} \gg x.$$

The first step of the proof is an adaptation of Heath-Brown's method [3] for detecting large prime factors of some polynomial values.

Let r_1 be a root of the polynomial P, N_P the norm in the $\mathbb{Q}$-extension $\mathbb{Q}(r_1)$. The arguments of Heath-Brown imply that if we can find δ_1, δ_2 strictly positif such that for all x large enough

$$\sharp\{n \in [x, 2x] : \prod_{\substack{\mathfrak{P}|(n-r_1)\\ N_P(\mathfrak{P})\leq x}} N_P(\mathfrak{P}) \geq x^{1+\delta_1}\} \geq \delta_2 x,$$

then there exists $c_P = c_P(P, \delta_1, \delta_2) > 0$ satisfying Theorem 1.

To achieve this we introduce a set of ideals J of the integer ring of $\mathbb{Q}(r_1)$ formed by principal ideals (α), $\alpha = a_0 + a_1 r_1 + a_2 r_1^2 + a_3 r_1^3$, where $(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$ are required to satisfy several technical conditions, in particular, we impose that $P^+(N_P(\alpha)) \leq x$ and $X^{1+\alpha_0/2} \leq N_P(\alpha) \leq X^{1+\alpha_0}$.

We need thus to understand the congruence $n - r_1 \in (\alpha)$. We prove that this congruence can be reformulated as a congruence between some integers. A crucial step of the proof is then to obtain non trivial bound of exponential sums of type

$$\sum_{(a_1,a_2,a_3)\in C} \sum_{\substack{A\leq a\leq A+B\\ (B_{14},q)=1}} \exp\Big(\frac{2i\pi h B_{13}(a_0,a_1,a_2,a_3)\overline{B_{14}(a_0,a_1,a_2,a_3)}}{q(a_1,a_2,a_3)}\Big),$$

where $B_{13}(a_0, a_1, a_2, a_3)$, $B_{14}(a_0, a_1, a_2, a_3)$ and $q(a_1, a_2, a_3)$ are some polynomials with integer coefficients.

This sum is bounded with a q-analogue Van der Corput's result obtained by Heath-Brown [3] provided the modulus $q(a_1, a_2, a_3)$ has only small prime factors.

It remains to prove that there exists a positive proportion of (a_1, a_2, a_3) such that $q(a_1, a_2, a_3)$ has a suitable factorisation.

La Bretèche and Mestre [1] have clarified the shape of the form q. Their result applied to quartic polynomials P implies that

$$q(a_1, a_2, a_3) = \pm \prod_{1\leq i<j\leq 4} \frac{a(r_i) - a(r_j)}{r_i - r_j},$$

where r_1, r_2, r_3, r_4 are the roots of P, and $a(r) = a_0 + a_1 r + a_2 r^2 + a_3 r^3$.

Let G denotes the Galois group of P. If G is the Klein group, $G = \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ as in [1] and [2], then $q(a_1, a_2, a_2)$ has a nice factorisation:

$$q(a_1, a_2, a_3) = q_1(a_1, a_2, a_3)q_2(a_1, a_2, a_3)q_3(a_1, a_2, a_3),$$

where q_1, q_2, q_3 are three ternary quadratic forms. It is then possible by using lattice counting points arguments, to prove that $q(a_1, a_2, a_3)$ don't have too large prime factors.

If $G = C_4$ or D_4 then we can order the roots of P such that $r_1r_2 + r_3r_4 \in \mathbb{Q}$. In this case $q(a_1, a_2, a_3)$ has the factorisation

$$q(a_1, a_2, a_3) = q_1(a_1, a_2, a_3)q_2(a_1, a_2, a_3),$$

where now $q_1(a_1, a_2, a_3)$ is an irreducible form of degree 4 and $q_2(a_1, a_2, a_3)$ is a quadratic form.

The methods of [1], [2] doesn't work in this case. However in our case, the form q_1 is not arbitrary. We prove that $q_1(a_1, a_2, a_3)$ is an incomplete norm form:

$$q_1(a_1, a_2, a_3) = N_{\mathbb{Q}(r_1+r_3)/\mathbb{Q}}(a_1 + a_2(r_1 + r_3) + a_3(r_1^2 + r_1 r_3 + r_3^2)).$$

Maynard [4] has obtained asymptotic formulae for the number of prime numbers represented by incomplete norm forms. Let $f(X) \in \mathbb{Z}[X]$ be monic, irreducible of degree n and θ be a root of f. Maynard's Theorem says that for $n \geq 4k$ we have:

$$\sharp\Big\{(a_1, \dots, a_{n-k}) \in [1, X]^{n-k} : N_{\mathbb{Q}(\theta)/\mathbb{Q}}\Big(\sum_{i=1}^{n-k} a_i \theta^{i-1}\Big)\Big\} = (C(f) + o(1))\frac{X^{n-k}}{n \log X},$$

with

$$C(f) = \prod_p \Big(1 - \frac{\nu(p)}{p^{n-k}}\Big)\Big(1 - \frac{1}{p}\Big)^{-1}$$

$$\nu(p) = \sharp\Big\{1 \leq a_1, \dots, a_{n-k} \leq p : N_{\mathbb{Q}(\theta)/\mathbb{Q}}\Big(\sum_{i=1}^{n-k} a_i \theta^{i-1}\Big) \equiv 0 \mod p\Big\}.$$

When $k = 1$, this Theorem can be used for polynomials of degree at least 4. An important part of the proof of Theorem 1 consists to generalise Maynard's ingredients for the type II sums in [4] in order to find a positive proportion of (a_1, a_2, a_3) such that $q_1(a_1, a_2, a_3)$ and $q_2(a_1, a_2, a_3)$ have a factorisation compatible to Heath-Brown's bound for very short exponential sums.

References

[1] R. de la Bretèche, *Plus grand facteur premier de valeurs de polynômes aux entiers*, Acta Arith. **169** (2015), 221–250.

[2] C. Dartyge, *Le problème de Tchébychev pour le douzième polynôme cyclotomique*, Proc. London Math. Soc. **111**(1) (2015), 1–62.

[3] D. R. Heath-Brown, *The largest prime factor of* $x^3 + 2$, Proc. London Math. Soc. **82**(3) (2001), 554–596.

[4] J. Maynard, *Primes represented by incomplete norm forms*, Forum of Mathematics, Pi **8**(3) (2020), 1–128.

[5] A. Schinzel and W. Sierpiński , *Sur certaines hypothèses concernant les nombres premeirs*, Acta Arith. **4**(3) (1958), 185–208.

[6] G. Tenenbaum, *Sur une question d'Erdős et Schinzel. II*, Invent. Math. **99** (1990), 215–224.

Extending the unconditional support in an Iwaniec–Luo–Sarnak family

Lucile Devin

(joint work with Daniel Fiorilli, Anders Södergren)

In [6], Katz and Sarnak conjectured the existence of symmetry groups that describe the distribution of the zeros close to the real line for L-functions in certain families. This conjecture is far from being proven, but many partial results have

been obtained. More precisely, given a family $\mathcal{F}$ of L-functions ordered by conductor, they conjecture that for all even Schwartz functions ϕ with compactly supported Fourier transform, the one-level density

$$\frac{1}{|\mathcal{F}(Q)|}\sum_{f\in\mathcal{F}(Q)}\sum_{\substack{\gamma\\ L(\frac{1}{2}+i\gamma,f)=0}}\phi\big(\tfrac{\log Q}{2\pi}\gamma\big)$$

converges as $Q\to\infty$ and the limit depends only on the symmetry type of the family (which can be Orthogonal, Orthogonal odd, Orthogonal even, Symplectic or Unitary). The limit is then given by the limiting distribution of eigenvalues close to 1 for random matrices in the corresponding group.

In their famous paper [5], Iwaniec, Luo and Sarnak studied the one-level density for families of L-functions attached to holomorphic newforms. Among many other results, they proved the Katz–Sarnak prediction for the family of L-functions attached to newforms of fixed even weight k and square-free level tending to infinity, under the condition that the Fourier transform $\widehat{\phi}$ of the test function has compact support included in $(-\frac{3}{2},\frac{3}{2})$. Moreover, assuming the Generalized Riemann Hypothesis, they were able to extend this admissible support to $(-2,2)$. In [1], we extend the unconditional admissible support in the harmonically weighted one-level density of the low-lying zeros of L-functions in this family with level tending to infinity through the primes.

To be more precise, let us introduce some notation. We fix a basis $B_k^*(N)$ of Hecke eigenforms of the space $H_k^*(N)$ of newforms of prime level N and weight k. Each of these forms has Fourier expansion $f(z)=\sum_{n=1}^{\infty}\lambda_f(n)n^{\frac{k-1}{2}}e^{2\pi inz}$, where we fix $\lambda_f(1)=1$. We use the harmonic weights defined as

$$\omega_f(N):=\frac{\Gamma(k-1)}{(4\pi)^{k-1}(f,f)_N};\qquad \text{where } (f,f)_N:=\int_{\Gamma_0(N)\backslash\mathbb{H}}y^{k-2}|f(z)|^2\mathrm{d}x\mathrm{d}y,$$

and observe that by [2, 3], these are essentially constant of size $|B_k^*(N)|^{-1}$. The harmonically weighted one-level density for this family is defined as

$$\mathcal{D}_{k,N}^*(\phi;N):=\frac{1}{\Omega_k(N)}\sum_{f\in B_k^*(N)}\omega_f(N)\sum_{\gamma_f}\phi\Big(\frac{\log(k^2N)}{2\pi}\gamma_f\Big),$$

where $\rho_f=\frac{1}{2}+i\gamma_f$ runs through the non-trivial zeros of $L(s,f)$ (note that γ_f is allowed to be non-real), ϕ is an even Schwartz function whose Fourier transform is compactly supported, and the total weight is given by

$$\Omega_k(N)=\sum_{f\in B_k^*(N)}\omega_f(N)=1+O_k(N^{-1}).$$

We prove the following result ([1, Theorem 1.1]).

Theorem 1. *Let ϕ be an even Schwartz function for which* $\mathrm{supp}(\widehat{\phi})\subset(-\Theta_k,\Theta_k)$, *where*

$$\Theta_k:=\begin{cases}1+\frac{\sqrt{3}}{2} & \text{if } k=2;\\ 2\big(1-\frac{1}{10k-5}\big) & \text{if } k\geq 4.\end{cases}$$

Then, for N running through the set of prime numbers, we have the estimate

$$D^*_{k,N}(\phi; N) = \int_{\mathbb{R}} W(O)(x)\phi(x)\mathrm{d}x + o_{N\to\infty}(1), \tag{1}$$

where $W(O)(x) = 1 + \frac{1}{2}\delta_0(x)$.

The novelty in our approach is that we use zero density estimates for Dirichlet L-functions after applying the Petersson formula. This extends the unconditional support that was obtained previously by using only the Weil bound for Kloosterman sums. The specific result we use is [4, Theorem 10.4], giving zero density estimates on average for a family of Dirichlet L-functions. We also show that the Grand Density Conjecture would lead to an admissible support of $(-2, 2)$, thus recovering the support previously obtained under the stronger assumption of the Generalized Riemann Hypothesis.

References

[1] L. Devin, D. Fiorilli, A. Södergren, Extending the unconditional support in an Iwaniec-Luo-Sarnak family, arXiv:2210.15782.

[2] J. Hoffstein, P. Lockhart, *Coefficients of Maass forms and the Siegel zero*, Ann. of Math. (2) **140** (1994), no. 1, 161–181.

[3] H. Iwaniec, *Small eigenvalues of Laplacian for $\Gamma_0(N)$, Acta Arith*, **56** (1990), no. 1, 65–82.

[4] H. Iwaniec, E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications **53**, American Mathematical Society, Providence, RI, 2004.

[5] H. Iwaniec, W. Luo, P. Sarnak, Low lying zeros of families of L-functions, Inst. Hautes Études Sci. Publ. Math. **91** (2000), 55–131.

[6] N. M. Katz, P. Sarnak, Zeroes of zeta functions and symmetry, Bull. Amer. Math. Soc. (N.S.) **36** (1999), no. 1, 1–26.

Longer gaps between values of binary quadratic forms

Rainer Dietmann

(joint work with Christian Elsholtz, Alexander Kalmynin, Sergei Konyagin and James Maynard)

Let $s_1, s_2, \ldots$ be an arithmetically interesting sequence of positive integers, arranged in increasing order, for example the sequence of primes or the sequence of integers that are sums of two squares. A natural question is the behaviour of the gaps $s_{n+1} - s_n$, in particular regarding short and longs gaps. This problem has been extensively studied for the primes. In this talk we consider numbers that are sums of two squares, or more generally numbers that are represented by *any* binary quadratic form of fixed fundamental discriminant D. As short gaps are well understood here, we want to focus on long gaps. For the sequence $s_1, s_2, \ldots$ of numbers that are sums of two squares, Erdős [2] obtained

$$s_{n+1} - s_n \gg \frac{\log s_n}{\sqrt{\log\log s_n}}$$

for infinitely many n. This was improved by Richards [3] who showed that for fixed fundamental discriminant D, for the sequence of positive integers $s_1, s_2, \ldots$ represented by any binary quadratic form of discriminant D we have

$$\limsup_{n\to\infty} \frac{s_{n+1} - s_n}{\log s_n} \geq \frac{1}{|D|}. \tag{1}$$

Note that the special case $D = -4$ corresponds to the sequence of numbers that are sums of two squares. This result held the record for the past 40 years. We recently obtained the following improvement [1], both in the special case $D = -4$ as well as for general D.

Theorem 1. *For $D = -4$, the $\frac{1}{4}$ in (1) can be replaced by*

$$\frac{390}{449} = 0.868\ldots$$

Theorem 2. *In general, the $\frac{1}{|D|}$ in (1) can be replaced by*

$$\frac{|D|}{2\varphi(|D|)(\log|D| + O((\log\log|D|)^3))},$$

where φ denotes Euler's totient function.

The dependence on $|D|$ now has become very mild in Theorem 2, which for convenience is only stated in its asymptotic form.

Our proof follows the basic idea of Richards, but introduces two new refinements, a *modular* and a *probabilistic* one, which we briefly sketched in our talk in the context of Theorem 1: Numbers in an interval of given length k are excluded to be sums of two squares by imposing suitable congruence conditions on the starting point y of the interval, and the modular and probabilistic refinements allow to make these conditions fewer and milder than in Richards' original work, which leads to a smaller y in terms of k.

References

[1] R. Dietmann, C. Elsholtz, A. Kalmynin, S. Konyagin, J. Maynard, *Longer gaps between values of binary quadratic forms*, to appear in *Int. Math. Res. Not. IMRN*.

[2] P. Erdös, *Some problems and results in elementary number theory*, Publ. Math. Debrecen **2** (1951), 103–109.

[3] Ian Richards, *On the gaps between numbers which are sums of two squares*, Adv. in Math. **46** (1982), 1–2.

Negative moments of the Riemann zeta-function

Alexandra Florea
(joint work with Hung Bui)

This report is concerned with the study of negative moments of the Riemann zeta-function. Positive moments of $\zeta(s)$ are relatively well-understood. For example, lower bounds and upper bounds (conditional on RH) of the right order of magnitude establish the rate of growth of all the positive moments. Much less is known about the negative moments, even conjecturally.

For $k > 0$ and $0 < \alpha \leq 1$, let

$$I_{-k}(T) = \frac{1}{T}\int_{T}^{2T} \Big|\zeta(1/2+\alpha+it)\Big|^{2k} \tag{1}$$

denote the negative $2k^{\text{th}}$ moments of $\zeta(s)$ with the shift α. A conjecture of Gonek [3] predicts the size of the negative moments in different ranges.

Conjecture 1. *Let $k > 0$ be fixed. Uniformly for $\frac{1}{\log T} \leq \alpha \leq 1$,*

$$I_{-k}(\alpha, T) \asymp \Big(\frac{1}{\alpha}\Big)^{k^2},$$

and uniformly for $0 < \alpha \leq \frac{1}{\log T}$,

$$I_{-k}(\alpha, T) \asymp \begin{cases} (\log T)^{k^2} & \text{if } k < 1/2, \\ (\log \frac{e}{\alpha \log T})(\log T)^{k^2} & \text{if } k = 1/2 \\ (\alpha(\log T))^{1-2k}(\log T)^{k^2} & \text{if } k > 1/2. \end{cases}$$

More recent random matrix theory (RMT) computations due to Berry and Keating [1] and Forrester and Keating [2] provide an alternative way of predicting formulas for negative moments. However, when $0 < \alpha \leq \frac{1}{\log T}$ and $k \geq 3/2$, RMT predictions diverge from Conjecture 1, and suggest certain "transition regimes" in the asymptotic formulas for $k = (2n+1)/2$, and n a positive integer.

Under RH, Gonek [3] proved lower bounds of the conjectured order of magnitude for all $k > 0$ and $\frac{1}{\log T} \leq \alpha \leq 1$ and for $k < 1/2$ and $0 < \alpha \leq \frac{1}{\log T}$.

In forthcoming work with Hung Bui, under RH, we obtain upper bounds for the negative moments in certain ranges of the shift α. Firstly, when the shift $\alpha \gg (\log\log T)^{a_k}/(\log T)^{\frac{1}{2k}}$ (where a_k is an explicit constant depending on k), we obtain almost sharp upper bounds (consistent with Conjecture 1), up to some $\log\log T$ factor. We also further refine the upper bound in this range to obtain an asymptotic formula for the negative moments. For example, we obtain an asymptotic formula for (1) when $\alpha \gg (\log\log T)^8/(\log T)$, and $k < 1/2$. Secondly, we obtain non-trivial upper bounds for (1) when $\alpha = o((\log\log T)^{a_k}/(\log T)^{\frac{1}{2k}})$ and $\log(1/\alpha)/\log\log T \ll 1$. As an application, we slightly improve a conditional bound of Soundararajan [4] on averages of the Möbius function.

The techniques used draw on ideas of Soundararajan and Harper on obtaining conditional sharp bounds for the positive moments of the Riemann zeta-function. However, while the contribution from zeros of $\zeta(s)$ turns out to be quite benign

in the case of positive moments, more care is needed to deal with the possibly large contributions from zeros in the case of negative moments. To obtain upper bounds for (1), one needs to use an a priori bound for the negative moments, which is done first by employing a pointwise bound for $\zeta(s)^{-1}$. In certain ranges, one is able to then use a recursive, self-improving bound to strengthen the results previously obtained.

References

[1] M. V. Berry, J. P. Keating, *Clusters of near-degenerate levels dominate negative moments of spectral determinants*, J. Phys. A **35** (2002), L1–L6.

[2] P. J. Forrester, J. P. Keating, *Singularity dominated strong fluctuations for some random matrix averages*, Commun. Math. Phys. **250** (2004), 119–131.

[3] S. M. Gonek, *On negative moments of the Riemann zeta-function*, Mathematika **36** (1989), 71–88.

[4] K. Soundararajan, *Partial sums of the Möbius function*, J. reine angew. Math. **631** (2009), 141–152.

On Sárközy's theorem for shifted primes

Ben Green

A set $S \subset \mathbf{N}$ is called intersective if, for any set $A \subseteq \mathbf{N}$ with positive upper density, we have $(A-A) \cap S \neq \emptyset$, that is to say some two elements of A differ by an element of S.

Solving a conjecture of Lovász, Sárközy and Furstenberg independently showed in the 1970s that the squares are intersective. They used rather different methods: Sárközy used the circle method in the spirit of Roth's proof that sets of positive density contain 3-term progressions, while Furstenberg used methods of ergdic theory.

Answering a conjecture of Erdős, Sárközy used similar methods to show that the set $\{p-1 : p \text{ prime}\}$ is intersective. (Simple examples such as the set of multiples of 4 show that the primes themselves are not intersective.)

My talk concerns quantitative versions of this latter result. Denote by $A(N)$ the size of the largest subset of $\{1, \dots, N\}$ not containing distinct elements a, a' with $a - a' = p - 1$, p a prime. Then Sárközy showed that $A(N) \ll N(\log\log N)^{-2+o(1)}$. This was subsequently improved by Lucier, and then by Ruzsa and Sanders, before Zoe Wang showed in 2020 that $A(N) \ll Ne^{-C(\log N)^{1/3}}$.

The main result of my talk is that $A(N) \ll N^{-c}$ for some positive constant c. A detailed proof of this result may be found in the manuscript [1]. Assuming GRH, c can be taken to be any constant less than $\frac{1}{12}$.

Previous approaches to the problem have used a mode of argument called *density increment*, which was introduced by Roth in his 1953 paper [3] on progressions of length 3. Assuming that $A \subset \{1, \dots, N\}$ is a set of density α which does not contain any pair of elements differing by $p-1$, some Fourier-analytic arguments are used to show that there is some large subprogression $P \subset \{1, \dots, N\}$ on which

the density of A is appreciably larger than α. Iterating this kind of argument eventually leads to a contradiction.

To prove the main result stated above, a different kind of argument is used: the shifted primes are shown to have a property called the *van der Corput property*, which is strictly stronger than being an intersective set. For the shifted primes, what this means is that there exists a function $\Phi : \{1, \dots, N\} \to \mathbf{R}$ which is supported on the shifted primes $\leq N$, which has average value 1, and which satisfies the Fourier positivity property

$$\sum_{n \leq N} \Phi(n) \cos(2\pi\theta n) \geq -N^{1-c}$$

for all $\theta \in \mathbf{R}/\mathbf{Z}$.

It is not hard (though not obvious) to show that this property implies the bound $A(N) \ll N^{1-c}$ mentioned above (Montgomery's book [2, Chapter 2] is a good source for this.)

Constructing Φ is a substantial task and only a brief sketch can be given in a talk. It may be noted that the bound $A(N) \ll N^{1-c}$ implies Linnik's theorem on the least prime $\equiv 1 \pmod q$, and so any construction must include a proof of this theorem or else use it as a black box. The former option applies here, so zero-density and exceptional zero repulsion estimates come into the analysis, alongside various other ideas from sieve theory and the circle method.

References

[1] B. J. Green, *On Sárközy's theorem for shifted primes*, arXiv:2206.08001.

[2] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis,* CBMS Regional Conference Series in Mathematics **84**, AMS 1994.

[3] K. F. Roth, *On certain sets of integers,* J. London Math. Soc **28** (1953), 104–109.

On non-archimedean analogue of a question of Atkin and Serre

Sanoli Gun

(joint work with Yuri F Bilu and Sunil L Naik)

Let f be a cusp form of integer weight k for $\Gamma_0(N)$, where $N \geq 1$ is an integer. Let the Fourier expansion of f be given by

$$f(z) = \sum_{n+1}^{\infty} a_f(n) q^n,$$

where $z \in \mathbf{C}$ with $\Im(z) > 0$ and $q = e^{2i\pi z}$. When f is a normalized Hecke eigen cusp form of weight $k \geq 4$ and without complex multiplication, a question of Atkin-Serre [9] predicts that

$$|a_f(p)| \geq c(\epsilon) p^{\frac{k-3}{2} - \epsilon}$$

for any real number $\epsilon > 0$. In particular, when $f = \Delta$, where

$$\Delta(z) = \sum_{n=1}^{\infty} \tau(n) q^n = q \prod_{n=1}^{\infty} (1-q^n)^{24},$$

this conjecture predicts that

$$|\tau(n)| \geq c(\epsilon) p^{\frac{9}{2}-\epsilon}$$

for any $\epsilon > 0$. An oft-quoted conjecture of Lehmer suggest that $\tau(p) \neq 0$ for all primes p and Serre [10] in 1981 showed that this conjecture is true for almost all primes p. There are several refinements of Serre's 1981 result but Lehmer's conjecture still remains elusive.

In 1987, R. Murty, K. Murty and Shorey [8] showed that there exists a constant $c > 0$ such that

$$|\tau(n)| \geq (\log n)^c$$

provided $\tau(n) \neq 0$ is odd. It is easy to observe from Jacobi's triple product identity or by a Theorem of Tate about non-existence of non-trivial Galois representation from Galois group of $\overline{\mathbb{Q}}/\mathbb{Q}$ to $\mathrm{GL}_2(\overline{\mathbb{F}_2})$ which is ramified only at 2 that $\tau(p)$ is always even. One year later, R. Murty, K. Murty and Saradha [7] showed that there exists a constant $c > 0$ such that

$$|a_f(p)| \geq (\log p)^c$$

for almost all primes p. The best known result in this direction is Gafni, Thorner and Wong [3]. They showed that

$$a_f(p) \geq 2p^{11/2} \frac{\log\log p}{\sqrt{\log p}}$$

for almost all primes p.

In 2022, Bennett, Gherga, Patel and Siksek [1] considered a non-Archimedean analogue of the question of Atkin and Serre and showed that for any prime p and integer $m \geq 2$, the largest prime factor $P(\tau(p^m))$ of $\tau(p^m)$ satisfies

$$P(\tau(p^m)) \ > \ \alpha \cdot \frac{\log\log(p^m)}{\log\log\log(p^m)}$$

provided $\tau(p) \neq 0$. Here α is an absolute positive constant and $P(n)$ denotes the largest primes factor of n with the convention that $P(0) = P(\pm 1) = 1$. In joint works with Bilu and Naik [2] and with Naik [4], we show that for any $\epsilon > 0$ and integer $m \geq 1$, the largest prime factor of the p-th Fourier coefficient $a_f(p)$ of f, denoted by $P(a_f(p))$, satisfies

$$P(a_f(p^m)) \ > \ (\log p)^{1/8} (\log\log p)^{3/8-\epsilon}$$

for almost all primes p. Here f is a non-CM normalized Hecke eigen cusp forms of weight k, level N with integer Fourier coefficients. The results in [2] and [4] can be strengthened if we assume Generalized Riemann hypothesis.

References

[1] M.A.Bennett, A. Gherga, V. Patel and S. Siksek, *Odd values of the Ramanujan tau function*, Math. Ann. **382** (2022), no. 1-2, 203–238.

[2] Y. Bilu, S. Gun and S. Naik *On non-Archimedean analogue of Atkin-Serre Question*, submitted.

[3] A. Gafni, J. Thorner and P-J Wong, *Almost all primes satisfy the Atkin-Serre conjecture and are not extremal* Res. Number Theory **7** (2021), no. 2, Paper No. 31, 5 pp.

[4] S. Gun and S. Naik *On the largest prime factor of non-zero Fourier coefficients of Hecke eigenforms*, submitted.

[5] D.H. Lehmer, *Ramanujan's function $\tau(n)$*, Duke Math. J **10** (1943), 483–492.

[6] D. H. Lehmer, *The vanishing of Ramanujan's $\tau(n)$*, Duke Math. J. **14** (1947), 429–433.

[7] M. R. Murty, V. K. Murty and N. Saradha, *Modular forms and the Chebotarev density theorem*, Amer. J. Math. **110** (1988), no. 2, 253–281.

[8] M. R. Murty, V. K. Murty and T. N. Shorey, *Odd values of the Ramanujan τ-function* Bull. Soc. Math. France **115** (1987), no. 3, 391–395.

[9] J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, Enseign. Math. (2) **22** (1976), no. 3-4, 227–260.

[10] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401.

The typical size of character sums

Adam J Harper

I discussed the following theorem, which improves and generalises a result I discussed in an earlier Oberwolfach meeting (1744a).

Theorem 1. *Let r be a large prime. Then uniformly for any $1 \le x \le r$, any $0 \le q \le 1$, and any multiplicative function $h(n)$ that has absolute value 1 on primes and absolute value at most 1 on prime powers, we have*

$$\frac{1}{r-1}\sum_{\chi \bmod r}|\sum_{n\le x}h(n)\chi(n)|^{2q} \ll \left(\frac{x}{1+(1-q)\sqrt{\log\log(10L)}}\right)^q,$$

where $L = L_r := \min\{x, r/x\}$.

Two important cases covered by the theorem are $h(n) \equiv 1$, where it becomes a low moment bound for incomplete character sums; and $h(n) = \mu(n)$. One has an analogous result for the integral averages $\frac{1}{T}\int_0^T |\sum_{n\le x} h(n)n^{it}|^{2q}dt$, with L_r replaced by $L_T := \min\{x, T/x\}$.

Theorem 1 is motivated by a corresponding result for random multiplicative functions. Thus if $f(n)$ is a Steinhaus (or Rademacher) random multiplicative function, then Theorem 1 of Harper [2] asserts that

$$\mathbb{E}|\sum_{n\le x} f(n)|^{2q} \asymp \left(\frac{x}{1+(1-q)\sqrt{\log\log x}}\right)^q \quad \forall\, 0 \le q \le 1.$$

Notice that this is an order of magnitude result, rather than just an upper bound.

In the case where $h(n) \equiv 1$, there is a well known duality between the character sum $\sum_{n\le x}\chi(n)$ and the character sum $\sum_{n\le r/x}\chi(n)$, arising from Poisson

summation (alternatively known, in this context, as the approximate functional equation or the Pólya Fourier expansion). Indeed, roughly speaking we have $\frac{1}{\sqrt{x}}|\sum_{n\leq x}\chi(n)| \approx \sqrt{\frac{x}{r}}|\sum_{n\leq r/x}\chi(n)|$. This means that the quantity $\log\log(10L)$ appearing in Theorem 1 is a natural substitute for the quantity $\log\log x$ in the random multiplicative setting, and so it seems reasonable to conjecture that Theorem 1 is sharp when $h(n)\equiv 1$ and $x \leq 0.99r$, say. (For non-principal χ, if $0.99r < x \leq r$ we can observe that $\sum_{n\leq x}\chi(n) = -\sum_{x<n\leq r}\chi(n) = -\sum_{1\leq n<r-x}\chi(r-n) = -\chi(-1)\sum_{1\leq n<r-x}\chi(n)$, and then get a stronger moment bound by applying Theorem 1 to these sums instead.)

In the case where $h(n) = \mu(n)$ there is no duality, and it seems reasonable to conjecture that one should be able to replace $\log\log(10L)$ simply by $\log\log x$ in Theorem 1, as well as substantially relaxing the restriction that $x \leq r$. This would be in the spirit of a recent paper of Gorodetsky [1], who conjectured (based on function field considerations) that for all *natural number* exponents $q < \log r$, the moments $\frac{1}{r-1}\sum_{\chi \bmod r}|\sum_{n\leq x}\mu(n)\chi(n)|^{2q}$ should be asymptotic to the corresponding random multiplicative moments as x and r become large. In particular, I conjecture that for any $0 \leq q \leq 1$ and any fixed $A > 0$, we should have

$$\frac{1}{r-1}\sum_{\chi \bmod r}|\sum_{n\leq x}\mu(n)\chi(n)|^{2q} \ll (\frac{x}{1+(1-q)\sqrt{\log\log x}})^q \quad \forall\, x \leq r^A,$$

and

$$\frac{1}{2T}\int_{-T}^{T}|\sum_{n\leq x}\mu(n)n^{it}|^{2q}dt \ll (\frac{x}{1+(1-q)\sqrt{\log\log x}})^q \quad \forall\, x \leq T^A. \tag{1}$$

Whilst I do not know how to prove this conjecture, it seems plausibly attackable (at least assuming standard conjectures like the Riemann Hypothesis), and if true it would have significant arithmetic consequences. Standard arguments with Perron's formula imply that

$$\begin{aligned}\Big|\sum_{x<n\leq x+y}\mu(n)\Big| &\approx \Big|\frac{1}{2\pi i}\int_{-i(x/y)}^{i(x/y)}(\sum_{n\leq 2x}\frac{\mu(n)}{n^s})\frac{x^s((1+y/x)^s-1)}{s}ds\Big| \\ &\lesssim \frac{y}{x}\int_{-x/y}^{x/y}|\sum_{n\leq 2x}\frac{\mu(n)}{n^{it}}|dt,\end{aligned}$$

and so (1) (if true) would deliver a bound $|\sum_{x<n\leq x+y}\mu(n)| \lesssim \frac{\sqrt{x}}{(\log\log x)^{1/4}}$ provided $y \leq x^{1-\epsilon}$, say. Thus we could deduce there is cancellation in sums of the Möbius function in *all* short intervals of length $y \gg \frac{\sqrt{x}}{(\log\log x)^{1/4}}$. It is a major open problem to go below, or even to reach, the squareroot interval barrier in problems of this kind. See e.g. the recent beautiful work of Matomäki and Radziwiłł [3], which (among many other results) establishes the existence of positive and negative Möbius values (or, strictly speaking, values of the closely related Liouville function) in intervals of length $C\sqrt{x}$, for a large constant C.

References

[1] O. Gorodetsky, *Magic squares, the symmetric group and Möbius randomness*, preprint available online at
https://arxiv.org/abs/2102.11966

[2] A. J. Harper. *Moments of random multiplicative functions, I: Low moments, better than squareroot cancellation, and critical multiplicative chaos*, Forum of Mathematics, Pi, **8**, e1, 95pp. 2020

[3] K. Matomäki and M. Radziwiłł, *Multiplicative functions in short intervals*, Ann. of Math. 183(2-16), 1015–1056.

On a question of Davenport and diagonal cubic forms over $\mathbb{F}_q(t)$

Leonhard Hochfilzer

(joint work with Jakob Glas)

Let $(k, \mathcal{O}) \in \{(\mathbb{Q}, \mathbb{Z}), (\mathbb{F}_q(t), \mathbb{F}_q[t])\}$ and consider a homogeneous, non-singular cubic form $F \in k[x_1, \dots, x_n]$. Denote by $X \subset \mathbb{P}_k^{n-1}$ the variety defined by $F = 0$. One way to try and understand $X(k)$ and whether the Hasse principle holds is to consider the counting function

$$N(P) = \#\left\{\mathbf{x} \in \mathcal{O}^n \colon F(\mathbf{x}) = 0, |x_i| \leq |P| \text{ for } i = 1, \dots, n\right\},$$

where $P \in \mathcal{O}$ and when $k = \mathbb{F}_q(t)$ we consider the absolute value given by $|f/g| = q^{\deg(f)-\deg(g)}$. If $n \geq 5$ then one expects

$$N(P) \sim c|P|^{n-3},$$

where $c > 0$ if and only if $X(k_v) \neq \emptyset$ for all completions k_v. Therefore proving a result of this shape implies the Hasse principle for X. If $n \leq 4$ the situation becomes more complicated. For example, if $n = 4$ then the contribution from rational lines to $N(P)$ is at least $|P|^2$ provided they exist. Thus it is more interesting to study the counting function $N^o(P)$, which only counts solutions away from rational lines. According to Manin's conjecture one expects

$$N^o(P) \sim |P| \log|P|^{\rho-1},$$

where ρ is the rank of the Picard group of X.

What is known about this problem? If $k = \mathbb{Q}$ and $n \geq 9$ then across a series of papers written 1988–2013 Hooley showed the asmyptotic formula of the above shape and thus the Hasse Principle (cf. [8, 9, 10, 11]). If $n = 8$, Hooley manages to establish the same, however he needs to assume the Riemann hypothesis for certain Hasse-Weil L-functions arising in this context for his argument to go through (cf. [12]). Assume now that F is diagonal, that is, it can be written as follows $F(\mathbf{x}) = \sum_{i=1}^n F_i x_i^3$. This problem was tackled by Heath-Brown in a small number of variables [7]. If $n = 6$ he could establish the upper bound $N(P) \ll_\varepsilon |P|^{3+\varepsilon}$, which only just about misses out on the expected order of $N(P)$. Moreover he could show $N^o(P) \ll_\varepsilon |P|^{3/2+\varepsilon}$ if $n = 4$. Both results are conditional on Riemann hypotheses on certain Hasse-Weil L-functions.

By virtue of Deligne's seminal work [4] this raises the natural question whether one can unconditionally prove these results if $k = \mathbb{F}_q(t)$. Browning and Vishe considered this question and could successfully show an asymptotic formula for $N(P)$ if $n = 8$, provided $\mathrm{char}(\mathbb{F}_q) > 3$ and thus establish weak approximation for cubic hypersurfaces in $n \geq 8$ variables. Recall that weak approximation states that

$$X(k) \subset \prod_v X(k_v),$$

is dense, where we consider the product with respect to the product topology. Analogously to Heath-Brown's approach Jakob Glas and I unconditionally showed the following [5].

Theorem 1. (Glas–H.) *Let $F = \sum_{i=1}^n F_i x_i^3$ be a diagonal cubic form where $F_i \in \mathbb{F}_q(t)$ for $i = 1, \dots, n$. Assume that $\mathrm{char}(\mathbb{F}_q) \neq 3$. If $n = 6$ then we have*

$$N(P) \ll_\varepsilon |P|^{3+\varepsilon}.$$

If $n = 4$ and $\mathrm{char}(\mathbb{F}_q) > 3$ then we have

$$N^o(P) \ll_\varepsilon |P|^{3/2+\varepsilon},$$

and if $\mathrm{char}(\mathbb{F}_q) = 2$ then we have

$$N(P) \ll_\varepsilon |P|^{2+\varepsilon}.$$

In particular, this affirmatively answers a question of Davenport who in a 1964 letter to Keith Matthews asked whether one can establish the mean value bound

$$\#\left\{\mathbf{x} \in \mathbb{F}_q[t]^6 \colon x_1^3 + x_2^3 + x_3^3 = x_4^3 + x_5^3 + x_6^3\right\} \ll |P|^{3+\varepsilon}. \tag{1}$$

We prove this result adapting the circle method in the spirit of the methods developed by Heath-Brown [6] as was previously similarly done by Browning–Vishe [1]. Usually when the circle method is used in the context of cubic forms, Weyl differencing produces a factor of 6. Thus it is often difficult to obtain results when $\mathrm{char}(\mathbb{F}_q) = 2$ or 3. We can avoid this issue since we essentially replace Weyl differencing by Poisson summation. We also remark that the case $\mathrm{char}(\mathbb{F}_q) = 3$ is in a way not particularly interesting since solving a diagonal cubic form then reduces to a system of linear equations.

The mean value estimate (1) together with Weyl's inequality enables us to significantly Waring's problem in this context (in characteristic 2, Weyl's inequality was shown by Car [2]). Write $\mathbb{J}_q[t]$ for the additive closure of cubes in $\mathbb{F}_q[t]$ and denote by $\widetilde{G}_q(3)$ the smallest number n such that we obtain an asymptotic formula for

$$R_n(P) = \#\left\{\mathbf{x} \in \mathbb{F}_q[t]^n \colon \sum_{i=1}^n x_i^3 = P, |x_i| \leq q^{\lceil \frac{\deg P}{3} \rceil}\right\},$$

where $|P| \to \infty$ for $P \in \mathbb{J}_q[t]$. Trivially, $\widetilde{G}_{3^h}(3) = 1$. Further, Kubota [13] showed $\widetilde{G}_q(3) \leq 9$ if q is odd. The case of even characteristic has been analysed by Car and Cherly [3] who showed $\widetilde{G}_{2^h}(3) \leq 11$. In [5] we establish the following. Note that there is no restriction on the characteristic.

Theorem 2. (Glas–H.) *We have $\widetilde{G}_q(3) \leq 7$. That is, if $n \geq 7$ then there exists an asymptotic formula for $R_n(P)$. In particular $R_n(P) \geq 1$ for all sufficiently large P.*

Finally, using (1) we can also deduce weak approximation for diagonal cubic forms in at least 7 variables.

Theorem 3. (Glas–H.) *Let X be the variety defined by $\sum_{i=1}^n F_i x_i^3 = 0$, where $F_i \in \mathbb{F}_q(t)$. If $n \geq 7$ and if $\mathrm{char}(\mathbb{F}_q) > 3$ then weak approximation holds for X.*

We expect that one can show the result Theorem 3 in the case of even characteristic by adjusting the techniques in [2] in order to obtain Weyl's inequality in this context.

References

[1] T. Browning and P. Vishe, *Rational points on cubic hypersurfaces over $\mathbb{F}_q(t)$*, Geometric and Functional Analysis **25.3** (2015), 671–732.
[2] M. Car, *Sommes d'exponentielles dans $\mathbb{F}_{2^h}((X^{-1}))$*, Acta Arithmetica **62** (1992), 303–328.
[3] M. Car and J. Cherly, *Sommes de cubes dans l'anneau $\mathbb{F}_{2^h}[X]$*, Acta Arithmetica **65.3** (1993), 227–241.
[4] P. Deligne, *La conjecture du Weil: II*, Publications Mathématiques de l'Institut des Hautes Études Scientifiques **52** (1980), 137–252
[5] J. Glas and L. Hochfilzer, *On a question of Davenport and diagonal cubic forms over $\mathbb{F}_q(t)$*, arXiv:2208.05422 (2022), 39 pages
[6] D. R. Heath-Brown, *A new form of the circle method, and its application to quadratic forms*, J. Reine Angew. Math. **481** (1996), 149–206
[7] D. R. Heath-Brown, *The circle method and diagonal cubic forms*, Pholosophical Transactions of the Royal Society of London **356.1738** (1998), 673–699
[8] C. Hooley, *On nonary cubic forms*, J. Reine Angew. Math. **386** (1988), 32–98
[9] C. Hooley, *On nonary cubic forms II*, J. Reine Angew. Math. **415** (1991), 95–165
[10] C. Hooley, *On nonary cubic forms III*, J. Reine Angew. Math. **456** (1994), 53–63
[11] C. Hooley, *On nonary cubic forms IV*, J. Reine Angew. Math. **680** (1988), 23–39
[12] C. Hooley, *On octonary cubic forms*, Proceedings of the London Mathematical Society **109.1** (2014), 241–281
[13] R. M. Kubota, *Waring's problem for $\mathbb{F}_q[x]$*, Dissertationes Math. **117** (1974), 60pp

Twisted multiplicativity and exponential sums

Emmanuel Kowalski
(joint work with K. Soundararajan)

For a polynomial $f \in \mathbf{Z}[X]$ (or in $\mathbf{Z}[X, X^{-1}]$, or ...), a squarefree integer $q \geq 1$ and an integer a coprime to q, define

$$W_f(a;q) = \frac{1}{\sqrt{q}} \sum_{x \bmod q} e\Big(\frac{af(x)}{q}\Big).$$

Extend $W_f(a;q)$ to other values of q and a by putting $W_f(a;q) = 0$. These exponential sums satisfy the "twisted-multiplicativity" property

$$W_f(a;q_1q_2) = W_f(a\bar{q}_1;q_2)W_f(a\bar{q}_2;q_1),$$

which reflects the fact that $a \mapsto W_f(a;q)$ is the discrete Fourier transform modulo q of the counting function of solutions of $f(y) = x$, and this counting function is "compatible with the Chinese Remainder theorem".

The "trivial" individual bound for these sums is provided by the Weil bound, namely $|W_f(a;q)| \leq (\deg(f)-1)^{\omega(q)}$. We are interested in obtaining bounds for averages

$$\sum_{q \leq x} W_f(a;q)$$

where a is a fixed non-zero integer. However, there are currently no known technique to do this in a robust way, except by using the triangle inequality

$$\Big|\sum_{q \leq x} W_f(a;q)\Big| \leq \sum_{q \leq x} |W_f(a;q)|$$

and using a method going back to Hooley [1964].

Theorem 1. *Suppose that* $\deg(f) \geq 3$*, and that* f *is indecomposable (i.e. that* $f \neq f_1 \circ f_2$ *with* $\deg(f_i) \geq 2$*). Fix* $a \neq 0$ *in* $\mathbf{Z}$*.*

(a) We have

$$\sum_{q \leq x} |W_f(a;q)|^2 \ll x(\log\log x)^{(d-1)^2} \tag{1}$$

for $x \geq 2$*.*

(b) There exists $\delta > 0$*, depending only on* $\deg(f)$ *such that*

$$\sum_{q \leq x} |W_f(a;q)| \ll \frac{x}{(\log x)^{\delta}} \tag{2}$$

for $x \geq 2$*.*

Problem 1. Find other methods to estimate sums of twisted-multiplicative functions, without modulus.

Problem 2. Obtain lower-bounds for the same quantities (with modulus).

Remark. Estimates for sums of this kind were obtained by Hooley [1964] for Kloosterman sums ($f = X + X^{-1}$) and generalized by Fouvry and Michel [2003] for "generic" rational functions. However, for the bound (2), they obtained an upper bound of size $x(\log\log x)^{c_f}$ for some constant $c_f > 0$. Thus Theorem 1 provides the qualitatively new information that the average of $W_f(a;q)$ goes to zero.

The proof of Theorem 1 involves two fairly different steps:

Step 1. Adapting the method of Hooley and Fouvry–Michel (based on splitting q as sf where s is suitably sifted and f friable), one obtains an analytic bound

$$\sum_{q\leq x}|W(a;q)|\ll\frac{x}{\log x}\exp\Big(\sum_{p\leq x}\frac{1}{p}\Big(\frac{1}{p}\sum_{(a,p)=1}|W(a;p)|\Big)\Big)(\log\log x)^M$$

for any twisted-multiplicative function $W(a;q)$ bounded by some real number $M\geq 0$. This reduces the proof of Theorem 1 to that of understanding the moments

$$\frac{1}{p}\sum_{(a,p)=1}|W_f(a;p)|^2,\qquad \frac{1}{p}\sum_{(a,p)=1}|W_f(a;p)|$$

modulo primes.

Step 2. We prove a dichotomy of independent interest for the *fourth* moment.

Theorem 2. *Assume that $d=\deg(f)\geq 3$. Either*

$$\lim_{p\to+\infty}\frac{1}{p}\sum_{(a,p)=1}|W_f(a;p)|^4=2$$

or there exists $\delta>0$ depending only on d and a set of primes of natural density $\geq\delta$ such that for such primes, we have

$$\frac{1}{p}\sum_{(a,p)=1}|W_f(a;p)|^4\geq 3+O(p^{-1/2}).$$

Using this, it is not too difficult to deduce Theorem 1 by exploiting the fact that if the second moment is equal to 1 (which is almost always true for f indecomposable), then the fourth moment is strictly larger than the second, hence the first moment is strictly smaller (in a quantitative way). For the general indecomposable case, a result of Shao on the average over p of the second moment is also used.

The proof of Theorem 2 depends in essential ways on the theory and formalism of Deligne and Katz for exponential sums over finite fields.

Problem 3. Can one prove special cases of Theorem 2 (say for $f=X^3+X$) using more elementary means? (E.g., not beyond the Chebotarev Density Theorem.)

Remark. In the work of Fouvry and Michel, the generic polynomials are defined (following results of Katz) as the *Morse–Sidon polynomials*, where:

- A polynomial is *Morse* if the derivative f' is squarefree and f separates the roots of f';
- A polynomial is *Sidon* if the values $f(\alpha)$ of f at zeros α of f' form a Sidon set in $\mathbf{C}$: if a, b, c, d are four such numbers and $a+b=c+d$, then $a\in\{c,d\}$.

Our next fairly natural problem is an attempt to show that if f and g are "unrelated" in some sense, then the exponential sums $W_f(a;q)$ and $W_g(a;q)$ are uncorrelated. The limitations about methods to handle sums of twisted-multiplicative functions mean that we cannot compare

$$\sum_{q\leq x}W_f(a;q)\overline{W_g(a;q)}$$

with

$$\sum_{q\leq x} |W_f(a;q)|^2$$

as we would like, but we can prove the following.

Theorem 3. *Suppose that* $\deg(f) \geq 3$, $\deg(g) \geq 3$ *and that* f *and* g *are Sidon–Morse polynomials. Assume that we do not have*

$$g(X) = \alpha f(\beta X + \gamma) + \delta$$

for some $(\alpha, \beta, \gamma, \delta) \in \mathbf{C}^4$.

Fix $a \neq 0$ *in* $\mathbf{Z}$. *There exists* $\delta > 0$, *depending only on* $\deg(f)$ *and* $\deg(g)$, *such that*

$$\sum_{q\leq x} |W_f(a;q)\overline{W_g(a;q)}| \ll \frac{x}{(\log x)^\delta} \tag{3}$$

for $x \geq 2$.

Remark. In the absence of matching lower bounds in (1), we cannot conclude that f and g are uncorrelated.

Finally, this result suggests a question:

Problem 4. Suppose that f and g are polynomials such that $|W_f(a;p)| = |W_g(a,p)|$ for $(a,p) = 1$, either for one large prime p, or for all primes p large enough. What are the relations, if any, between f and g?

Implicitly (and explicitly within the proof), Theorem 3 shows that this condition implies that f and g are "linearly related" if they are both Sidon–Morse of degree ≥ 3. In work in progress, we are attempting to extend this result to a larger class of polynomials.

We note a formal analogy with a problem attributed by Fried to Davenport: if f and g are integral polynomials such that

$$f(\mathbf{F}_p) = g(\mathbf{F}_p)$$

for all p large enough, does it follow that f and g are linearly related?

The link is that one can understand (by methods of Fried in particular) the polynomials f and g with $\mu_{f,p} = \mu_{g,p}$ for large p, where

$$\mu_{f,p} = \frac{1}{p}\sum_{x \bmod p} \delta_{f(x)}, \qquad \mu_{g,p} = \frac{1}{p}\sum_{x \bmod p} \delta_{g(x)}$$

are probability measures on $\mathbf{F}_p$, and this condition is equivalent to $W_f(a;p) = W_g(a;p)$ for all a. Davenport's question asks about relations between f and g if only the support of the measures is remembered, while Problem 4 asks for relations if the *phase* of the discrete Fourier transform of the measures is discarded.

Remark. Most of the results reported here are proved in Kowalski & Soundararajan [2022].

References

[2003] E. Fouvry and P. Michel, *Sommes de modules de sommes d'exponentielles*, Pacific J. Math. 209 (2003), 261–288.

[1964] C. Hooley, *On the distribution of the roots of polynomial congruences*, Mathematika, 11(1964), 39-49.
https://doi.org/10.1112/S0025579300003466

[2022] E. Kowalski and K. Soundararajan, *Exponential sums, twisted multiplicativity, and moments*, in "Analysis at Large", Springer, 2022, 299–332.

A proof of the Erdős primitive set conjecture

Jared Duker Lichtman

A set of integers $A \subset \mathbb{Z}_{>1}$ is *primitive* if no member in A divides another. For example, the integers in a dyadic interval $(x, 2x]$ form a primitive set. Similarly the set of primes $\mathcal{P}$ is primitive, along with the set $\mathcal{P}^{(k)}$ of numbers with exactly k prime factors (with multiplicity), for each $k \geq 1$. Another well-known example is the set of perfect numbers. Since Ancient Greece, a number n is classified as 'perfect,' 'abundant,' or 'deficient,' depending on whether the sum of its proper divisors equals n, is greater than n, or is less than n, respectively.

The study of primitive sets emerged in the 1930s as a generalization of one special problem. A classical theorem of Davenport asserts that the set of abundant numbers has a positive asymptotic density. This was originally proved by sophisticated analytic methods, but Erdős soon found an elementary proof by using primitive abundant numbers. (More precisely, primitive non-deficient numbers). The proof ideas led people to introduce the abstract definition of primitive sets and study them for their own sake. See Hall [9] or Halberstam–Roth [8, §5] for detailed introductions to the subject.

There are a number of interesting and sometimes unexpected theorems about primitive sets. For instance, in 1934 Besicovitch [3] showed that the upper asymptotic density of a primitive set can be arbitrarily close to $1/2$, whereas in 1935 Behrend [2] and Erdős [5] proved the lower asymptotic density is always 0. In fact, Erdős proved the stronger result that

$$f(A) := \sum_{a \in A} \frac{1}{a \log a} \ < \ \infty,$$

uniformly over all primitive sets A. Later in 1988 Erdős famously asked if the maximum is attained by the primes $\mathcal{P}$.

Conjecture 1 (Erdős primitive set conjecture)**.** *For any primitive set A, $f(A) \leq f(\mathcal{P})$.*

The prime sum is $f(\mathcal{P}) = \sum_p 1/(p \log p) = 1.6366\cdots$ after computations of Cohen [4]. In 1993, Erdős and Zhang [7] proved the bound $f(A) < 1.84$ for all primitive A. Recently in 2019, Lichtman and Pomerance [11] improved the bound to $f(A) < e^\gamma = 1.781\cdots$, where γ is the Euler-Mascheroni constant. Note the tail of the series for $f(\mathcal{P})$ converges quite slowly $O(1/\log x)$, and moreover there are

sets $A \subset [x, \infty)$ for which $f(A) \sim 1$ as $x \to \infty$ (in this connection see Conjecture 2 below). As such, Conjecture 1 is not susceptible to direct attack by computing partial sums up to x.

We note a natural analogue of Conjecture 1 for the translated sum $f(A, h) = \sum_{a \in A} 1/a(\log a + h)$ is false. Namely, there are primitive A for which $f(A, h) > f(\mathcal{P}, h)$ once $h \geq 1.04$ [10]. This suggests that the original conjecture (when $h = 0$), if true, is only 'barely' so.

Nevertheless we answer Conjecture 1 in the affirmative.

Theorem 1 (L., 2022)**.** *For any primitive set A, we have $f(A) \leq f(\mathcal{P})$.*

Another question related to Conjecture 1, in 1968 Erdős, Sárközy, and Szemerédi posed the following [6, eq. (11)].

Conjecture 2 (Erdős–Sárközy–Szemerédi)**.** *We have*

$$\lim_{x \to \infty} \sup_{\substack{A \subset [x, \infty) \\ A \text{ primitive}}} f(A) \ \leq \ 1.$$

The methods in this paper also enable the following initial progress towards Conjecture 2.

Theorem 2 (L., 2022)**.** *We have*

$$\lim_{x \to \infty} \sup_{\substack{A \subset [x, \infty) \\ A \text{ primitive}}} f(A) \ \leq \ e^{\gamma} \frac{\pi}{4} \approx 1.399.$$

References

[1] W. D. Banks, G. Martin, *Optimal primitive sets with restricted primes*, Integers **13** (2013),#A69, 10pp.

[2] F. Behrend, *On sequences of numbers not divisible by one another*, J.London Math. Soc. **10**(1935), 42–44.

[3] A. S. Besicovitch, *On the density of certain sequences of integers*, Math. Ann. **110** (1934), 336–341.

[4] H. Cohen, *High precision computation of Hardy-Littlewood constants*, preprint `https://www.math.u-bordeaux.fr/~hecohen/` .

[5] P. Erdős, *Note on sequences of integers no one of which is divisible by any other*, J. London Math. Soc. **10** (1935), 126–128.

[6] P. Erdős, A. Sárközy, E. Szemerédi, *On divisibility properties of sequences of integers*, Colloq. Math. Soc. János Bolyai, **2** (1968), 35–49.

[7] P. Erdős and Z. Zhang, *Upper bound of $\sum 1/(a_i \log a_i)$ for primitive sequences*, Proc. Amer. Math. Soc. **117** (1993), 891–895.

[8] H. Halberstam, K. F. Roth, *Sequences*, Oxford University Press (1966)

[9] R. R. Hall, *Sets of multiples*, Cambridge Tracts in Mathematics, **118**, Cambridge University Press (1996)

[10] J. D. Lichtman, *Translated sums of primitive sets*, Comptes Rendus. Mathématique, to appear.

[11] J. D. Lichtman, C. Pomerance, *The Erdős conjecture for primitive sets*, Proc. Amer. Math. Soc. Ser. B **6** (2019), 1–14.

Large order Dirichlet characters and an analogue of a conjecture of Vinogradov

Alexander P. Mangerel

Let q be a large prime, and let n_q denote the least quadratic non-residue modulo q. It is a classical problem to obtain upper bounds for n_q as a function of q. Viewing the event $\left(\frac{n}{q}\right) = \pm 1$ as an outcome of a fair coin toss, probabilistic heuristics suggest that $n_q \ll_\epsilon (\log q)^{1+\epsilon}$, a suggestion bolstered by a result of Ankeny [1], conditional on the Generalized Riemann Hypothesis (GRH), that $n_q \ll (\log q)^2$. More modestly, a still open conjecture of I.M. Vinogradov posits that $n_q \ll_\epsilon q^\epsilon$ for any $\epsilon > 0$, a claim that is known to hold for "almost all" q (in a precise sense) as a consequence of the large sieve and zero-density estimates for Dirichlet L-functions. In this connection, the best unconditional result $n_q \ll_\epsilon q^{\frac{1}{4\sqrt{e}}+\epsilon}$, due to Burgess [2], makes crucial use of bounds for short character sums

$$\sum_{n \leq x} \left(\frac{n}{q}\right), \quad x > q^{1/4+\epsilon}.$$

Improvements in the range of x, e.g., to any $x > q^\epsilon$, in such an estimate would immediately resolve Vinogradov's conjecture in the affirmative.

By analogy, given χ a primitive character modulo a prime q, define n_χ to be the least n for which $\chi(n) \neq 0, 1$. It is of interest to determine sufficient conditions on χ and q, *independent of* the distribution of zeros of corresponding L-functions, that guarantee that, in analogy to Vinogradov's conjecture, $n_\chi \ll_\epsilon q^\epsilon$ for any $\epsilon > 0$. Going further, it is of interest to show, for suitable χ and q, significant variation in the values of $\chi(n)$ for $n \leq q^\epsilon$, and for $\chi(p)$ when $p \leq q^\epsilon$ is prime. One would also hope to improve the range of Burgess' estimate in such cases.

In this talk, based on the article [4], we discuss such questions in the case that χ has *large order*, i.e., for minimal d such that χ^d is principal, $d \to \infty$ as $q \to \infty$. Our results show that for any $\delta, \epsilon > 0$ there is a (quantitative) $d_0 = d_0(\delta, \epsilon)$ such that whenever $d \geq d_0$ and $x > q^\delta$:

(1) the least n with $\chi(n) \neq 0, 1$ satisfies $n_\chi \leq q^\delta$, a result proven by K.K. Norton [5], but for which we give an alternative, elementary proof;
(2) if d is squarefree then the level sets $\{n \leq q^\delta : \chi(n) = \alpha\}$, where $\alpha^d = 1$, are *sparse*, i.e., of size $\leq \epsilon x$, and thus no clustering of fixed values of $\chi(n)$ occurs even in the short segment $[1, q^\delta]$;
(3) the set of prime values $\chi(p) \neq 1$ is *substantial* in the sense that the sum $\sum_{\substack{p \leq q^\delta \\ \chi(p) \neq 0,1}} p^{-1}$ is $\geq 1/\epsilon$; and
(4) if the least prime factor of d is $> 1/\epsilon$ then for *all but* $O(\epsilon d)$ choices of exponents $1 \leq \ell \leq d$ we may go beyond the Burgess range and obtain

$$|S_{\chi^\ell}(x)| := \left|\sum_{n\le x} \chi^\ell(n)\right| \le \epsilon x. \tag{1}$$

The last of these items is perhaps the most interesting, for at least two reasons.

First, though it is the consequence of an averaging result over the family $\{\chi^\ell\}_{\ell=1}^d$, this family could be growing arbitrarily slowly in size (as we make no assumptions on how quickly d grows with q). Moreover, this family is structured, whereas e.g., zero density estimates do not provide specific structural information (outside of information about L-functions) on the characters giving rise to small partial sums.

Second, the proof invokes results from additive combinatorics, in particular inverse sumset results, to understand the structure of the set $\Xi_d(\epsilon)$ of exponents ℓ for which (1) fails to hold. For such "bad" ℓ there is a choice of real number $t_\ell \in [-1/\epsilon, 1/\epsilon]$ such that the prime sum

$$\sum_{p\le x} \frac{1-\mathrm{Re}(\chi^\ell(p)p^{-it_\ell})}{p} = O_\epsilon(1).$$

If $t_\ell = 0$ for all ℓ then sieve-theoretic considerations of a different kind allow us to conversely conclude that the corresponding prime sums are still large, and hence equivalently that $|S_{\chi^\ell}(x)|$ is still small as a function of ϵ even when $\ell \in \Xi_d(\epsilon)$. To deduce that, indeed, $t_\ell = 0$ may be taken here, the key idea, arising from the pretentious theory of multiplicative functions pioneered by Granville and Soundararajan (as in e.g., [3]), is that, roughly speaking, the map $\ell \mapsto t_\ell$ is an *approximate homomorphism* on $\Xi_d(\epsilon)$. This property may be extended to all of $\mathbb{Z}/d\mathbb{Z}$ by covering the latter cyclic group efficiently (i.e., with m not too large) by sumsets

$$m\Xi_d(\epsilon) = \{\ell_1 + \cdots + \ell_m : \ell_j \in \Xi_d(\epsilon)\}$$

(which can be done when d has only large prime factors). As approximate homomorphisms on abelian groups are uniformly approximable by *genuine* homomorphisms (see e.g., [6]), and as the only homomorphism $\mathbb{Z}/d\mathbb{Z} \to \mathbb{R}$ is identically zero, we conclude that t_ℓ is (sufficiently well-approximated by) 0 for *each* ℓ.

References

[1] N.C. Ankeny, *The least quadratic non-residue*, Ann. Math. **55(1)** (1952), 65–72

[2] D.A. Burgess, *On character sums and primitive roots*, Proc. Lond. Math. Soc. **12(3)** (1962), 179–192.

[3] A. Granville, and K. Soundararajan, *Large character sums: pretentious characters and the Pólya-Vinogradov inequality*, J. Amer. Math. Soc. **20(2)** (2007), 357–384.

[4] A.P. Mangerel, *Large sums of high order characters*, arXiv: 2207.14377 [math.NT, math.CO]

[5] K.K. Norton, *Numbers with small prime factors and the least kth power non-residue*, Memoirs of the AMS **106** (1971)

[6] I.Z. Ruzsa, *On the concentration of additive functions*, Acta Math. Acad. Sci. Hung. **36** (1980), 215–232

Products of primes in arithmetic progressions

Kaisa Matomäki
(joint work with J. Teräväinen)

For $k, q \in \mathbb{N}$ and a real number $x \geq 2$, write

$$E_k(x) = \{a \in \mathbb{Z}_q^\times : a \equiv p_1 \cdots p_k \pmod q \text{ for some primes } p_1, \ldots, p_k \leq x\},$$

where $\mathbb{Z}_q^\times$ is the set of reduced residue classes $\pmod q$. We study $E_k(x)$ for $k \in \{2, 3\}$.

Erdős conjectured (see [1]) that $E_2(q) = \mathbb{Z}_q^\times$ for all large enough primes q. This can be seen as a multiplicative analogue of the Goldbach conjecture and remains open even under the Generalized Riemann Hypothesis. In our on-going work we establish the ternary variant of Erdős' conjecture:

Theorem 1. (1) *Let $q \in \mathbb{N}$ be cube-free and sufficiently large. Then*

$$E_3(q) = \mathbb{Z}_q^\times.$$

(2) *Let $\varepsilon > 0$ and let $q \in \mathbb{N}$ be sufficiently large in terms of ε. Then*

$$E_3(q^{1+\varepsilon}) = \mathbb{Z}_q^\times.$$

Previously it was shown independently by Szabó [3] and Zhao [4] that $E_6(q) = \mathbb{Z}_q^\times$ (Szabó [3] needed to assume that q is prime). On the other hand, several authors have considered the least x for which $E_3(x) = \mathbb{Z}_q^\times$. The best result before Theorem 1 was that $x = q^{6/5+\varepsilon}$ works for all sufficiently large q due to Szabó [3].

We also note that Klurman, Mangerel and Teräväinen [2] proved that, once $\delta > 0$ is sufficiently small, $E_3(q) = \mathbb{Z}_q^\times$ for all large enough q which are q^δ-smooth. The method in [2] depends on the quality of the zero-free regions available for Dirichlet L-functions $\pmod q$, and hence it does not work for arbitrary q.

We also consider another approximation toward the conjecture of Erdős, that is the problem of lower bounding the density of $E_2(q)$ inside $\mathbb{Z}_q^\times$.

Theorem 2. *Let $\varepsilon > 0$, and let $q \in \mathbb{N}$ be sufficiently large in terms of ε. Then*

$$|E_2(q)| \geq \left(\frac{29}{44} - \varepsilon\right)\varphi(q).$$

Here $29/44 \approx 0.659$ whereas the previous record was due to Szabó [3] with $3/8 = 0.375$ in place of $29/44$ and an additional condition that q is cube-free.

In order to prove Theorem 1(i), we let $a \in \mathbb{Z}_q^\times$ and aim to prove that $a \in E_3(q)$. The starting point is the identity

$$(1) \qquad \sum_{\substack{a = p_1p_2p_3 \\ p_j \leq q}} \log p_1 \log p_2 \log p_3 = \frac{1}{\varphi(q)} \sum_{\chi \pmod q} \left(\sum_{p \leq q} \overline{\chi}(p) \log p\right)^3 \chi(a).$$

By the prime number theorem, principal characters contribute here $(1+o(1))\frac{q^3}{\varphi(q)}$. If we knew that, for every non-principal χ, we have

$$\sum_{p\le q}\overline{\chi}(p)\log p \ll \frac{q}{(\log q)^{10}}, \tag{2}$$

say, the claim would follow quickly using also orthogonality of characters. However, unfortunately, there are no chances to establish (2) — note that the sum is only over $p \le q$ with q the conductor of the character.

We overcome this obstacle by establishing a dense model theorem for character sums over primes in the spirit of the transference principle in additive number theory. More precisely, we show that there exists $g\colon \mathbb{Z}_q^\times \to [0, \frac{8}{3}+\varepsilon]$ such that, for every $\chi \pmod q$,

$$\left|\sum_{p\le q}\overline{\chi}(p)\log p - \frac{q}{\varphi(q)}\sum_{a\in\mathbb{Z}_q^\times} g(a)\overline{\chi}(a)\right| = o(q).$$

Combining this with (1), the orthogonality of characters and a Halász-Montgomery type inequality, we can show that

$$\sum_{\substack{a=p_1p_2p_3\\ p_j\le q}}\log p_1\log p_2\log p_3 = \frac{q^3}{\varphi(q)^3}\sum_{\substack{a=a_1a_2a_3\\ a_j\in\mathbb{Z}_q^\times}} g(a_1)g(a_2)g(a_3) + o\left(\frac{q^3}{\varphi(q)}\right).$$

Writing $A = \{a\in\mathbb{Z}_q^\times : |g(a)| \ge \varepsilon\varphi(q)\}$, we obtain that $a\in E_3(q)$ if $\mathbf{1}_A * \mathbf{1}_A * \mathbf{1}_A \gg \varphi(q)^2$. Furthermore, by construction, we have

$$|A| \ge \left(\frac{3}{8} - 3\varepsilon\right)\varphi(q).$$

Using (popular) Kneser's theorem, we can show that $E_3(q) = \mathbb{Z}_q^\times$ unless A is essentially stuck in $k+1$ cosets of a subgroup $H \le \mathbb{Z}_q^\times$ of index $3k+2$, for some $k\in\{0,1,2\}$, and $A\cdot A$ is essentially the union of $2k+1$ cosets. The dense model g is defined in such a way that this means that also the primes $p\le q$ are essentially stuck in these cosets. To deal with such cases, we apply the dense model theorem in somewhat different ways. In particular we have to be very careful in case there exists a quadratic character $\psi \pmod q$ such that $\psi(p) = -1$ for almost all primes $p\le q$.

References

[1] P. Erdős, A. M. Odlyzko, and A. Sárközy, *On the residues of products of prime numbers*, Period. Math. Hungar. **18** (1987), 229–239.

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

[3] B. Szabó, *On the existence of products of primes in arithmetic progressions*, **arXiv:2208.05762**.

[4] L. Zhao, *On products of primes and almost primes in arithmetic progressions*, Acta Arith. **204** (2022), 253–267.

Half-isolated zeros and zero density estimates

James Maynard
(joint work with Roger Heath-Brown, Kyle Pratt)

Let $N(\sigma, T)$ denote the number of zeros of $\zeta(s)$ in a box:

$$N(\sigma, T) := \#\{\rho : \zeta(\rho) = 1, \Re(\rho) \geq \sigma, 0 \leq \Im(\rho) \leq T\}.$$

Of course it is believed that $N(\sigma, T) = 0$ whenever $\sigma > 1/2$ by the Riemann Hypothesis, but one can look for weaker bounds which still have implications for the distribution of primes. Of particular importance is the following conjecture.

Conjecture 1 (Density Hypothesis)**.** *For any $\sigma, T > 0$ we have*

$$N(\sigma, T) < T^{2-2\sigma+o(1)}.$$

For many applications, the Density Hypothesis would give results which are comparably strong to the Riemann Hypothesis. Unconditionally Huxley [1] showed that $N(\sigma, T) \leq T^{(12-12\sigma)/5+o(1)}$, which gives essentially the strongest known bounds for asymptotics for primes in short intervals. Unfortunately applications are limited by our bounds when $\sigma = 3/4$, and the bounds for $\sigma \leq 3/4$ have seen essentially no improvement for 80 years following Ingham's work [2].

Our main result is to prove the Density Hypothesis under the assumption of some constraints on the possible patterns of zeros.

Theorem 1. *Assume the non-trivial zeros of $\zeta(s)$ lie on finitely many vertical lines. Then the Density Hypothesis is true.*

Corollary 2. *Assume the non-trivial zeros of $\zeta(s)$ lie on finitely many vertical lines. Then for any $\epsilon > 0$ we have:*

(1) *(Primes in short intervals) For $y \in [x^{1/2+\epsilon}, x]$ we have*

$$\#\{p \in [x, x+y]\} = (1+o(1))\frac{y}{\log x}.$$

(2) *(Primes in almost all short intervals) For $y \in [X^{\epsilon}, X]$ we have*

$$\#\{p \in [x, x+y]\} = (1+o(1))\frac{y}{\log x}$$

for all $x \in [X, 2X]$ outside of a set of measure $o(X)$.

The assumption of finitely many vertical lines could be weakened significantly, but our method requires some assumption on horizontal rigidity of zeros.

A key concept in our result is 'half-isolated zeros'. On a given vertical line, we call a zero $\rho = \beta + i\gamma$ of $\zeta(s)$ 'half-isolated' if there are no other zeros within $(\log|\gamma|)^3$ of the zero on the same vertical line with smaller imaginary part. We see that for any line to the right of the critical line, zeros must appear in 'clumps' with a half-isolated zero at the bottom of each clump. This is partly inspired by previous work of Heath-Brown, Ramachandra-Balusubramanian and Conrey-Iwaniec on 'isolated' zeros.

Our key technical proposition is that half-isolated zeros have short zero detecting polynomials.

Proposition 3. *There exists an absolute constant $C \geq 1$ and a fixed nonnegative smooth function w_0 supported in $[1/2, 2]$ such that the following holds.*

If $\rho_0 = \beta_0 + i\gamma_0$ is a half-isolated zero with $\gamma_0 \in [T, 2T]$, then there exists a real $Y \in [T^{(\log\log T)^3/\log T}, T^{3/\log\log T}]$ such that

$$\Big|\sum_n \frac{\Lambda(n)}{n^{\rho_0}} w_0(n/Y)\Big| \geq (\log T)^{-C}.$$

By combining this proposition with more traditional zero-detecting technology, we are able to prove Theorem 1. As a proof of principle, we see that by estimating moments Proposition 3 shows that there are few half-isolated zeros, and so few 'clumps' on any vertical line. Therefore there are few zeros on these lines unless the clumps typically consist of many zeros, in which case the zeros are very concentrated on a few short vertical segments, and we have some useful information that we can hope to exploit.

In turn, the key to proving Proposition 3 is a Turán power sum type lemma. A simplified version of it is the following:

Lemma 4 (Simple case of power sum inequality)**.** *Let $\theta_1 \leq \cdots \leq \theta_R$ be real numbers. There exists an absolute constant $B_0 \geq 1$ such that the following is true. For any $A > 0$, there exists a real $t \in [A, 2A]$ such that*

$$\Big|\sum_{r=1}^{R} \exp(it\theta_r)\Big| \geq (B_0 R)^{-99}.$$

Traditional power-sum methods would yield a lower bound which is exponentially small in R, but for our application it is vital that we have a polynomial lower bound.

The key barrier to making these results unconditional appears to be showing that certain configurations which we call 'bows' cannot appear frequently. A 'bow' of zeros is a set of zeros where the imaginary parts lie in an arithmetic progression with common difference $\approx \frac{1}{\log T}$, and where the real parts of the zeros vary smoothly between $\frac{1}{2}$ and some $\sigma > \frac{1}{2}$ and then back to $\frac{1}{2}$ again.

References

[1] M. N. Huxley. On the difference between consecutive primes. *Invent. Math.*, 15:164–170, 1972.

[2] A. E. Ingham. On the estimation of $N(\sigma, T)$. *Quart. J. Math. Oxford Ser.*, 11:291–292, 1940.

On the Gaussian moat problem

Jori Merikoski

(joint work with James Maynard)

The Gaussian moat problem (posed by Basil Gordon in 1962) asks if it is possible to walk to infinity in the complex plane using Gaussian primes as stepping stones with step size bounded by an absolute constant. While a heuristic suggests that

the answer is no, we may ask what happens if we let the step size increase with the size of the Gaussian primes. That is, what is the infimum of exponents $\theta > 0$ such that there is a sequence of Gaussian primes $z_j \to \infty$ satisfying $|z_{j+1} - z_j| \ll_\theta |z_j|^\theta$?

A simple argument shows that $\theta \le \theta'$, where θ' is the best known exponent for the problem of Gaussian primes in small discs. By the works of Coleman, Baker, Harman, Kumchev, and Lewis [1, 3, 5, 8] it is known that for all $z \in \mathbb{C}$ there is a Gaussian prime p with

$$|p - z| \ll |z|^{\theta'} \quad \text{for} \quad \theta' = 0.528.$$

As mentioned, this implies $\theta \le 0.528$ for the exponent in the Gaussian moat problem. Even conditional on GRH the best exponent to date is

$$\theta \le \theta' \le 1/2 + o(1).$$

Our main result breaks past this square-root barrier unconditionally for the Gaussian moat problem.

Theorem 1. *(Maynard, Merikoski) We have $\theta \le 1/2 - 1/100$. Assuming GRH we have $\theta \le 1/3 + o(1)$.*

This result is still work-in-progress and we will likely improve the saving $1/100$ once we optimize our argument. We also prove analogous results for the Gaussian moat problem with smooth numbers or E_3 numbers (which have exactly three prime factors).

Theorem 2. *(Maynard, Merikoski) For the Gaussian moat problem with steps restricted to $|z|^\varepsilon$-smooth Gaussian numbers or E_3-numbers we can take $\theta \le 1/3 + o(1)$ unconditionally.*

Let $B(c, S)$ denote the the disc $\{|z - c| \le S\}$ of radius S centered at c and let $A(R)$ denote the annulus $\{R \le |z| \le 2R\}$. By a dyadic pigeon-hole argument Theorem 1 is a consequence of the following result on primes in almost all discs restricted to a sparse collection of discs.

Theorem 3. *(Maynard, Merikoski) Denote $S = R^{1/2-1/100}$. Let $\mathcal{C} \subseteq A(R) \cap \mathbb{Z}[i]$ be an S-separated set (that is, for all distinct $c, c' \in \mathcal{C}$ we have $|c - c'| \ge S$). Suppose that $|\mathcal{C}| \ge RS$. Then for all but $\ll |\mathcal{C}|/(\log R)^{100}$ of the points $c \in \mathcal{C}$ we have*

$$\sum_{p \in B(c,S)} 1 \gg \frac{S^2}{\log R},$$

where the sum runs over Gaussian primes p.

The above theorem states that for almost all $c \in \mathcal{C}$ we have a correct order lower bound for the number Gaussian primes in the disc $B(c, S)$. To prove this result we first use Harman's sieve method [4] to establish a combinatorial decomposition for primes as Type I and Type II sums. The Type II sums are handled by a Cauchy-Schwarz argument, which reduces the task to two parts, a certain lattice point estimate and the distribution of primes in almost all discs at a smaller scale. The lattice point problem is solved by using geometry of numbers similarly as in

the recent work of Heath-Brown [6]. The distribution of primes in almost all discs is controlled by the work of Coleman [2], which gives a generalization of Huxley's work [7] to the Gaussian integers.

References

[1] M. D. Coleman. *The distribution of points at which binary quadratic forms are prime*, Proc. London Math. Soc. (3) **61** (1990), 433–456.

[2] M. D. Coleman. *Distribution of points at which norm-forms are prime*, J. Number Theory **41** (1992), no. 3, 359–378.

[3] M. D. Coleman. *Relative norms of prime ideals in small regions*, Mathematika **43** (1996), 40–62.

[4] G. Harman. *Prime-detecting sieves*, volume 33 of London Mathematical Society Monographs Series. Princeton University Press, Princeton, NJ, 2007.

[5] G. Harman, A. Kumchev, and P. A. Lewis. *The distribution of prime ideals of imaginary quadratic fields*, Trans. Amer. Math. Soc. **356** (2003), 599–620.

[6] D.R. Heath-Brown, *The differences between consecutive smooth numbers*, Acta Arithmetica, **184** (2018), 267–285.

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

[8] P. Lewis. *Finding Gaussian primes by analytic number theory sieve methods*, Ph.D. thesis, Cardiff University, 2002.

Problem Session

Hugh Montgomery

1. (Proposed by Hugh Montgomery) For an odd prime p, let $n_2(p)$ denote the least positive quadratic nonresidue of p. In 1949, V. R. Friedlander and H. Salié independently showed that $n_2(p) = \Omega(\log p)$. Turán also observed that this follows easily from Linnik's theorem concerning the least prime in an arithmetic progression. However, this argument is inefficient since it locates a prime in one particular arithmetic progression modulo a product of many small primes, when actually many other arithmetic progressions would serve equally well. By averaging over such residue classes, in 1971 Montgomery showed that GRH implies that $n_2(p) = \Omega\big((\log p)\log\log p\big)$. The problem now proposed is to show this, or something close to this, unconditionally. It seems that the result $n_2(p) = \Omega\big((\log p)\log\log\log p\big)$ due to Graham and Ringrose is the best unconditional one known.

2. (Proposed by Hugh Montgomery) In 1970, Gallagher showed that if λ_n are distinct real numbers, $\sum_n |a_n| < \infty$, $\varepsilon > 0$, and $\delta T \le 1 - \varepsilon$, then

$$\int_{-T}^{T} \left| \sum_n a_n e(\lambda_n t) \right|^2 dt \ll_\varepsilon \delta^{-2} \int_{-\infty}^{\infty} \left| \sum_{\substack{n \\ |\lambda_n - x| < \delta/2}} a_n \right|^2 dx.$$

It is believed that in most situations this upper bound is of the correct order of magnitude. It would be useful to have a corresponding lower bound. Gallagher

achieved the above by appealing to Plancherel's identity to show that

$$\int_{-\infty}^{\infty} \Big| \sum_n a_n e(\lambda_n t) \Big|^2 \Big(\frac{\sin \pi\delta t}{\pi\delta t} \Big)^2 = \delta^{-2} \int_{-\infty}^{\infty} \Big| \sum_{\substack{n \\ |\lambda_n - x| < \delta/2}} a_n \Big|^2 dx.$$

One might try replacing the kernel on the left hand side above by

$$\frac{(\sin \pi\delta t)^2}{(\pi\delta t)^2(1-\delta t)(1+\delta t)},$$

which minorizes the characteristic function of the interval $[-1/\delta, 1/\delta]$, but on the Fourier Transform side this gives rise to a bilinear form whose eigenvalues will need to be determined. Alternatively, one might construct a minorant that is the difference of two squares, and apply Phancherel's identity twice.

3. (proposed by Roger Heath-Brown) Consider the following triple of problems:

A. Express every large $N \equiv 2 \pmod 4$ as $N = a + b$ where $p|a \implies p \equiv 1 \pmod 4$, $p|b \implies p \equiv 1 \pmod 4$.

B. Express every large $N \equiv 0 \pmod 4$ as $N = a + b$ where $p|a \implies p \equiv 3 \pmod 4$, $p|b \implies p \equiv 1 \pmod 4$.

C. Express every large $N \equiv 0 \pmod 2$ as $N = a + b$ where $p|a \implies p \equiv 3 \pmod 4$, $p|b \implies p \equiv 3 \pmod 4$.

4. (proposed by Bob Vaughan) Let $d \geq 1$, $m \geq 0$ and $n = d+m$. Further let ψ be a positive valued function defined on $\mathbb{N}$ such that $\psi(h) \to 0$ as $h \to \infty$. Suppose that $\mathbf{f} : \mathbb{R}^d \to \mathbb{R}^m$. For notational convenience put $\alpha_{d+j} = f_j(\alpha_1, \ldots, \alpha_d)$. Let $\mathcal{A}(h)$ denote the set of $(\alpha_1, \ldots, \alpha_d)$ in $\mathbb{R}^d$ such that there are $q_1, ..., q_n$ with $q_j \leq h$ for which

$$\|q_j \alpha_j\| \leq \psi(h)$$

and let $\mathcal{A}^*$ denote the set of $(\alpha_1, \ldots, \alpha_d)$ in $\mathbb{R}^d$ which are contained in infinitely many of the $\mathcal{A}(h)$. Is it true that, with suitable "non-degeneracy" conditions on the f that there is a 0 - 1 law, namely $\mathcal{A}^*$ contains almost no, or almost all $(\alpha_1, \ldots, \alpha_d)$ in $\mathbb{R}^d$ according as

$$\sum_{h=1}^{\infty} h^{n-1} \psi(h)$$

converges or diverges.

The case $n = 1$ is Khinchin's theorem. There is a considerable body of work on the metrical theory of simultaneous diophantine approximation. The question here is an attempt to move away from the restriction that the denominators in the approximations a_j/q_j to a given $\boldsymbol{\alpha}$ have to be identical.

An assertion which is likely to be essentially equivalent is as follows. Given a rational point $\boldsymbol{\rho} = (a_1/q_1, \ldots, a_n/q_n)$ in $\mathbb{Q}^n$ define the height

$$H(\boldsymbol{\rho}) = \max(|a_1|, \ldots |a_n|, |q_1|, \ldots, |q_n|).$$

Then take instead $\mathcal{A}(h) = \{\boldsymbol{\alpha} : |\boldsymbol{\alpha} - \boldsymbol{\rho}| < \psi(h)/h, H(\boldsymbol{\rho}) \leq h\}$ and ask if the same conclusion holds.

5. (proposed by Emmanuel Kowalski) We want $\gamma > 0$ and $\delta > 0$ such that if $I \subseteq \mathbb{F}_p^\times$ is an interval of size $|I| \geq p^{1/2-\gamma}$, then

$$\frac{1}{p}\sum_{a\,(p)}\left|\frac{1}{\sqrt{p}}\sum_{x\in I} e\Big(\frac{ax+\overline{x}}{p}\Big)\right|^4 \ll \Big(\frac{|I|}{p}\Big)^{1+\delta}.$$

This would have the following application: It would yield the equidistribution of Kloosterman paths for $\mathrm{Kl}_2(a;p)$ instead of $\mathrm{Kl}_2(a,b;p)$.

6. (proposed by Brian Conrey) Michael Rubinstein has called attention to the following issue: In 2018, Keating, Rodgers, Roditty-Gershon, Rudnick considered the k-fold divisor function in short intervals, which led them to consider

$$\int_{U(N)} \det(I-xU)^k \det(I-U^*)^k\, dU = \sum_{m=0}^{kN} I_k(m,N)x^m.$$

Subsequently, A. Medjedovic showed that the above is

$$= \frac{c_{N,k}}{(1-x)^{k^2}} \underbrace{\det\left(\frac{1-x^{N+i+j-1}}{N+i+j-1}\right)_{i,j=1}^{k}}_{=:G_{k,N}(x)}$$

with

$$c_{N,k} = \prod_{j=1}^{k} \frac{(N+k-j-1)!}{(j-1)!^2\,(N+j-1)!}.$$

Rubinstein has conducted experiments that suggest that $F := xG'/G$ seems to satisfy the following differential equation:

$$\begin{aligned} x^2(x-1)^2F''' + x(5x-1)(x-1)F'' + 6x(x-1)^2(F')^2 + 4(x-1)(x+1)FF' \\ + ((-4k^2-4Nk-N^2+4)x^2 + (4k^2+4Nk+2N^2-2)x - N^2)F' \\ + 2F^2 + (-2k^2-2Nk)F = 0 \end{aligned}$$

The problem is to prove that F does indeed satisfy this differential equation, and why. The differential equation is an example of a type of ordinary differential equation known as a Painlevé equation. The further question is why such a differetial equation should arise in this conext.

7. (proposed by Julia Brandes) In Brandes, Parsell, Poulias, Shakan, Vaughan, Mathematische Annalen 379(2021), 347–376, arXiv:2001.05629 [math.NT] it is shown that

$$\sup_{\alpha_1}\Big|\sum_{x\leq X} e\big(\alpha_1(x^k+x)+\alpha_2 x^k\big)\Big| \gg X^{3/4}$$

for almost all α_2. Also in Brandes and Shparlinski, arXiv:2012.08877 [math.NT] it is shown that

$$\sup_{\alpha_1}\Big|\sum_{x\leq X} e\big(\alpha_1(f(x)+x)+\alpha_2 f(x)\big)\Big| \gg X^{3/4}$$

for almost all α_2. The challenge now is to find f_1, f_2 of degree ≥ 2 such that

$$\sup_{\alpha_1} \Big| \sum_{x \leq X} e\big(\alpha_1(f_1(x) + f_2(x)) + \alpha_2 f_1(x)\big) \Big| \gg X^{1/2+\tau}$$

for almost all α_2, for some $\tau > 0$.

8. (proposed by Trevor Wooley) Apéry showed that $\zeta(3) \notin \mathbb{Q}$. Show that $\zeta(3) \notin \mathbb{Q}\big(\sqrt{2}\big)$. Alternatively find a nonsquare $d > 0$ such that $\zeta(3) \notin \mathbb{Q}\big(\sqrt{d}\big)$. Finally, show that

$$\sum_{n=0}^{\infty} \big(n + \sqrt{2}\big)^{-2} \notin \mathbb{Q}.$$

9. (proposed by Trevor Wooley) Suppose that $f(x) \in \mathbb{Z}[x]$ has degree $d \geq 2$. We say that f is 2-*superirreducible* if $f(g(x))$ is irreducible whenever the degree of $g(x) \in \mathbb{Z}[x]$ is ≤ 2. In 1967, Schinzel showed that if $\deg f = d \geq 3$, then there is a polynomial g of degree $d-1$ such that $f(g(x))$ is reducible. Question: Does there exist a polynomial of degree 5 that is 2-superirreducible? (This is a question of J. Bober, D. Fretwell, G. Kopp, L. Du and T. Wooley).

10. (proposed by Trevor Wooley) If G is a finite abelian group, then there exist integers n and d such that $G \cong \big\{z^d : z \in (\mathbb{Z}/n\mathbb{Z})^\times\big\}$. Obtain sharp upper bounds for the parameters n and d in terms of $|G|$.

11. (proposed by Jori Merikowski) Do there exist polynomials

$$f, g \in \mathbb{Z}[x_1, \ldots, x_4, x_5]$$

with f homogeneous of degree 3 and g homogeneous of degree 2 such that

$$f^2 + g^3 = N(x_1, \ldots, x_5) = N_{K/\mathbb{Q}}(x_1\omega_1 + \cdots + x_5\omega_5) \ ?$$

12. (proposed by Ben Green) Cover the integers $\{1, 2, \ldots, N\}$ by residue classes $a_p \pmod p$, one residue class per prime.

(1) Can you cover each number twice (meaning at least 2 times each), using only primes $p \leq N$? (This was asked by Erdős.)

(2) Can you do it with $\sum_p 1/p \leq K$? (This has been considered by Erdős–Ruzsa and by Hildebrand.)

13. (proposed by Sarah Peluse and Robert Lemke Oliver) In 2000, Daniel Shiu showed that if $(a, q) = 1$, then there exist arbitrarily long strings of consecutive primes $\equiv a \pmod q$. Could something similar be shown for more general patterns of residue classes, say residues 1, 2, 1, 2, 1, 2, ... (mod 5)?

14. (proposed by Simon Myerson) Can one develop something like the circle method, or Weyl sums, or Poisson summation for quaternions?

Statistical properties of the character table of the symmetric group

Sarah Peluse
(joint work with Kannan Soundararajan)

It is a standard fact that, for all natural numbers n, the irreducible characters of S_n take only integer values. In 2017, Miller [3] computed the character tables of S_n for all $n \leq 38$ and investigated the statistical properties of these integers as n grew. He made the following observations:

(1) the density of even entries seemed to be tending to 1,
(2) the density of entries divisible by 3 and the density of entries divisible by 5 also seemed to be increasing as n grew,
(3) about half of the nonzero entries were positive,
(4) and the density of zeros in the character table seemed to be decreasing as n grew, but not very quickly.

Based on this first observation, Miller conjectured [3, 4] that, as $n \to \infty$, almost every entry in the character table of S_n is even. Following partial progress due to McKay [2], Gluck [1], and Morotti [6], I proved this conjecture:

Theorem 1 (P., 2020 [7]). *There exists a $\delta > 0$ such that the proportion of odd entries in the character table of S_n goes to 0 as $n \to \infty$.*

Based on the second piece of evidence mentioned above, Miller also conjectured, more generally, that for any fixed prime p, almost every entry of the character table of S_n is a multiple of p as n goes to infinity. Soundararajan and I proved this conjecture [8] with a bound that is uniform in the prime p:

Theorem 2 (P.–Soundararajan, 2022 [8]). *Let n be large and p be a prime with $p \leq \log n/(\log\log n)^2$. The proportion of entries in the character table of S_n that are not divisible by p is at most*

$$O\left(\frac{1}{n^{1/12p}}\right).$$

Later Miller conjectured [5], even more generally, that as $n \to \infty$, almost all entries in the character table of S_n are divisible by any fixed prime power. We have now proven this most general of Miller's conjectures:

Theorem 3 (P.–Soundararajan, 2022+). *Let n be large and p^r be a prime power with $p^r \leq 10^{-3}\log n/(\log\log n)^2$. The proportion of entries in the character table of S_n that are not divisible by p^r is at most*

$$O\left(\frac{r\,(p^r+1)^{r-1}}{n^{1/13p^r}}\right).$$

It then follows the union bound that almost every entry of the character table of S_n is divisible by any fixed integer as n goes to infinity. Our methods don't seem to shed any light on Miller's third and fourth observations.

References

[1] D. Gluck, *Parity in columns of the character table of S_n*, Proc. Amer. Math. Soc., 147(2019), 1005–1011.

[2] J. McKay, *Irreducible representations of odd degree*, J. Algebra, 20(1972), 416–418.

[3] A. R. Miller, *Note on parity and the irreducible characters of the symmetric*, preprint, 2017. arXiv:1708.03267.

[4] A. R. Miller, *On parity and characters of symmetric groups*, J. Combin. Theory Ser. A, 162(2019), 231-240.

[5] A. R. Miller, *Congruences in character tables of symmetric groups*, preprint, 2019. arXiv:1908.03741.

[6] L. Morotti, *On divisibility by primes in columns of character tables of symmetric groups*, Arch. Math. (Basel), 114(2020), 361–365.

[7] S. Peluse, *On even entries in the character table of the symmetric group*, preprint, 2020. arXiv:2007.06652.

[8] S. Peluse and K. Soundararajan, *Almost all entries in the character table of the symmetric group are multiples of any given prime*, J. Reine Angew. Math., 786(2022), 45–53.

The irrationality of a divisor function series of Erdős and Kac

Kyle Pratt

For a positive integer k, let $\sigma_k(n)$ be the sum of the kth powers of the divisors of n. Paul Erdős and Mark Kac [3] conjectured that the number

$$\alpha_k := \sum_{n\geq 1} \frac{\sigma_k(n)}{n!}$$

is irrational for every $k \geq 1$.

The conjecture seems *ad hoc*, but is related to some important and interesting mathematics. In particular, the Erdős-Kac conjecture is connected to questions about irrationality and transcendence of *E-functions* evaluated at algebraic points. Introduced by Siegel in 1929 [10], E-functions are generalizations of the exponential function. They are entire functions given by

$$f(z) = \sum_{n\geq 1} \frac{a_n}{n!} z^n,$$

where the a_n are algebraic numbers which do not grow too quickly and whose denominators also do not grow too quickly (see [11, p. 33]). If an E-function f satisfies a simple differential equation then ideas of Siegel and Shidlovskii [9] allow one to prove that $f(\alpha)$ is transcendental for all algebraic α except possibly for a finite number in an explicit set depending on f.

We therefore interpret the Erdős-Kac conjecture to be asserting something about the E-functions

$$f_k(z) = \sum_{n\geq 1} \frac{\sigma_k(n)}{n!} z^n$$

evaluated at $z = 1$. This suggests immediate generalizations of the Erdős-Kac conjecture. For our purposes here we just note that the E-functions $f_k(z)$ seem to lack

any suitable differential structure, so the ideas of Siegel-Shidlovskii are not available. Irrationality and transcendence results for E-functions without differential structure are hard to come by.

It is on the level of an exercise to prove that α_1 and α_2 are irrational [6, 1]. Schlage-Puchta [8] and Friedlander-Luca-Stoiciu [5] independently proved that α_3 is irrational. Their proofs used sieve theory arguments on the level of Chen's theorem that infinitely often $p+2$ has at most two prime factors (see [4, Theorem 25.10]). One can prove that α_k is irrational for every k if one assumes difficult conjectures like the Hardy-Littlewood prime k-tuples conjecture [5, Theorem 2] or Schinzel's Hypothesis H [8, Theorem].

Going slightly beyond irrationality, Deajim and Siksek [2] proved a criterion (conditional on Schinzel's Hypothesis H) for the set $\{1, \alpha_1, \alpha_2, \cdots, \alpha_r\}$ to be linearly independent over $\mathbb{Q}$, and showed the criterion holds for $r = 50$.

We recently proved the following theorem [7].

Theorem 1. *The number*

$$\alpha_4 = \sum_{n\geq 1} \frac{\sigma_4(n)}{n!} = 42.30104\ldots$$

is irrational.

Let us describe some of the ideas in the proof of the theorem. Like the previous works [5, 8] the proof relies on the machinery of sieve theory, but our proof is rather more complicated. In fact, it seems we push the methods to the limit, and that fundamentally new ideas are required to establish cases of the Erdős-Kac conjecture for $k \geq 5$.

As in all irrationality proofs, we begin by assuming for contradiction that $\alpha_4 = a/b$ is rational, where a, b are positive integers. For large x we take a prime $p \asymp x$ and consider

$$N_p := (p-1)! \sum_{n\geq p} \frac{\sigma_4(n)}{n!} = (p-1)!\frac{a}{b} - \sum_{n\leq p-1} \sigma_4(n)\frac{(p-1)!}{n!}.$$

Since the right-hand side is an integer, we must have that N_p is an integer. Naturally, we aim to show there is some prime $p \asymp x$ such that N_p is *not*, in fact, an integer. We can expand out N_p in its first few terms, obtaining

$$N_p = \frac{\sigma_4(p)}{p} + \frac{\sigma_4(p+1)}{p(p+1)} + \frac{\sigma_4(p+2)}{p(p+1)(p+2)} + \frac{\sigma_4(p+3)}{p(p+1)(p+2)(p+3)} + \sum_{j\geq 4} \frac{\sigma_4(p+j)}{p(p+1)\cdots(p+j)}.$$

The sum over $j \geq 4$ has size $O(x^{-1})$ and is negligible. Hence, N_p is very close to the sum of the four terms involving $p, p+1, p+2$, and $p+3$. Since integers have fractional part equal to zero, we succeed in showing that N_p is non-integral if we can find some p such that the fractional part of the sum of the four terms on the right-hand side deviates significantly from zero. We accomplish this, in turn, by

controlling three of the terms very precisely, and then showing the last term (the one involving $\sigma_4(p+1)$) has a fractional part which forces N_p to be non-integral.

The term with $\sigma_4(p)$ is nearly integral since p is prime. If we impose the additional condition that $\frac{p+3}{2}$ has no prime factors $\leq (\log x)^{100}$ then the term with $\sigma_4(p+3)$ is $\frac{17}{16} + O((\log x)^{-200})$, which is also well-controlled. We control the term with $\sigma_4(p+2)$ by further requiring that $p+2$ has no prime factors $\leq x^{1/4+\epsilon}$. (In actuality we need a more subtle argument, but we ignore that for the sake of this sketch.) This requires some involved sieve theory computations.

The upshot of all this is that N_p is equal to some terms with well-understood fractional parts, plus $\frac{\sigma_4(p+1)}{p(p+1)} \approx \frac{\sigma_4(p+1)}{(p+1)^2}$. Essentially, we wish to show that we can find a prime p such that the fractional part of $\frac{\sigma_4(p+1)}{(p+1)^2}$ is not very close to $\frac{15}{16} + o(1)$.

We now utilize the fact that, for almost every p, the shifted prime $p+1$ will have a prime factor $q \approx x^\epsilon$. We can then factor $p+1 = qm$ and by multiplicativity we may write

$$\frac{\sigma_4(p+1)}{(p+1)^2} = \frac{\sigma_4(m)}{m^2}(q^2 + q^{-2}).$$

We use Fourier analysis to control the condition on the fractional part, and we succeed if we can obtain nontrivial bounds on exponential sums of the form

$$\sum_{q \approx x^\epsilon} e^{2\pi i A(q^2+q^{-2})},$$

where $A \approx x^2$ is a large real number. These exponential sums can be bounded using classical techniques of Weyl-van der Corput.

References

[1] R. Breusch, Amer. Math. Monthly **61** (1954) 264–265.

[2] A. Deajim, S. Siksek, *On the $\mathbb{Q}$-linear independence of the sums $\sum_{n=1}^{\infty} \sigma_k(n)/n!$*, J. Number Theory **131** (2011), no. 4, 745–749.

[3] P. Erdős and M. Kac, Problem 4518, Amer. Math. Monthly **60** (1953) 47

[4] J. B. Friedlander, H. Iwaniec, *Opera de Cribro*. American Mathematical Society Colloquium Publications, **57**. American Mathematical Society, Providence, RI, 2010.

[5] J. B. Friedlander, F. Luca, M. Stoiciu, *On the irrationality of a divisor function series*, Integers **7** (2007), A31, 9 pp.

[6] J.B. Kelly, Amer. Math. Monthly **60** (1953) 557–558.

[7] K. Pratt, *The irrationality of a divisor function series of Erdős and Kac*, `arXiv:2209.11124`

[8] J. C. Schlage-Puchta, *The irrationality of a number theoretical series*, Ramanujan J. **12** (2006), no. 3, 455–460.

[9] A. B. Shidlovskii, *Transcendental numbers*. Translated from the Russian by Neal Koblitz. With a foreword by W. Dale Brownawell. De Gruyter Studies in Mathematics, 12. Walter de Gruyter & Co., Berlin, 1989.

[10] C.L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. **1**, 1929.

[11] C. L. Siegel, *Transcendental numbers*. Annals of Mathematics Studies, No. 16 Princeton University Press, Princeton, N. J., 1949.

Limit theorems for squarefrees and B-frees in short intervals

Brad Rodgers
(joint work with Ofir Gorodetsky, Alexander Mangerel)

Let S be the set of squarefree integers, and use the notation $N_S(x) := |\{n \leq x : n \in S\}$. It is well known that $N_S(x) \sim \frac{6}{\pi^2}x$. The purpose of this talk was to describe some probabilistic limit theorems proved in the paper [1], regarding the distribution of squarefrees in short intervals. The theorems have a generalization to B-free integers, described later in this abstract.

Let $N_S(n, H) := N_S(n + H) - N_S(n)$ be the count of squarefrees in a short interval of size H. We show that if n is chosen randomly and H is growing slowly that these counts satisfy a central limit theorem:

Theorem 1: *If $X \to \infty$ and $H = H(X) \to \infty$ in such a way that $H = X^{o(1)}$, then for any fixed $z \in \mathbb{R}$,*

$$\lim_{X\to\infty} \frac{1}{X}\Big|\Big\{n \leq X : \frac{N_S(n, H) - \frac{6}{\pi^2}H}{\sqrt{AH^{1/2}}}\Big\}\Big| = \frac{1}{\sqrt{2\pi}}\int_z^\infty e^{-t^2/2}\,dt,$$

where A is a certain arithmetic constant.

In fact we prove the k-th centered moment of $N_S(n; H)$ is Gaussian (and thus of order of magnitude $H^{k/4}$) as long as $H \leq X^{4/(9k)-\varepsilon}$. It would be of interest for e.g. analyzing gaps between squarefrees to replace the exponents $4/(9k)$ with ones that do not decay like $O(1/k)$, but this seems difficult. (One expects Theorem 1 to hold even for $H \leq X^{1-\varepsilon}$.)

Characterizing the distribution of $N_S(n, H)$ answers a question asked by R.R. Hall in [2], who showed that the k-th centered moment of $N_S(n, H)$ is $O(H^{(k-1)/2})$ as long as H grows arbitrarily slowly with X. This was recently improved by R. Nunes [4] who showed for $H \leq X^{4/(9k)-\varepsilon}$ an almost optimal bound that the k-th centered moment is $O(H^{k/4+\varepsilon})$. The ideas of Nunes are one important ingredient in the proof of Theorem 1 as explained below.

One might naively guess that the variance of counts in an interval of length H should be of size roughly H. That it is of the smaller size $H^{1/2}$ speaks to how rigidly the squarefrees are spaced. We elaborate on this idea by proving a functional limit theorem:

For a random starting point $n \leq X$, define random variables $\xi_1, \xi_2, \ldots$ in terms of n by

$$\xi_k = \begin{cases} 1 - 6/\pi^2 & \text{if } n + k \text{ is squarefree} \\ -6/\pi^2 & \text{otherwise,} \end{cases}$$

and define a random function $Q : \mathbb{R}_{\geq 0} \to \mathbb{R}$ by setting

$$Q(\tau) := \sum_{k=1}^{\tau} \xi_k,$$

for $\tau \in \mathbb{N}_{\geq 0}$ and linearly interpolating Q between these values for $\tau \notin \mathbb{N}_{\geq 0}$. The function Q thus records a random walk which increases at squarefree integers and

decreases otherwise. Q is a random function because it depends on the random starting point n.

Theorem 2: *Let $X \to \infty$ and $H = H(X) \to \infty$ in such a way that $H = X^{o(1)}$, and let $n \in [1, X]$ be a random integers chosen at uniform. Define a rescaled variant of Q,*

$$W_X(t) := \frac{1}{\sqrt{AH^{1/2}}} Q(t \cdot H).$$

Then as a random element of $C[0,1]$, the function W_X converges in distribution to a fractional Brownian motion with Hurst parameter $1/4$ as $X \to \infty$.

Fractional Brownian motion is a generalization of classical Brownian motion which depends on a parameter $\gamma \in (0,1)$ called the Hurst parameter. (See e.g. [5] for an introduction.) If $\gamma < 1/2$ increments of the process are negatively correlated; in the context of the squarefrees this has the meaning that if a random short interval contains a relative abundance of squarefrees, it is likely to be followed by an interval with a relative paucity of squarefrees.

In fact a central limit theorem and a functional limit theorem of this sort can be proved for B-free integers, a generalization of the squarefree integers in which indivisibility by squares of primes is replaced by indivisibility by elements of an essentially arbitrary sparse set B. In general the variance asymptotic $AH^{1/2}$ and the Hurst parameter $1/4$ for the squarefrees are replaced by quantities which depend on the sparseness of the set B; further details can be found in [1].

We describe the key features of the proof of Theorem 1 in the language of squarefrees, the proof for B-frees being similar. Using the identity $\mu(m)^2 = \sum_{d^2|m} \mu(d)$ and finite Fourier analysis, the k-th centered moment of a short interval count of squarefrees is related to a (weighted) count of solutions to

$$\frac{\ell_1}{d_1^2} + \cdots \frac{\ell_k}{d_k^2} \in \mathbb{Z} \quad \text{with} \quad \left\| \frac{\ell_i}{d_i^2} \right\| \ll \frac{1}{H},$$

where d_i and (ℓ_i, d_i^2) are squarefree for all i. One expects the dominant contribution to come from diagonal terms, and this produces Gaussian moments. There is a technique for bounding off-diagonal contributions to counts of this sort originating in work of Montgomery-Vaughan [3], but because the main terms here for k-th moments are of smaller size than usual ($H^{k/4}$ rather than $H^{k/2}$), additional ideas are required for a proper bound of off-diagonal contributions.

The first is due to Nunes in [4], who observed that from simple estimates one may restrict attention in counts above to d_i which are large in terms of H. The second is that a (complicated) expression due to Montgomery-Vaughan bounding off-diagonal contributions can be written as a count (still complicated) of certain congruence conditions, which can in turn be bounded using the Pólya-Vinogradov inequality for character sums.

The proof of Theorem 2 involves similar ideas but requires one to consider a weighted count of squarefrees in short intervals in place of $N_S(n, H)$.

References

[1] O. Gorodetsky, A. Mangerel, and B. Rodgers, *Squarefrees are Gaussian in short intervals*, to appear, J. fur reine angew. Math.
[2] R. Hall, *The distribution of squarefree numbers*, J. reine und angew. Math. **394** (1989), 107–117.
[3] H. Montgomery and R. Vaughan, *On the distribution of reduced residues*, Ann. Math. **123 (2)** (1986), 311–333.
[4] R. M. Nunes, *Moments of the distribution of k-free numbers in short intervals and arithmetic progressions*, Bull. Lond. Math. Soc. **54** (2022), no. 4, 1282–1298.
[5] I. Nourdin, *Selected aspects of fractional Brownian motion*, Bocconi & Springer Series **4** (2012).

Bounds on 2-torsion in class groups over number fields

Per Salberger

We sketched in our talk a proof of the following result.

Theorem 1. *Let K be a number field of degree n and $h_2(K)$ the size of the 2-torsion subgroup of the class group of K. Let O_K be the ring of integers in K and $\{1, v_1, \dots, v_{n-1}\}$ be a Minkowski reduced basis of O_K with $1 \le |v_1| \le \dots \le |v_{n-1}|$ and $|v_1| = O_n(|\mathrm{Disc}(K)|^{\mu})$. Then,*

$$h_2(K) = O_{n,\varepsilon}(|\mathrm{Disc}(K)|^{\frac{1}{2}-\frac{2}{n}+\mu+\frac{2}{n}\sqrt{\frac{1-n\mu}{2}}+\varepsilon}).$$

This result is an improvement of the bound $h_2(K) = O_{n,\varepsilon}(|\mathrm{Disc}(K)|^{\frac{1}{2}-\frac{1}{n}+\varepsilon})$ in [1] in case $\mu \le \frac{1}{2n}$. The condition on $|v_1|$ is relatively mild for large n as $|v_1| = O_n(|\mathrm{Disc}(K)|^{\frac{1}{2(n-1)}})$.

To prove the theorem, we refine the method in [1] by reducing to a counting problem for affine surfaces instead of affine curves. This counting problem is treated with the authors global determinant method [3] and an estimate in [2].

References

[1] M. Bhargava, A. Shankar, T. Taniguchi, F. Thorne, J. Tsimerman, Y.Zhao : *Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves*, J. Amer. Math. Soc. 33 (2020), 1087-1099.
[2] D.R. Heath-Brown : *Counting rational points on algebraic varieties.* Analytic number theory, 51–95, Lecture Notes in math 1891. Springer, Berlin, 2006.
[3] P. Salberger : *Counting rational points on projective varieties*, to appear in The Proceedings of the London Mathematical Society.

Algebraic integers with conjugates in a prescribed distribution

Alexander Smith

Take λ to be the maximal positive real number so that, for any $\epsilon > 0$, there are only finitely many totally positive algebraic integers satisfying

$$\frac{\text{trace}(\alpha)}{\text{degree}(\alpha)} < \lambda - \epsilon.$$

A simple construction using the roots of unity shows that λ is at most 2. The *trace problem*, as codified in [3], is to show that $\lambda = 2$.

Smyth developed a method for finding lower bounds on λ that exploited the fact that, for a given algebraic integer with conjugates $\alpha_1, \ldots, \alpha_n$, and for any integer polynomial Q not having these integers as roots, we have $\prod_{i \leq n} |Q(\alpha_i)| \geq 1$. By applying this result with about 15 polynomials Q, Smyth was able to prove $\lambda > 1.7719$ [6]. Though this bound has been slightly improved [7], the method for producing such lower bounds has not advanced.

Serre and Smyth both observed that Smyth's method could not get close to proving $\lambda = 2$, with Serre showing that Smyth's method could not prove that $\lambda \geq 1.8984$ [1, Appendix B]. We give a simple explanation for this result.

Theorem 1 ([5])**.** *We have* $\lambda < 1.8984$.

To prove this, we characterize which probability measures are expressible as a limit of the distribution of conjugates for some sequence of totally real algebraic integers.

Theorem 2 ([5])**.** *Take* Σ *to be a subinterval of* $\mathbb{R}$ *of length greater than* 4. *Take* μ *to be a probability measure on* Σ. *Then the following two conditions are equivalent.*

(1) *There is a sequence of distinct algebraic integers* $\alpha_1, \alpha_2, \ldots$ *whose conjugates all lie in* Σ *and whose distribution of conjugates weak* converge to* μ.
(2) *For every nonzero integer polynomial* Q,

$$\int_\Sigma \log |Q(x)| d\mu(x) \geq 0.$$

The proof that (2) implies (1) is nonconstructive, relying on abstract existence results from the geometry of numbers that guarantee the presence of lattice points in convex bodies. These include Minkowski's second theorem [4, p. 376] and the more recent flatness theorem [2, Corollary 2.5].

References

[1] J. Aguirre and J. C. Peral, *The trace problem for totally positive algebraic integers*, Number theory and polynomials, London Math. Soc. Lecture Note Ser., vol. 352, Cambridge Univ. Press, Cambridge, 2008, With an appendix by J.-P. Serre, pp. 1–19.

[2] W. Banaszczyk, A. E. Litvak, A. Pajor, and S. J. Szarek, *The flatness theorem for nonsymmetric convex bodies via the local theory of Banach spaces*, Math. Oper. Res. **24** (1999), no. 3, 728–750.

[3] P. Borwein, *Computational excursions in analysis and number theory*, CMS Books in Mathematics/Ouvrages de Mathématiques de la SMC, vol. 10, Springer-Verlag, New York, 2002.
[4] P. M. Gruber, *Convex and discrete geometry*, Grundlehren der Mathematischen Wissenschaften, vol. 336, Springer, Berlin, 2007.
[5] A. Smith. Algebraic integers with conjugates in a prescribed distribution. *arXiv preprint arXiv:2111.12660*, 2021.
[6] C. J. Smyth, *The mean values of totally real algebraic integers*, Math. Comp. **42** (1984), no. 166, 663–681.
[7] Cong Wang, Jie Wu, and Qiang Wu, *Totally positive algebraic integers with small trace*, Math. Comp. **90** (2021), no. 331, 2317–2332.

Primes and squares with preassigned digits

Cathy Swaenepoel

Let $g \geq 2$ be an integer. Any integer $k \geq 0$ may be written in base g as

$$k = \sum_{j \geq 0} \varepsilon_j(k) g^j$$

where, for any $j \geq 0$, $\varepsilon_j(k) \in \{0, \dots, g-1\}$ is the digit of k at the position j in base g.

In 2015, Bourgain [2] obtained an asymptotic formula for the number of primes with a proportion $c > 0$ of preassigned digits in base 2 (c was an absolute constant not specified). This significantly improved on [1, 3, 4, 5, 7] where fewer digits could be preassigned. In [6], we generalize Bourgain's result to any base.

Theorem 1. *Let $g \geq 2$ be an integer. There is an explicit $c_0 = c_0(g) \in [0,1)$ with the following property. For any $c \in (0, c_0)$, there exists $\delta = \delta(g,c) \in (0,1]$ such that for any integer $n \geq 1$, for any $A \subset \{0, \dots, n-1\}$ satisfying $\{0, n-1\} \subset A$ and $|A| \leq cn$, for any $\boldsymbol{d} = (d_j)_{j \in A} \in \{0, \dots, g-1\}^A$ such that $\gcd(d_0, g) = 1$ and $d_{n-1} \geq 1$, we have*

$$|\{p < g^n : p \text{ prime}, \forall j \in A, \varepsilon_j(p) = d_j\}| = \frac{g^{n-|A|}}{\log g^n} \frac{g}{\varphi(g)} \left(1 + O_{g,c}\left(n^{-\delta}\right)\right).$$

Moreover, we provide explicit admissible values for the proportion c_0 depending on g. For instance, Theorem 1 holds with $c_0(2) = 0.0021$ and $c_0(10) = 0.0047$. Our proof, which adapts, develops and refines Bourgain's strategy, is based on the circle method and combines techniques from harmonic analysis with results on zeros of Dirichlet L-functions due to Iwaniec.

More recently, we obtain a result for squares. Let $v_2(g)$ denote the 2-adic valuation of g and for $m \geq 1$, let $\mathcal{Q}(m) = \{k \in \mathbb{Z} : k \text{ is a square mod } m\}$. The digits of squares satisfy algebraic constraints. This leads to the following hypothesis:

$$(1) \quad \begin{cases} \{0,1,2\} \subset A,\ \gcd(d_0, g) = 1,\ d_2 g^2 + d_1 g + d_0 \in \mathcal{Q}(g^3) & \text{if } v_2(g) = 1, \\ \{0,1\} \subset A,\ \gcd(d_0, g) = 1,\ d_1 g + d_0 \in \mathcal{Q}(g^2) & \text{if } v_2(g) = 2, \\ \{0\} \subset A,\ \gcd(d_0, g) = 1,\ d_0 \in \mathcal{Q}(g) & \text{otherwise.} \end{cases}$$

For any base we obtain an asymptotic formula for the number of squares with a proportion $c > 0$ of preassigned digits:

Theorem 2. *Let $g \geq 2$ be an integer. There is an explicit $c_0 = c_0(g) \in [0, 1/2)$ with the following property. For any $c \in (0, c_0)$, there exists $\delta = \delta(c) > 0$ such that for any integer $n \geq 4$, for any $A \subset \{0, \dots, n-1\}$ and $\boldsymbol{d} = (d_j)_{j \in A} \in \{0, \dots, g-1\}^A$ satisfying the condition (1), $n - 1 \in A$, $d_{n-1} \geq 1$ and $|A| \leq cn$, we have*

$$|\{k < g^n : k \text{ square}, \forall j \in A, \varepsilon_j(k) = d_j\}| = \mathfrak{S}(g, n, A, \boldsymbol{d}) \left(1 + O_{g,c}\left(n^{-\delta}\right)\right)$$

where

$$\mathfrak{S}(g, n, A, \boldsymbol{d}) = \eta(g) \sum_{\substack{k < g^n \\ \forall j \in A,\, \varepsilon_j(k) = d_j}} \frac{1}{2\sqrt{k}}$$

with

$$\eta(g) = \begin{cases} 2^{\omega(g)} & \text{if } g \text{ is odd,} \\ 2^{\omega(g)+1} & \text{if } g \text{ is even.} \end{cases}$$

The order of magnitude of the main term is $g^{\frac{n}{2} - |A|}$ as expected. We also provide explicit values for c_0 depending on g: Theorem 2 holds with $c_0(2) = 0.0058$ and $c_0(10) = 0.0163$. Our proof mainly follows the strategy in [2, 6] for primes with preassigned digits. Since squares are much sparser than primes, new difficulties arise. Moreover, we have to deal with new algebraic constraints on the digits. The proof uses the circle method and combines techniques from harmonic analysis with arithmetic properties of squares and bounds for quadratic Weyl sums.

References

[1] J. Bourgain, *Prescribing the binary digits of primes*, Israel J. Math., 194(2013), 935–955.

[2] ———, *Prescribing the binary digits of primes, II*, Israel J. Math., 206(2015), 165–182.

[3] G. Harman, *Primes with preassigned digits*, Acta Arith., 125(2006), 179–185.

[4] G. Harman and I. Kátai, *Primes with preassigned digits. II*, Acta Arith., 133(2008), 171–184.

[5] I. Kátai, *Distribution of digits of primes in q-ary canonical form*, Acta Math. Hungar., 47(1986), 341–359.

[6] C. Swaenepoel, *Prime numbers with a positive proportion of preassigned digits*, Proceedings of the London Mathematical Society, 121(2020), 83–151.

[7] D. Wolke, *Primes with preassigned digits*, Acta Arith., 119(2005), 201–209.

Reporters:
Kaisa Matomäki, Kannan Soundararajan, Robert C. Vaughan, Trevor D. Wooley

Participants

Dr. Christoph Aistleitner
Institut für Analysis und Zahlentheorie
Technische Universität Graz
Steyrergasse 30
8010 Graz
AUSTRIA

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

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

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

Dr. Thomas Bloom
Mathematical Institute
Oxford University
Woodstock Road
Oxford OX2 6GG
UNITED KINGDOM

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

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

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

Prof. Dr. Vorrapan Chandee
Department of Mathematics
Kansas State University
Manhattan, KS 66506-2602
UNITED STATES

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

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

Dr. Cecile Dartyge
Institut Elie Cartan
-Mathématiques-
Université Henri Poincare, Nancy I
Boite Postale 239
54506 Vandoeuvre-lès-Nancy Cedex
FRANCE

Prof. Dr. Régis De La Bretèche
Université Paris Cité
Institut de Mathématiques de Jussieu
Paris Rive Gauche
75205 Paris Cedex 13
FRANCE

Dr. Lucile Devin
Département de Mathématiques
Université du Littoral
50 Rue F. Buisson
P.O. Box CS 80699
62100 Calais
FRANCE

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

Dr. Alexandra Florea
Department of Mathematics
University of California, Irvine
Irvine, CA 92697-3875
UNITED STATES

Prof. Dr. Etienne Fouvry
Laboratoire de mathématiques d'Orsay
CNRS, Université Paris-Saclay
Bâtiment 307
91405 Orsay Cedex
FRANCE

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

Prof. Dr. Sanoli Gun
The Institute of Mathematical Sciences
IV Cross Road, CIT Campus
Tamil Nadu Taramani,Chennai 600 113
INDIA

Dr. Shaoming Guo
Department of Mathematics
University of Wisconsin-Madison
480 Lincoln Drive
Madison WI 53706
UNITED STATES

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

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

Prof. Dr. Harald A. Helfgott
Dept. de Mathématiques et Applications
École Normale Superieure
45, rue d'Ulm
75230 Paris Cedex 05
FRANCE

Leonhard Hochfilzer
Mathematisches Institut
Georg-August-Universität Göttingen
Bunsenstr. 3-5
37073 Göttingen
GERMANY

Prof. Dr. Emmanuel Kowalski
Departement Mathematik
ETH - Zentrum
Rämistrasse 101
8092 Zürich
SWITZERLAND

Dr. Vivian Kuperberg
Department of Mathematics
School of Mathematical Sciences
Tel Aviv University
P.O.Box 39040
Ramat Aviv, Tel Aviv 69978
ISRAEL

Prof. Dr. Matilde N. Lalin
Department of Mathematics and Statistics
University of Montreal
CP 6128, succ. Centre Ville
Montréal QC H3C 3J7
CANADA

Dr. Stephen Lester
King's College London
Department of Mathematics
Strand
London WC2R 2LS
UNITED KINGDOM

Dr. Junxian Li
Mathematisches Institut
Universität Bonn
Endenicher Allee 60
53115 Bonn
GERMANY

Jared Duker Lichtman
Mathematical Institute
University of Oxford
Oxford OX2 6GG
UNITED KINGDOM

Dr. Alexander Mangerel
Dept. of Mathematical Sciences
Durham University
Science Laboratories
Stockton Road
Durham DH1 3LE
UNITED KINGDOM

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

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

Dr. Jori Merikoski
Mathematical Institute
Oxford University
24-29 St. Giles
Oxford OX1 3LB
UNITED KINGDOM

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

Dr. Simon L. R. Myerson
Mathematics Institute, University of Warwick
Zeeman Building
Coventry CV4 7AL
UNITED KINGDOM

Dr. Sarah Peluse
Department of Mathematics
Princeton University
Fine Hall
Washington Road
Princeton, NJ 08544-1000
UNITED STATES

Dr. Javier Pliego Garcia
Department of Mathematics
KTH
10044 Stockholm
SWEDEN

Dr. Kyle Pratt
All Souls College
Oxford OX1 4AL
UNITED KINGDOM

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

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

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

Prof. Dr. Damaris Schindler
Mathematisches Institut
Georg-August-Universität Göttingen
Bunsenstr. 3-5
37073 Göttingen
GERMANY

Dr. Fernando Xuancheng Shao
Department of Mathematics
University of Kentucky
Lexington, KY 40506-0027
UNITED STATES

Dr. Alexander Smith
Department of Mathematics
Stanford University
Stanford, CA 94305-2125
UNITED STATES

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

Dr. Ade Irma Suriajaya
Faculty of Mathematics
Kyushu University
744 Motooka, Nishi-ku
Fukuoka 819-0395
JAPAN

Dr. Cathy Swaenepoel
Institut de Mathématiques de Jussieu-Paris Rive Gauche
Université Paris Cité
8 Place Aurélie Nemours
P.O. Box 7012
75205 Paris Cedex 13
FRANCE

Dr. Joni Teräväinen
Department of Mathematics and Statistics
Turku University
20014 University of Turku
FINLAND

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

Prof. Dr. Lola Thompson
Mathematisch Instituut
Universiteit Utrecht
Budapestlaan 6
P. O. Box 80.010
3508 TA Utrecht
NETHERLANDS

Dr. Lilu Zhao
Department of Mathematics
Shandong University
27 Shanda Nanlu
Jinan
Jinan, Shandong 250100
CHINA

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